Independent Service Auditor's Report to SOC2 type 2 for Big Dig Data s.r.o.

SERVICE ORGANIZATION CONTROL (SOC) 2 TYPE 2 REPORT
REPORT ON CONTROLS AT SERVICE ORGANIZATION RELEVANT TO DESCRIPTION OF Big Dig Data s.r.o. SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS TO MEET THE CRITERIA FOR THE SECURITY, AVAILABILITY AND CONFIDENTIALITY.
THROUGHOUT THE PERIOD 16.07.2025 THROUGH 16.07.2026

AUDIT REPORT SUMMARY

Scope	Big Dig Data s.r.o.
Period of Examination	16.07.2025 – 16.07.2026
Applicable Trust Principle(s)	Security, Availability, Confidentiality
Location (s)	U Větrníku 40/1, Praha, 16200 Czech Republic
Subservice Providers	
Opinion Result	**Unqualified**
Testing Exceptions	**-**

INDEPENDENT SERVICE AUDITOR´S REPORT

To: Board of Directors of Big Dig Data s.r.o.

Scope:

We have examined Big Dig Data s.r.o. accompanying description of its system throughout the period 16.07.2025 to 16.07.2026, based on the criteria set forth in paragraph 1.26 of the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Confidentiality (SOC 2®) (description criteria) and the suitability of the design and operating effectiveness of controls included in the description throughout the period 16.07.2025 to 16.07.2026 to meet the criteria for security, availability and confidentiality set forth in TSP section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability and Confidentiality (applicable trust services criteria).

Service Organization's Responsibilities

Big Dig Data s.r.o. has provided the accompanying assertion titled, about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. Big Dig Data s.r.o. is responsible for preparing the description and assertion; including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and documenting controls that are suitably designed; and operating effectively to meet the applicable trust services criteria stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination. Our examination was conducted in accordance with ISAE 3000 standard. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period 16.07.2025 to 16.07.2026. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion. An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the

design and operating effectiveness of the controls to meet the applicable trust services criteria.
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria.
- Testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met.
- Evaluating the overall presentation of the description.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs. Because of their nature, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria are subject to the risks that the system may change or that controls at a service organization may become ineffective.

Description of Tests of Controls The specific controls we tested, and the nature, timing, and results of those tests are listed in Section IV of this report.

Opinion

In our opinion, in all material respects, based on the description criteria and the applicable trust services criteria:

a. The description fairly presents the system that was designed and implemented throughout the period 16.07.2025 to 16.07.2026.

b. The controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period 16.07.2025 to 16.07.2026.

c. The controls operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period 16.07.2025 to 16.07.2026.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Big Dig Data s.r.o. user entities of Big Dig Data s.r.o. system during some or all of the period 16.07.2025 to 16.07.2026, and prospective user entities, independent auditors, and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, subservice organizations, and other parties.
- Internal control and its limitations.
- User entity responsibilities, complementary user entity controls, and how they interact with related controls at the service organization to meet the applicable trust services criteria.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

URS s.r.o.
16.07.2026

MAGEMENT OF Big Dig Data s.r.o. SERVICE ORGANIZATION ´S ASSERTION

We have prepared the accompanying description of Big Dig Data s.r.o. (service organization, or Company) customer communications management solutions system titled Big Dig Data s.r.o. Description of Its Customer Communications Management Solutions System throughout the period y 16.07.2025 to 16.07.2026 (description), based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) (description criteria). The description is intended to provide report users with information about the customer communications management solutions system that may be useful when assessing the risks arising from interactions with Big Dig Data s.r.o. system, particularly information about system controls that Big Dig Data s.r.o. has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 (Update 2022) Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

The description also indicates that certain trust services criteria specified in the description can be met only if complementary user entity controls contemplated in the design of Big Dig Data s.r.o. organization's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of user entities.

We confirm, to the best of our knowledge and belief, that:

a. the description fairly presents the system throughout the period 16.07.2025 to 16.07.2026, based on the following description criteria:

i. The description contains the following information:

(1) The types of services provided.

(2) The components of the system used to provide the services, which are as follows:

(a) Infrastructure. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other tele- communications networks).

(b) Software. The application programs and IT system software that support application programs (operating systems, middleware, and utilities).

(c) People. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).

(d) Procedures. The automated and manual procedures.

(e) Data. Transaction streams, files, databases, tables, and output used or processed by the system.

(3) The boundaries or aspects of the system covered by the description.

(4) For information provided to, or received from, subservice organizations or other parties:

(a) how such information is provided or received and the role of the sub- service organization and other parties, and

(b) the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

(5) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

(a) Complementary user entity controls contemplated in the design of the service organization's system.

(b) When the inclusive method is used to present a subservice organi- zation, controls at the subservice organization.

(6) If the service organization presents the subservice organization using the carve- out method:

(a) the nature of the services provided by the subservice organization,

(b) each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with con- trols at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.

(7) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons.

(8) In the case of a type 2 report, relevant details of changes to the service organization's system during the period covered by the description.

ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated as described.

The Big Dig Data s.r.o. organization's controls stated in the description operated effectively throughout the period 16.07.2025 to 16.07.2026 to meet the applicable trust services.

.....

Big Dig Data s.r.o.

16. 07. 2026

DESCRIPTION OF BIG DIG DATA S.R.O. SYSTEM

USABILITY OF THE REPORT
COMPANY PROFILE

Big Dig Data s.r.o. (“Big Dig Data”) operates CELUS, a software-as-a-service platform that harvests, processes, and analyzes electronic-resource usage statistics (COUNTER and non-COUNTER, via SUSHI) for libraries and institutions.

We have prepared the accompanying description titled “Description of the CELUS System of Big Dig Data s.r.o. throughout the period June 2025 to June 2026” (the description) based on the criteria for a description of a service organization’s system set forth in DC section 200, 2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report (description criteria).

The description is intended to provide report users with information about the CELUS system that may be useful when assessing the risks arising from interactions with Big Dig Data’s system, particularly information about system controls that Big Dig Data has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria).

Subservice organizations
Big Dig Data uses DigitalOcean to provide cloud hosting and infrastructure services for the CELUS system. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Big Dig Data, to achieve Big Dig Data’s service commitments and system requirements based on the applicable trust services criteria. The description presents Big Dig Data’s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Big Dig Data’s controls. The description does not disclose the actual controls at the subservice organization (carve-out method).

Complementary user entity controls
The description also indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Big Dig Data, to achieve the service commitments and system requirements based on the applicable trust services criteria. The description presents Big Dig Data’s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Big Dig Data’s controls.

Our assertion
We confirm, to the best of our knowledge and belief, that:

A. the description presents the CELUS system that was designed and implemented throughout the period June 2025 to June 2026 in accordance with the description criteria;
B. the controls stated in the description were suitably designed throughout the period June 2025 to June 2026 to provide reasonable assurance that Big Dig Data's service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Big Dig Data's controls throughout that period;
C. the controls stated in the description operated effectively throughout the period June 2025 to June 2026 to provide reasonable assurance that Big Dig Data's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization controls and complementary user entity controls assumed in the design of Big Dig Data's controls operated effectively throughout that period.

INFORMATION PROVIDED BY INDEPENDENT SERVICE AUDITORS

Introduction

This report and the description of tests of controls, tests of Big Dig Data s.r.o. 's compliance with the commitments in its statement of privacy practices, and results thereof in Section IV of this report are intended solely for the information and use of Big Dig Data s.r.o. ; user entities of Big Dig Data s.r.o. 's system using the Big Dig Data s.r.o. software, during some or all of the period 16.07.2025 to 16.07.2026; and those prospective user entities, independent auditors, and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

A. The nature of the service provided by the service organization;
B. How the service organization's system interacts with user entities, subservice organizations, and other parties;
C. Internal control and its limitations;
D. Complementary user entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria;
E. The applicable trust services criteria;
F. The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties.

This examination was performed in accordance with ISAE 3000 and the guidance contained in the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability and Confidentiality . This description does not encompass all aspects of the procedures and controls performed by Big Dig Data s.r.o. and is intended to describe only controls that may be relevant to the Big Dig Data s.r.o. System using the Big Dig Data s.r.o. Software, provided to Big Dig Data s.r.o. user entities throughout the period 16.07.2025 to 16.07.2026. URS s.r.o.'s tests of controls were restricted to the controls specified by Big Dig Data s.r.o. in Section IV and were not extended to controls in effect at user entities or other controls which were not documented as tested under each criterion listed in Section IV.

TRUST SERVICES criteria and control activities provided by Big Dig Data s.r.o. and Test Results provided by URS

CRITERIA COMMON TO ALL SECURITY, ABAILABILITY AND CONFIDENTIALITY PRINCIPLES

CC1.0 Control Environment

Criteria		Controls Defined by Big Dig Data s.r.o.	Tests of Controls Performed by URS	Results of Tests
CC1.1	**COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.**			
	Sets the Tone at the Top—The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.	Management promotes integrity and ethical conduct through its policies and day-to-day leadership. Expectations for ethical behavior are formally defined in the Company's Code of Ethics (version 1.0, effective 1 January 2026, publicly classified), referenced from the top-level ISMS Policy and reinforced through the disciplinary process described in the Human Resources Security Policy. The Code covers conflicts of interest, protection of client and personal data, a non-discriminatory working environment, environmental responsibility, and violation reporting with whistleblower protection under Act No. 171/2023 Coll. Deviations from expected conduct are addressed by the Cybersecurity Manager (CSM) and, for serious cases, escalated to management. Contractors and freelance collaborators operate under contracts that include confidentiality and compliance requirements and are explicitly within the Code's scope.	URS inspected the applicable policies, process descriptions, and supporting evidence (1.01 Information Security Management System Policy; 1.07 Human Resources Security Policy (3.6); Code of Ethics v1.0 (effective 1 Jan 2026)) and confirmed that the rules and related processes addressing 'Sets the Tone at the Top' are defined and operating as described. URS further confirmed that integrity and ethical conduct requirements are formally defined, communicated, applied to personnel and contractors, and supported by escalation and disciplinary processes.	**No exceptions noted.**

	Establishes Standards of Conduct—The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the entity and by outsourced service providers and business partners.	Management promotes integrity and ethical conduct through its policies and day-to-day leadership. Expectations for ethical behavior are formally defined in the Company's Code of Ethics (version 1.0, effective 1 January 2026, publicly classified), referenced from the top-level ISMS Policy and reinforced through the disciplinary process described in the Human Resources Security Policy. The Code covers conflicts of interest, protection of client and personal data, a non-discriminatory working environment, environmental responsibility, and violation reporting with whistleblower protection under Act No. 171/2023 Coll. Deviations from expected conduct are addressed by the Cybersecurity Manager (CSM) and, for serious cases, escalated to management. Contractors and freelance collaborators operate under contracts that include confidentiality and compliance requirements and are explicitly within the Code's scope.	URS verified the documented control design and supporting records mapped to CC1.1 and assessed the specific requirement that the expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the entity and by outsourced service providers and business partners. Based on the POA description and the referenced evidence, URS found that management promotes integrity and ethical conduct through its policies and day-to-day leadership. Deviations from expected conduct are addressed by the Cybersecurity Manager (CSM) and, for serious cases, escalated to management.	**No exceptions noted.**
	Evaluates Adherence to Standards of Conduct—Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.	Management promotes integrity and ethical conduct through its policies and day-to-day leadership. Expectations for ethical behavior are formally defined in the Company's Code of Ethics (version 1.0, effective 1 January 2026, publicly classified), referenced from the top-level ISMS Policy and reinforced through	URS reviewed the applicable policy requirements and implementation evidence mapped to CC1.1 and assessed the specific requirement that processes are in place to evaluate the performance of individuals and teams against	**No exceptions noted.**

		the disciplinary process described in the Human Resources Security Policy. The Code covers conflicts of interest, protection of client and personal data, a non-discriminatory working environment, environmental responsibility, and violation reporting with whistleblower protection under Act No. 171/2023 Coll. Deviations from expected conduct are addressed by the Cybersecurity Manager (CSM) and, for serious cases, escalated to management. Contractors and freelance collaborators operate under contracts that include confidentiality and compliance requirements and are explicitly within the Code's scope.	the entity's expected standards of conduct. Based on the POA description and the referenced evidence, URS concluded that management promotes integrity and ethical conduct through its policies and day-to-day leadership. Deviations from expected conduct are addressed by the Cybersecurity Manager (CSM) and, for serious cases, escalated to management	
	Addresses Deviations in a Timely Manner— Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.	Management promotes integrity and ethical conduct through its policies and day-to-day leadership. Expectations for ethical behavior are formally defined in the Company's Code of Ethics (version 1.0, effective 1 January 2026, publicly classified), referenced from the top-level ISMS Policy and reinforced through the disciplinary process described in the Human Resources Security Policy. The Code covers conflicts of interest, protection of client and personal data, a non-discriminatory working environment, environmental responsibility, and violation reporting with whistleblower protection under Act	URS examined the applicable policy requirements and implementation evidence mapped to CC1.1 and assessed the specific requirement that deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner. Based on the POA description and the referenced evidence, URS found that deviations from expected conduct are addressed by the Cybersecurity Manager (CSM) and, for serious cases, escalated to	**No exceptions noted.**

		No. 171/2023 Coll. Deviations from expected conduct are addressed by the Cybersecurity Manager (CSM) and, for serious cases, escalated to management. Contractors and freelance collaborators operate under contracts that include confidentiality and compliance requirements and are explicitly within the Code's scope.	management. Management promotes integrity and ethical conduct through its policies and day-to-day leadership	
	Additional point of focus when using the trust services criteria:			
	Considers Contractors and Vendor Employees in Demonstrating Its Commitment—Management and the board of directors consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner.	Management promotes integrity and ethical conduct through its policies and day-to-day leadership. Expectations for ethical behavior are formally defined in the Company's Code of Ethics (version 1.0, effective 1 January 2026, publicly classified), referenced from the top-level ISMS Policy and reinforced through the disciplinary process described in the Human Resources Security Policy. The Code covers conflicts of interest, protection of client and personal data, a non-discriminatory working environment, environmental responsibility, and violation reporting with whistleblower protection under Act No. 171/2023 Coll. Deviations from expected conduct are addressed by the Cybersecurity Manager (CSM) and, for serious cases, escalated to management. Contractors and freelance collaborators operate under contracts that include confidentiality	URS assessed the applicable policy requirements and implementation evidence mapped to CC1.1 and assessed the specific requirement that management and the board of directors consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner. Based on the POA description and the referenced evidence, URS determined that contractors and freelance collaborators operate under contracts that include confidentiality and compliance requirements and are explicitly within the Code's scope. Management promotes integrity	**No exceptions noted.**

		and compliance requirements and are explicitly within the Code's scope.	and ethical conduct through its policies and day-to-day leadership	
CC1.2	**COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.**			
	Establishes Oversight Responsibilities—The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.	BDD does not have a formal board of directors; management consists of the managing director and one additional manager. Oversight of the ISMS is exercised through compensating structures appropriate to the company's size: the Cybersecurity Manager (CSM) is responsible for the day-to-day design and operation of the ISMS, while independent oversight of the ISMS itself is provided by an externally sourced, independent Auditor of Cybersecurity, who is organizationally separate from the CSM and from IT operations and reports results directly to management. An external cybersecurity audit has already been performed, confirming that this oversight is not only defined but actively exercised. Security, availability, and confidentiality expertise is supplemented through external consultants as needed.	URS inspected the governing procedures and referenced evidence mapped to CC1.2 and assessed the specific requirement that the board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations. Based on the POA description and the referenced evidence, URS established that oversight of the ISMS is exercised through compensating structures appropriate to the company's size: the Cybersecurity Manager (CSM) is responsible for the day-to-day design and operation of the ISMS, while independent oversight of the ISMS itself is provided by an externally sourced, independent Auditor of Cybersecurity, who is organizationally separate from the CSM and from IT operations and reports results directly to management. An external cybersecurity audit has already	**No exceptions noted.**

			been performed, confirming that this oversight is not only defined but actively exercised	
	Operates Independently—The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.	BDD does not have a formal board of directors; management consists of the managing director and one additional manager. Oversight of the ISMS is exercised through compensating structures appropriate to the company's size: the Cybersecurity Manager (CSM) is responsible for the day-to-day design and operation of the ISMS, while independent oversight of the ISMS itself is provided by an externally sourced, independent Auditor of Cybersecurity, who is organizationally separate from the CSM and from IT operations and reports results directly to management. An external cybersecurity audit has already been performed, confirming that this oversight is not only defined but actively exercised. Security, availability, and confidentiality expertise is supplemented through external consultants as needed.	URS reviewed the relevant policies, technical arrangements, and retained evidence mapped to CC1.2 and assessed the specific requirement that the board of directors has sufficient members who are independent from management and objective in evaluations and decision making. Based on the POA description and the referenced evidence, URS confirmed that bDD does not have a formal board of directors; management consists of the managing director and one additional manager. Oversight of the ISMS is exercised through compensating structures appropriate to the company's size: the Cybersecurity Manager (CSM) is responsible for the day-to-day design and operation of the ISMS, while independent oversight of the ISMS itself is provided by an externally sourced, independent Auditor of Cybersecurity, who is organizationally separate from	**No exceptions noted.**

			the CSM and from IT operations and reports results directly to management	
	Applies Relevant Expertise—The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate action.	BDD does not have a formal board of directors; management consists of the managing director and one additional manager. Oversight of the ISMS is exercised through compensating structures appropriate to the company's size: the Cybersecurity Manager (CSM) is responsible for the day-to-day design and operation of the ISMS, while independent oversight of the ISMS itself is provided by an externally sourced, independent Auditor of Cybersecurity, who is organizationally separate from the CSM and from IT operations and reports results directly to management. An external cybersecurity audit has already been performed, confirming that this oversight is not only defined but actively exercised. Security, availability, and confidentiality expertise is supplemented through external consultants as needed.	URS examined the control documentation, assigned responsibilities, and available records mapped to CC1.2 and assessed the specific requirement that the board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate action. Based on the POA description and the referenced evidence, URS verified that security, availability, and confidentiality expertise is supplemented through external consultants as needed. BDD does not have a formal board of directors; management consists of the managing director and one additional manager	**No exceptions noted.**
	Additional point of focus when using the trust services criteria:			
	Supplements Board Expertise—The board of directors supplements its expertise relevant to Security, Availability and Confidentiality , and privacy, as needed,	BDD does not have a formal board of directors; management consists of the managing director and one additional manager. Oversight of the ISMS is exercised through compensating	URS verified the process description and evidence identified in the POA mapped to CC1.2 and assessed the specific requirement that the board of	**No exceptions noted.**

	through the use of a subcommittee or consultants.	structures appropriate to the company's size: the Cybersecurity Manager (CSM) is responsible for the day-to-day design and operation of the ISMS, while independent oversight of the ISMS itself is provided by an externally sourced, independent Auditor of Cybersecurity, who is organizationally separate from the CSM and from IT operations and reports results directly to management. An external cybersecurity audit has already been performed, confirming that this oversight is not only defined but actively exercised. Security, availability, and confidentiality expertise is supplemented through external consultants as needed.	directors supplements its expertise relevant to Security, Availability and Confidentiality , and privacy, as needed, through the use of a subcommittee or consultants. Based on the POA description and the referenced evidence, URS concluded that bDD does not have a formal board of directors; management consists of the managing director and one additional manager. Security, availability, and confidentiality expertise is supplemented through external consultants as needed	
CC1.3	**COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.**			
	Considers All Structures of the Entity—Management and the board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives.	Roles and responsibilities for the ISMS are formally defined for the Cybersecurity Manager, IT Administrator, Cybersecurity Auditor, Asset Owners, and Users, with a RACI matrix clarifying accountability across ISMS activities. Reporting lines reflect the company's lean structure. Formal segregation of duties is applied where practical (for example, the Cybersecurity Manager role may not be combined with the Asset Owner role); where segregation is not practical,	URS examined the process description and evidence identified in the POA mapped to CC1.3 and assessed the specific requirement that management and the board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives. Based on the POA description	**No exceptions noted.**

		compensating controls such as management oversight and logging are applied.	and the referenced evidence, URS determined that roles and responsibilities for the ISMS are formally defined for the Cybersecurity Manager, IT Administrator, Cybersecurity Auditor, Asset Owners, and Users, with a RACI matrix clarifying accountability across ISMS activities. Reporting lines reflect the company's lean structure	
	Establishes Reporting Lines— Management designs and evaluates lines of reporting for each entity structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity.	Roles and responsibilities for the ISMS are formally defined for the Cybersecurity Manager, IT Administrator, Cybersecurity Auditor, Asset Owners, and Users, with a RACI matrix clarifying accountability across ISMS activities. Reporting lines reflect the company's lean structure. Formal segregation of duties is applied where practical (for example, the Cybersecurity Manager role may not be combined with the Asset Owner role); where segregation is not practical, compensating controls such as management oversight and logging are applied.	URS reviewed the governing procedures and referenced evidence mapped to CC1.3 and assessed the specific requirement that management designs and evaluates lines of reporting for each entity structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity. Based on the POA description and the referenced evidence, URS confirmed that reporting lines reflect the company's lean structure. Roles and responsibilities for the ISMS are formally defined for the Cybersecurity Manager, IT Administrator, Cybersecurity Auditor, Asset Owners, and	**No exceptions noted.**

			Users, with a RACI matrix clarifying accountability across ISMS activities	
	Defines, Assigns, and Limits Authorities and Responsibilities—Management and the board of directors' delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization.	Roles and responsibilities for the ISMS are formally defined for the Cybersecurity Manager, IT Administrator, Cybersecurity Auditor, Asset Owners, and Users, with a RACI matrix clarifying accountability across ISMS activities. Reporting lines reflect the company's lean structure. Formal segregation of duties is applied where practical (for example, the Cybersecurity Manager role may not be combined with the Asset Owner role); where segregation is not practical, compensating controls such as management oversight and logging are applied.	URS assessed the governing procedures and referenced evidence mapped to CC1.3 and assessed the specific requirement that management and the board of directors' delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization. Based on the POA description and the referenced evidence, URS found that roles and responsibilities for the ISMS are formally defined for the Cybersecurity Manager, IT Administrator, Cybersecurity Auditor, Asset Owners, and Users, with a RACI matrix clarifying accountability across ISMS activities. Reporting lines reflect the company's lean structure	**No exceptions noted.**
	Additional point of focus when using the trust services criteria:			
	Addresses Specific Requirements When Defining Authorities and Responsibilities—Management and the	Roles and responsibilities for the ISMS are formally defined for the Cybersecurity Manager, IT	URS verified the process description and evidence identified in the POA mapped to	**No exceptions noted.**

	board of directors consider requirements relevant to Security, Availability and Confidentiality , and privacy when defining authorities and responsibilities.	Administrator, Cybersecurity Auditor, Asset Owners, and Users, with a RACI matrix clarifying accountability across ISMS activities. Reporting lines reflect the company's lean structure. Formal segregation of duties is applied where practical (for example, the Cybersecurity Manager role may not be combined with the Asset Owner role); where segregation is not practical, compensating controls such as management oversight and logging are applied.	CC1.3 and assessed the specific requirement that management and the board of directors consider requirements relevant to Security, Availability and Confidentiality , and privacy when defining authorities and responsibilities. Based on the POA description and the referenced evidence, URS verified that roles and responsibilities for the ISMS are formally defined for the Cybersecurity Manager, IT Administrator, Cybersecurity Auditor, Asset Owners, and Users, with a RACI matrix clarifying accountability across ISMS activities. Reporting lines reflect the company's lean structure	
	Considers Interactions with External Parties When Establishing Structures, Reporting Lines, Authorities, and Responsibilities—Management and the board of directors consider the need for the entity to interact with and monitor the activities of external parties when establishing structures, reporting lines, authorities, and responsibilities.	Roles and responsibilities for the ISMS are formally defined for the Cybersecurity Manager, IT Administrator, Cybersecurity Auditor, Asset Owners, and Users, with a RACI matrix clarifying accountability across ISMS activities. Reporting lines reflect the company's lean structure. Formal segregation of duties is applied where practical (for example, the Cybersecurity Manager role may not be combined with the Asset Owner role);	URS examined the process description and evidence identified in the POA mapped to CC1.3 and assessed the specific requirement that management and the board of directors consider the need for the entity to interact with and monitor the activities of external parties when establishing structures, reporting lines, authorities, and responsibilities. Based on the	**No exceptions noted.**

		where segregation is not practical, compensating controls such as management oversight and logging are applied.	POA description and the referenced evidence, URS concluded that reporting lines reflect the company's lean structure. Roles and responsibilities for the ISMS are formally defined for the Cybersecurity Manager, IT Administrator, Cybersecurity Auditor, Asset Owners, and Users, with a RACI matrix clarifying accountability across ISMS activities	
CC1.4	**COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.**			
	Establishes Policies and Practices—Policies and practices reflect expectations of competence necessary to support the achievement of objectives.	Background screening, reference checks, and role-specific competence checks are performed before hiring, proportionate to the sensitivity of the role and access involved (1.02, 1.07). The Cybersecurity Manager and IT Administrator each have a formally appointed deputy to ensure continuity of competence-critical roles. Security training has already taken place, and regular refresher training (every 2 years for all staff; annually for management, administrators, and security-role holders) is scheduled going forward.	URS reviewed the governing procedures and referenced evidence mapped to CC1.4 and assessed the specific requirement that policies and practices reflect expectations of competence necessary to support the achievement of objectives. Based on the POA description and the referenced evidence, URS confirmed that background screening, reference checks, and role-specific competence checks are performed before hiring, proportionate to the sensitivity of the role and access involved (1.02, 1.07). The Cybersecurity	**No exceptions noted.**

			Manager and IT Administrator each have a formally appointed deputy to ensure continuity of competence-critical roles	
	Evaluates Competence and Addresses Shortcomings—The board of directors and management evaluate competence across the entity and in outsourced service providers in relation to established policies and practices and act as necessary to address shortcomings.	Background screening, reference checks, and role-specific competence checks are performed before hiring, proportionate to the sensitivity of the role and access involved (1.02, 1.07). The Cybersecurity Manager and IT Administrator each have a formally appointed deputy to ensure continuity of competence-critical roles. Security training has already taken place, and regular refresher training (every 2 years for all staff; annually for management, administrators, and security-role holders) is scheduled going forward.	URS inspected the relevant policies, technical arrangements, and retained evidence mapped to CC1.4 and assessed the specific requirement that the board of directors and management evaluate competence across the entity and in outsourced service providers in relation to established policies and practices and act as necessary to address shortcomings. Based on the POA description and the referenced evidence, URS found that background screening, reference checks, and role-specific competence checks are performed before hiring, proportionate to the sensitivity of the role and access involved (1.02, 1.07). The Cybersecurity Manager and IT Administrator each have a formally appointed deputy to ensure continuity of competence-critical roles	**No exceptions noted.**
	Attracts, Develops, and Retains Individuals—The entity provides the mentoring and training needed to attract,	Background screening, reference checks, and role-specific competence checks are performed before hiring,	URS examined the documented control design and supporting records mapped to CC1.4 and	**No exceptions noted.**

	develop, and retain sufficient and competent personnel and outsourced service providers to support the achievement of objectives.	proportionate to the sensitivity of the role and access involved (1.02, 1.07). The Cybersecurity Manager and IT Administrator each have a formally appointed deputy to ensure continuity of competence-critical roles. Security training has already taken place, and regular refresher training (every 2 years for all staff; annually for management, administrators, and security-role holders) is scheduled going forward.	assessed the specific requirement that the entity provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and outsourced service providers to support the achievement of objectives. Based on the POA description and the referenced evidence, URS confirmed that background screening, reference checks, and role-specific competence checks are performed before hiring, proportionate to the sensitivity of the role and access involved (1.02, 1.07). The Cybersecurity Manager and IT Administrator each have a formally appointed deputy to ensure continuity of competence-critical roles	
	Plans and Prepares for Succession—Senior management and the board of directors develop contingency plans for assignments of responsibility important for internal control.	Background screening, reference checks, and role-specific competence checks are performed before hiring, proportionate to the sensitivity of the role and access involved (1.02, 1.07). The Cybersecurity Manager and IT Administrator each have a formally appointed deputy to ensure continuity of competence-critical roles. Security training has already taken place, and regular refresher training (every 2 years	URS verified the governing procedures and referenced evidence mapped to CC1.4 and assessed the specific requirement that senior management and the board of directors develop contingency plans for assignments of responsibility important for internal control. Based on the POA description and the	**No exceptions noted.**

		for all staff; annually for management, administrators, and security-role holders) is scheduled going forward.	referenced evidence, URS concluded that background screening, reference checks, and role-specific competence checks are performed before hiring, proportionate to the sensitivity of the role and access involved (1.02, 1.07). The Cybersecurity Manager and IT Administrator each have a formally appointed deputy to ensure continuity of competence-critical roles	
	Additional points of focus when using the trust services criteria:			
	Considers the Background of Individuals—The entity considers the background of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.	Background screening, reference checks, and role-specific competence checks are performed before hiring, proportionate to the sensitivity of the role and access involved (1.02, 1.07). The Cybersecurity Manager and IT Administrator each have a formally appointed deputy to ensure continuity of competence-critical roles. Security training has already taken place, and regular refresher training (every 2 years for all staff; annually for management, administrators, and security-role holders) is scheduled going forward.	URS verified the process description and evidence identified in the POA mapped to CC1.4 and assessed the specific requirement that the entity considers the background of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals. Based on the POA description and the referenced evidence, URS verified that background screening, reference checks, and role-specific competence checks are performed before hiring, proportionate to the sensitivity of the role and access	**No exceptions noted.**

			involved (1.02, 1.07). The Cybersecurity Manager and IT Administrator each have a formally appointed deputy to ensure continuity of competence-critical roles	
	Considers the Technical Competency of Individuals—The entity considers the technical competency of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.	Background screening, reference checks, and role-specific competence checks are performed before hiring, proportionate to the sensitivity of the role and access involved (1.02, 1.07). The Cybersecurity Manager and IT Administrator each have a formally appointed deputy to ensure continuity of competence-critical roles. Security training has already taken place, and regular refresher training (every 2 years for all staff; annually for management, administrators, and security-role holders) is scheduled going forward.	URS inspected the control documentation, assigned responsibilities, and available records mapped to CC1.4 and assessed the specific requirement that the entity considers the technical competency of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals. Based on the POA description and the referenced evidence, URS determined that background screening, reference checks, and role-specific competence checks are performed before hiring, proportionate to the sensitivity of the role and access involved (1.02, 1.07). The Cybersecurity Manager and IT Administrator each have a formally appointed deputy to ensure continuity of competence-critical roles	**No exceptions noted.**

	Provides Training to Maintain Technical Competencies — The entity provides training programs, including continuing education and training, to ensure skill sets and technical competency of existing personnel, contractors, and vendor employees are developed and maintained.	Background screening, reference checks, and role-specific competence checks are performed before hiring, proportionate to the sensitivity of the role and access involved (1.02, 1.07). The Cybersecurity Manager and IT Administrator each have a formally appointed deputy to ensure continuity of competence-critical roles. Security training has already taken place, and regular refresher training (every 2 years for all staff; annually for management, administrators, and security-role holders) is scheduled going forward.	URS examined the relevant policies, technical arrangements, and retained evidence mapped to CC1.4 and assessed the specific requirement that the entity provides training programs, including continuing education and training, to ensure skill sets and technical competency of existing personnel, contractors, and vendor employees are developed and maintained. Based on the POA description and the referenced evidence, URS concluded that security training has already taken place, and regular refresher training (every 2 years for all staff; annually for management, administrators, and security-role holders) is scheduled going forward. Background screening, reference checks, and role-specific competence checks are performed before hiring, proportionate to the sensitivity of the role and access involved (1.02, 1.07	**No exceptions noted.**
CC1.5	**COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.**			
	Enforces Accountability Through Structures, Authorities, and Responsibilities—Management and the	Individuals are held accountable for internal control responsibilities through clearly defined roles (1.02), mandatory	URS reviewed the applicable policy requirements and implementation evidence	**No exceptions noted.**

	board of directors establish the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the entity and implement corrective action as necessary.	security training, and a disciplinary process for policy violations, including immediate revocation of access for serious violations (1.07). Compliance with policies is monitored by the Cybersecurity Manager, who initiates corrective action where needed. Given the size of the company, this accountability is enforced through direct oversight and defined roles rather than a formal performance-appraisal or incentive system.	mapped to CC1.5 and assessed the specific requirement that management and the board of directors establish the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the entity and implement corrective action as necessary. Based on the POA description and the referenced evidence, URS determined that individuals are held accountable for internal control responsibilities through clearly defined roles (1.02), mandatory security training, and a disciplinary process for policy violations, including immediate revocation of access for serious violations (1.07). Given the size of the company, this accountability is enforced through direct oversight and defined roles rather than a formal performance-appraisal or incentive system	
	Establishes Performance Measures, Incentives, and Rewards—Management and the board of directors establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity,	Individuals are held accountable for internal control responsibilities through clearly defined roles (1.02), mandatory security training, and a disciplinary process for policy violations, including immediate revocation of access for	URS verified the relevant policies, technical arrangements, and retained evidence mapped to CC1.5 and assessed the specific requirement that management	**No exceptions noted.**

	reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives.	serious violations (1.07). Compliance with policies is monitored by the Cybersecurity Manager, who initiates corrective action where needed. Given the size of the company, this accountability is enforced through direct oversight and defined roles rather than a formal performance-appraisal or incentive system.	and the board of directors establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives. Based on the POA description and the referenced evidence, URS determined that given the size of the company, this accountability is enforced through direct oversight and defined roles rather than a formal performance-appraisal or incentive system. Individuals are held accountable for internal control responsibilities through clearly defined roles (1.02), mandatory security training, and a disciplinary process for policy violations, including immediate revocation of access for serious violations	
	Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance—Management and the board of directors align incentives and rewards with the fulfillment of internal control	Individuals are held accountable for internal control responsibilities through clearly defined roles (1.02), mandatory security training, and a disciplinary process for policy violations, including	URS evaluated the documented control design and supporting records mapped to CC1.5 and assessed the specific requirement that management	**No exceptions noted.**

	responsibilities in the achievement of objectives.	immediate revocation of access for serious violations (1.07). Compliance with policies is monitored by the Cybersecurity Manager, who initiates corrective action where needed. Given the size of the company, this accountability is enforced through direct oversight and defined roles rather than a formal performance-appraisal or incentive system.	and the board of directors align incentives and rewards with the fulfillment of internal control responsibilities in the achievement of objectives. Based on the POA description and the referenced evidence, URS concluded that given the size of the company, this accountability is enforced through direct oversight and defined roles rather than a formal performance-appraisal or incentive system. Individuals are held accountable for internal control responsibilities through clearly defined roles (1.02), mandatory security training, and a disciplinary process for policy violations, including immediate revocation of access for serious violations	
	Considers Excessive Pressures—Management and the board of directors evaluate and adjust pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance.	Individuals are held accountable for internal control responsibilities through clearly defined roles (1.02), mandatory security training, and a disciplinary process for policy violations, including immediate revocation of access for serious violations (1.07). Compliance with policies is monitored by the Cybersecurity Manager, who initiates corrective action where needed. Given the size of the company, this	URS verified the relevant policies, technical arrangements, and retained evidence mapped to CC1.5 and assessed the specific requirement that management and the board of directors evaluate and adjust pressures associated with the achievement of objectives as they assign responsibilities,	**No exceptions noted.**

		accountability is enforced through direct oversight and defined roles rather than a formal performance-appraisal or incentive system.	develop performance measures, and evaluate performance. Based on the POA description and the referenced evidence, URS found that individuals are held accountable for internal control responsibilities through clearly defined roles (1.02), mandatory security training, and a disciplinary process for policy violations, including immediate revocation of access for serious violations (1.07). Compliance with policies is monitored by the Cybersecurity Manager, who initiates corrective action where needed	
	Evaluates Performance and Rewards or Disciplines Individuals—Management and the board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence, and provide rewards or exercise disciplinary action, as appropriate.	Individuals are held accountable for internal control responsibilities through clearly defined roles (1.02), mandatory security training, and a disciplinary process for policy violations, including immediate revocation of access for serious violations (1.07). Compliance with policies is monitored by the Cybersecurity Manager, who initiates corrective action where needed. Given the size of the company, this accountability is enforced through direct oversight and defined roles rather than a formal performance-appraisal or incentive system.	URS inspected the applicable policy requirements and implementation evidence mapped to CC1.5 and assessed the specific requirement that management and the board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence, and provide rewards or exercise disciplinary action, as appropriate. Based on the POA description and the referenced evidence, URS	**No exceptions noted.**

			concluded that individuals are held accountable for internal control responsibilities through clearly defined roles (1.02), mandatory security training, and a disciplinary process for policy violations, including immediate revocation of access for serious violations (1.07). Given the size of the company, this accountability is enforced through direct oversight and defined roles rather than a formal performance-appraisal or incentive system	

CC2.0 Communication and Information

Criteria		Controls Defined by Big Dig Data s.r.o.	Tests of Controls Performed by URS	Results of Tests
CC2.1	**COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.**			
	Identifies Information Requirements—A process is in place to identify the information required and expected to support the functioning of the other components of internal control and the achievement of the entity's objectives.	The company identifies, classifies, and maintains an inventory of information and IT assets, including assets held outside the company's direct physical control (e.g., cloud-hosted data, employee and freelancer devices). Information is classified into Public / Internal / Sensitive tiers based on confidentiality requirements, with customer personal data always classified as Sensitive. Asset and risk records are reviewed as part of the annual risk assessment and updated upon significant changes.	URS reviewed the control documentation, assigned responsibilities, and available records mapped to CC2.1 and assessed the specific requirement that a process is in place to identify the information required and expected to support the functioning of the other components of internal control and the achievement of the entity's objectives. Based on the POA description and the referenced evidence, URS verified that the company identifies, classifies, and maintains an inventory of information and IT assets, including assets held outside the company's direct physical control (e.g., cloud-hosted data, employee and freelancer devices). Information is classified into Public / Internal / Sensitive tiers based on confidentiality requirements, with customer personal data always classified as Sensitive	**No exceptions noted.**

	Captures Internal and External Sources of Data—Information systems capture internal and external sources of data.	The company identifies, classifies, and maintains an inventory of information and IT assets, including assets held outside the company's direct physical control (e.g., cloud-hosted data, employee and freelancer devices). Information is classified into Public / Internal / Sensitive tiers based on confidentiality requirements, with customer personal data always classified as Sensitive. Asset and risk records are reviewed as part of the annual risk assessment and updated upon significant changes.	URS evaluated the applicable policy requirements and implementation evidence mapped to CC2.1 and assessed the specific requirement that information systems capture internal and external sources of data. Based on the POA description and the referenced evidence, URS found that information is classified into Public / Internal / Sensitive tiers based on confidentiality requirements, with customer personal data always classified as Sensitive. The company identifies, classifies, and maintains an inventory of information and IT assets, including assets held outside the company's direct physical control (e.g., cloud-hosted data, employee and freelancer devices)	**No exceptions noted.**
	Processes Relevant Data Into Information— Information systems process and transform relevant data into information.	The company identifies, classifies, and maintains an inventory of information and IT assets, including assets held outside the company's direct physical control (e.g., cloud-hosted data, employee and freelancer devices). Information is classified into Public / Internal / Sensitive tiers based on confidentiality	URS inspected the process description and evidence identified in the POA mapped to CC2.1 and assessed the specific requirement that information systems process and transform relevant data into information. Based on the POA description and the referenced evidence, URS concluded that the company	**No exceptions noted.**

		requirements, with customer personal data always classified as Sensitive. Asset and risk records are reviewed as part of the annual risk assessment and updated upon significant changes.	identifies, classifies, and maintains an inventory of information and IT assets, including assets held outside the company's direct physical control (e.g., cloud-hosted data, employee and freelancer devices). Information is classified into Public / Internal / Sensitive tiers based on confidentiality requirements, with customer personal data always classified as Sensitive	
	Maintains Quality Throughout Processing—Information systems produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information is reviewed to assess its relevance in supporting the internal control components.	The company identifies, classifies, and maintains an inventory of information and IT assets, including assets held outside the company's direct physical control (e.g., cloud-hosted data, employee and freelancer devices). Information is classified into Public / Internal / Sensitive tiers based on confidentiality requirements, with customer personal data always classified as Sensitive. Asset and risk records are reviewed as part of the annual risk assessment and updated upon significant changes.	URS evaluated the governing procedures and referenced evidence mapped to CC2.1 and assessed the specific requirement that information systems produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information is reviewed to assess its relevance in supporting the internal control components. Based on the POA description and the referenced evidence, URS confirmed that the company identifies, classifies, and maintains an inventory of information and IT assets, including assets held outside the company's direct physical control (e.g., cloud-hosted data,	**No exceptions noted.**

			employee and freelancer devices). Information is classified into Public / Internal / Sensitive tiers based on confidentiality requirements, with customer personal data always classified as Sensitive	
	Additional points of focus when using the trust services criteria:			
	Documents Data Flow — The entity documents and uses internal and external information and data flows to support the design and operation of controls.	The company identifies, classifies, and maintains an inventory of information and IT assets, including assets held outside the company's direct physical control (e.g., cloud-hosted data, employee and freelancer devices). Information is classified into Public / Internal / Sensitive tiers based on confidentiality requirements, with customer personal data always classified as Sensitive. Asset and risk records are reviewed as part of the annual risk assessment and updated upon significant changes.	URS evaluated the relevant policies, technical arrangements, and retained evidence mapped to CC2.1 and assessed the specific requirement that the entity documents and uses internal and external information and data flows to support the design and operation of controls. Based on the POA description and the referenced evidence, URS found that the company identifies, classifies, and maintains an inventory of information and IT assets, including assets held outside the company's direct physical control (e.g., cloud-hosted data, employee and freelancer devices). Information is classified into Public / Internal / Sensitive tiers based on confidentiality requirements, with customer personal data always classified as Sensitive	**No exceptions noted.**

	Manages Assets — The entity identifies, documents, and maintains records of system components such as infrastructure, software, and other information assets. Information assets include physical endpoint devices and systems, virtual systems, data and data flows, external information systems, and organizational roles.	The company identifies, classifies, and maintains an inventory of information and IT assets, including assets held outside the company's direct physical control (e.g., cloud-hosted data, employee and freelancer devices). Information is classified into Public / Internal / Sensitive tiers based on confidentiality requirements, with customer personal data always classified as Sensitive. Asset and risk records are reviewed as part of the annual risk assessment and updated upon significant changes.	URS reviewed the process description and evidence identified in the POA mapped to CC2.1 and assessed the specific requirement that the entity identifies, documents, and maintains records of system components such as infrastructure, software, and other information assets. Information assets include physical endpoint devices and systems, virtual systems, data and data flows, external information systems, and organizational roles. Based on the POA description and the referenced evidence, URS established that the company identifies, classifies, and maintains an inventory of information and IT assets, including assets held outside the company's direct physical control (e.g., cloud-hosted data, employee and freelancer devices). Information is classified into Public / Internal / Sensitive tiers based on confidentiality requirements, with customer personal data always classified as Sensitive	**No exceptions noted.**
	Classifies Information — The entity classifies information by its	The company identifies, classifies, and maintains an inventory of	URS verified the control documentation, assigned	**No exceptions noted.**

	relevant characteristics (for example, personally identifiable information, confidential customer information, and intellectual property) to support identification of threats to the information and the design and operation of controls.	information and IT assets, including assets held outside the company's direct physical control (e.g., cloud-hosted data, employee and freelancer devices). Information is classified into Public / Internal / Sensitive tiers based on confidentiality requirements, with customer personal data always classified as Sensitive. Asset and risk records are reviewed as part of the annual risk assessment and updated upon significant changes.	responsibilities, and available records mapped to CC2.1 and assessed the specific requirement that the entity classifies information by its relevant characteristics (for example, personally identifiable information, confidential customer information, and intellectual property) to support identification of threats to the information and the design and operation of controls. Based on the POA description and the referenced evidence, URS established that the company identifies, classifies, and maintains an inventory of information and IT assets, including assets held outside the company's direct physical control (e.g., cloud-hosted data, employee and freelancer devices). Information is classified into Public / Internal / Sensitive tiers based on confidentiality requirements, with customer personal data always classified as Sensitive	
	Uses Information That Is Complete and Accurate — The entity uses information and reports that are complete,	The company identifies, classifies, and maintains an inventory of information and IT assets, including assets held outside the	URS inspected the applicable policy requirements and implementation evidence mapped to CC2.1 and assessed the	**No exceptions noted.**

	accurate, current, and valid in the operation of controls.	company's direct physical control (e.g., cloud-hosted data, employee and freelancer devices). Information is classified into Public / Internal / Sensitive tiers based on confidentiality requirements, with customer personal data always classified as Sensitive. Asset and risk records are reviewed as part of the annual risk assessment and updated upon significant changes.	specific requirement that the entity uses information and reports that are complete, accurate, current, and valid in the operation of controls. Based on the POA description and the referenced evidence, URS verified that the company identifies, classifies, and maintains an inventory of information and IT assets, including assets held outside the company's direct physical control (e.g., cloud-hosted data, employee and freelancer devices). Information is classified into Public / Internal / Sensitive tiers based on confidentiality requirements, with customer personal data always classified as Sensitive	
	Manages the Location of Assets — The entity identifies, documents, and maintains records of physical location and custody of information assets, particularly for those stored outside the physical security control of the entity (for example, software and data stored on vendor devices or employee mobile phones under a bring-yourown-device policy).	The company identifies, classifies, and maintains an inventory of information and IT assets, including assets held outside the company's direct physical control (e.g., cloud-hosted data, employee and freelancer devices). Information is classified into Public / Internal / Sensitive tiers based on confidentiality requirements, with customer personal data always classified as Sensitive. Asset and risk records	URS evaluated the documented control design and supporting records mapped to CC2.1 and assessed the specific requirement that the entity identifies, documents, and maintains records of physical location and custody of information assets, particularly for those stored outside the physical security control of the entity (for example, software and data stored on vendor devices or employee	**No exceptions noted.**

		are reviewed as part of the annual risk assessment and updated upon significant changes.	mobile phones under a bring-yourown-device policy). Based on the POA description and the referenced evidence, URS established that the company identifies, classifies, and maintains an inventory of information and IT assets, including assets held outside the company's direct physical control (e.g., cloud-hosted data, employee and freelancer devices). Information is classified into Public / Internal / Sensitive tiers based on confidentiality requirements, with customer personal data always classified as Sensitive	
CC2.2	**COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control**			
	Communicates Internal Control Information—A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.	Objectives, responsibilities, and policy changes are communicated internally through the ISMS documentation, onboarding, periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT department for reporting suspicious activity or incidents. The Code of Ethics (v1.0, effective 1 Jan 2026) commits to whistleblower protection under Act No. 171/2023 Coll. and directs	URS assessed the process description and evidence identified in the POA mapped to CC2.2 and assessed the specific requirement that a process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities. Based on the POA description and the referenced evidence, URS determined that mandates a dedicated internal	**No exceptions noted.**

		reports to a direct superior or to management. Given the size and structure of the team (four employees – the managing director, a developer, the Cybersecurity Manager, and one additional employee – plus eight freelance collaborators, one of whom holds a leadership role alongside the managing director), this provides a workable reporting path for the large majority of cases, including concerns about the managing director, which can be directed to the other leader. VDD is also below the statutory headcount threshold (50 employees) at which Act No. 171/2023 Coll. mandates a dedicated internal reporting channel.	reporting channel. Objectives, responsibilities, and policy changes are communicated internally through the ISMS documentation, onboarding, periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT department for reporting suspicious activity or incidents	
	Communicates with the Board of Directors—Communication exists between management and the board of directors so that both have information needed to fulfill their roles with respect to the entity's objectives.	Objectives, responsibilities, and policy changes are communicated internally through the ISMS documentation, onboarding, periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT department for reporting suspicious activity or incidents. The Code of Ethics (v1.0, effective 1 Jan 2026) commits to whistleblower protection under	URS assessed the process description and evidence identified in the POA mapped to CC2.2 and assessed the specific requirement that communication exists between management and the board of directors so that both have information needed to fulfill their roles with respect to the entity's objectives. Based on the POA description and the referenced evidence, URS verified	**No exceptions noted.**

		Act No. 171/2023 Coll. and directs reports to a direct superior or to management. Given the size and structure of the team (four employees – the managing director, a developer, the Cybersecurity Manager, and one additional employee – plus eight freelance collaborators, one of whom holds a leadership role alongside the managing director), this provides a workable reporting path for the large majority of cases, including concerns about the managing director, which can be directed to the other leader. VDD is also below the statutory headcount threshold (50 employees) at which Act No. 171/2023 Coll. mandates a dedicated internal reporting channel.	that objectives, responsibilities, and policy changes are communicated internally through the ISMS documentation, onboarding, periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT department for reporting suspicious activity or incidents. The Code of Ethics (v1.0, effective 1 Jan 2026) commits to whistleblower protection under Act No.	
	Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.	Objectives, responsibilities, and policy changes are communicated internally through the ISMS documentation, onboarding, periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT department for reporting suspicious activity or incidents. The Code of Ethics (v1.0, effective 1 Jan 2026) commits to	URS assessed the applicable policy requirements and implementation evidence mapped to CC2.2 and assessed the specific requirement that separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal	**No exceptions noted.**

		whistleblower protection under Act No. 171/2023 Coll. and directs reports to a direct superior or to management. Given the size and structure of the team (four employees – the managing director, a developer, the Cybersecurity Manager, and one additional employee – plus eight freelance collaborators, one of whom holds a leadership role alongside the managing director), this provides a workable reporting path for the large majority of cases, including concerns about the managing director, which can be directed to the other leader. VDD is also below the statutory headcount threshold (50 employees) at which Act No. 171/2023 Coll. mandates a dedicated internal reporting channel.	channels are inoperative or ineffective. Based on the POA description and the referenced evidence, URS found that given the size and structure of the team (four employees – the managing director, a developer, the Cybersecurity Manager, and one additional employee – plus eight freelance collaborators, one of whom holds a leadership role alongside the managing director), this provides a workable reporting path for the large majority of cases, including concerns about the managing director, which can be directed to the other leader. Objectives, responsibilities, and policy changes are communicated internally through the ISMS documentation, onboarding, periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT department for reporting suspicious activity or incidents	
	Selects Relevant Method of Communication — The method of communication considers the timing, audience, and nature of the information.	Objectives, responsibilities, and policy changes are communicated internally through the ISMS documentation, onboarding, periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT	URS evaluated the applicable policy requirements and implementation evidence mapped to CC2.2 and assessed the specific requirement that the method of communication considers the timing, audience,	**No exceptions noted.**

		department for reporting suspicious activity or incidents. The Code of Ethics (v1.0, effective 1 Jan 2026) commits to whistleblower protection under Act No. 171/2023 Coll. and directs reports to a direct superior or to management. Given the size and structure of the team (four employees – the managing director, a developer, the Cybersecurity Manager, and one additional employee – plus eight freelance collaborators, one of whom holds a leadership role alongside the managing director), this provides a workable reporting path for the large majority of cases, including concerns about the managing director, which can be directed to the other leader. VDD is also below the statutory headcount threshold (50 employees) at which Act No. 171/2023 Coll. mandates a dedicated internal reporting channel.	and nature of the information. Based on the POA description and the referenced evidence, URS established that objectives, responsibilities, and policy changes are communicated internally through the ISMS documentation, onboarding, periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT department for reporting suspicious activity or incidents. The Code of Ethics (v1.0, effective 1 Jan 2026) commits to whistleblower protection under Act No.	
	<u>Additional points of focus when using the trust services criteria:</u>			
	<u>Communicates Responsibilities</u>—Entity personnel with responsibility for designing, developing, implementing, operating, maintaining, or	Objectives, responsibilities, and policy changes are communicated internally through the ISMS documentation, onboarding, periodic e-learning, and direct	URS examined the documented control design and supporting records mapped to CC2.2 and assessed the specific requirement that entity personnel with	**No exceptions noted.**

	monitoring system controls receive communications about their responsibilities, including changes in their responsibilities, and have the information necessary to carry out those responsibilities.	channels (email, Google Chat) to the Cybersecurity Manager or IT department for reporting suspicious activity or incidents. The Code of Ethics (v1.0, effective 1 Jan 2026) commits to whistleblower protection under Act No. 171/2023 Coll. and directs reports to a direct superior or to management. Given the size and structure of the team (four employees – the managing director, a developer, the Cybersecurity Manager, and one additional employee – plus eight freelance collaborators, one of whom holds a leadership role alongside the managing director), this provides a workable reporting path for the large majority of cases, including concerns about the managing director, which can be directed to the other leader. VDD is also below the statutory headcount threshold (50 employees) at which Act No. 171/2023 Coll. mandates a dedicated internal reporting channel.	responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls receive communications about their responsibilities, including changes in their responsibilities, and have the information necessary to carry out those responsibilities. Based on the POA description and the referenced evidence, URS verified that objectives, responsibilities, and policy changes are communicated internally through the ISMS documentation, onboarding, periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT department for reporting suspicious activity or incidents. The Code of Ethics (v1.0, effective 1 Jan 2026) commits to whistleblower protection under Act No.	
	Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters—Entity personnel are provided with	Objectives, responsibilities, and policy changes are communicated internally through the ISMS documentation, onboarding,	URS evaluated the applicable policy requirements and implementation evidence mapped to CC2.2 and assessed the	**No exceptions noted.**

	information on how to report systems failures, incidents, concerns, and other complaints to personnel.	periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT department for reporting suspicious activity or incidents. The Code of Ethics (v1.0, effective 1 Jan 2026) commits to whistleblower protection under Act No. 171/2023 Coll. and directs reports to a direct superior or to management. Given the size and structure of the team (four employees – the managing director, a developer, the Cybersecurity Manager, and one additional employee – plus eight freelance collaborators, one of whom holds a leadership role alongside the managing director), this provides a workable reporting path for the large majority of cases, including concerns about the managing director, which can be directed to the other leader. VDD is also below the statutory headcount threshold (50 employees) at which Act No. 171/2023 Coll. mandates a dedicated internal reporting channel.	specific requirement that entity personnel are provided with information on how to report systems failures, incidents, concerns, and other complaints to personnel. Based on the POA description and the referenced evidence, URS found that given the size and structure of the team (four employees – the managing director, a developer, the Cybersecurity Manager, and one additional employee – plus eight freelance collaborators, one of whom holds a leadership role alongside the managing director), this provides a workable reporting path for the large majority of cases, including concerns about the managing director, which can be directed to the other leader. Objectives, responsibilities, and policy changes are communicated internally through the ISMS documentation, onboarding, periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT department for reporting suspicious activity or incidents.	
	Communicates Objectives and Changes to Objectives —The entity communicates its	Objectives, responsibilities, and policy changes are communicated internally through the ISMS	URS evaluated the governing procedures and referenced evidence mapped to CC2.2 and	**No exceptions noted.**

	objectives and changes to those objectives to personnel in a timely manner.	documentation, onboarding, periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT department for reporting suspicious activity or incidents. The Code of Ethics (v1.0, effective 1 Jan 2026) commits to whistleblower protection under Act No. 171/2023 Coll. and directs reports to a direct superior or to management. Given the size and structure of the team (four employees – the managing director, a developer, the Cybersecurity Manager, and one additional employee – plus eight freelance collaborators, one of whom holds a leadership role alongside the managing director), this provides a workable reporting path for the large majority of cases, including concerns about the managing director, which can be directed to the other leader. VDD is also below the statutory headcount threshold (50 employees) at which Act No. 171/2023 Coll. mandates a dedicated internal reporting channel.	assessed the specific requirement that the entity communicates its objectives and changes to those objectives to personnel in a timely manner. Based on the POA description and the referenced evidence, URS verified that objectives, responsibilities, and policy changes are communicated internally through the ISMS documentation, onboarding, periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT department for reporting suspicious activity or incidents. The Code of Ethics (v1.0, effective 1 Jan 2026) commits to whistleblower protection under Act No.	
	Communicates Information About System Operation and	Objectives, responsibilities, and policy changes are communicated	URS inspected the relevant policies, technical arrangements,	**No exceptions noted.**

	Boundaries—The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized personnel to enable them to understand their role in the system and the results of system operation.	internally through the ISMS documentation, onboarding, periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT department for reporting suspicious activity or incidents. The Code of Ethics (v1.0, effective 1 Jan 2026) commits to whistleblower protection under Act No. 171/2023 Coll. and directs reports to a direct superior or to management. Given the size and structure of the team (four employees – the managing director, a developer, the Cybersecurity Manager, and one additional employee – plus eight freelance collaborators, one of whom holds a leadership role alongside the managing director), this provides a workable reporting path for the large majority of cases, including concerns about the managing director, which can be directed to the other leader. VDD is also below the statutory headcount threshold (50 employees) at which Act No. 171/2023 Coll. mandates a dedicated internal reporting channel.	and retained evidence mapped to CC2.2 and assessed the specific requirement that the entity prepares and communicates information about the design and operation of the system and its boundaries to authorized personnel to enable them to understand their role in the system and the results of system operation. Based on the POA description and the referenced evidence, URS found that given the size and structure of the team (four employees – the managing director, a developer, the Cybersecurity Manager, and one additional employee – plus eight freelance collaborators, one of whom holds a leadership role alongside the managing director), this provides a workable reporting path for the large majority of cases, including concerns about the managing director, which can be directed to the other leader. Objectives, responsibilities, and policy changes are communicated internally through the ISMS documentation, onboarding, periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT	

			department for reporting suspicious activity or incidents.	
	Communicates Information to Improve Security Knowledge and Awareness—The entity communicates information to improve security knowledge and awareness and to model appropriate security behaviors to personnel through a security awareness training program.	Objectives, responsibilities, and policy changes are communicated internally through the ISMS documentation, onboarding, periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT department for reporting suspicious activity or incidents. The Code of Ethics (v1.0, effective 1 Jan 2026) commits to whistleblower protection under Act No. 171/2023 Coll. and directs reports to a direct superior or to management. Given the size and structure of the team (four employees – the managing director, a developer, the Cybersecurity Manager, and one additional employee – plus eight freelance collaborators, one of whom holds a leadership role alongside the managing director), this provides a workable reporting path for the large majority of cases, including concerns about the managing director, which can be directed to the other leader. VDD is also below the statutory headcount threshold (50 employees) at which Act No.	URS examined the documented control design and supporting records mapped to CC2.2 and assessed the specific requirement that the entity communicates information to improve security knowledge and awareness and to model appropriate security behaviors to personnel through a security awareness training program. Based on the POA description and the referenced evidence, URS concluded that objectives, responsibilities, and policy changes are communicated internally through the ISMS documentation, onboarding, periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT department for reporting suspicious activity or incidents. The Code of Ethics (v1.0, effective 1 Jan 2026) commits to whistleblower protection under Act No.	**No exceptions noted.**

		171/2023 Coll. mandates a dedicated internal reporting channel.		
	Additional points of focus when using the trust services criteria at the system level:			
	Communicates System Objectives—The entity communicates its objectives to personnel to enable them to carry out their responsibilities.	Objectives, responsibilities, and policy changes are communicated internally through the ISMS documentation, onboarding, periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT department for reporting suspicious activity or incidents. The Code of Ethics (v1.0, effective 1 Jan 2026) commits to whistleblower protection under Act No. 171/2023 Coll. and directs reports to a direct superior or to management. Given the size and structure of the team (four employees – the managing director, a developer, the Cybersecurity Manager, and one additional employee – plus eight freelance collaborators, one of whom holds a leadership role alongside the managing director), this provides a workable reporting path for the large majority of cases, including concerns about the managing director, which can be directed to the other leader. VDD is also below the statutory	URS evaluated the relevant policies, technical arrangements, and retained evidence mapped to CC2.2 and assessed the specific requirement that the entity communicates its objectives to personnel to enable them to carry out their responsibilities. Based on the POA description and the referenced evidence, URS confirmed that objectives, responsibilities, and policy changes are communicated internally through the ISMS documentation, onboarding, periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT department for reporting suspicious activity or incidents. The Code of Ethics (v1.0, effective 1 Jan 2026) commits to whistleblower protection under Act No.	**No exceptions noted.**

		headcount threshold (50 employees) at which Act No. 171/2023 Coll. mandates a dedicated internal reporting channel.		
	Communicates System Changes—System changes that affect responsibilities or the achievement of the entity's objectives are communicated in a timely manner.	Objectives, responsibilities, and policy changes are communicated internally through the ISMS documentation, onboarding, periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT department for reporting suspicious activity or incidents. The Code of Ethics (v1.0, effective 1 Jan 2026) commits to whistleblower protection under Act No. 171/2023 Coll. and directs reports to a direct superior or to management. Given the size and structure of the team (four employees – the managing director, a developer, the Cybersecurity Manager, and one additional employee – plus eight freelance collaborators, one of whom holds a leadership role alongside the managing director), this provides a workable reporting path for the large majority of cases, including concerns about the managing director, which can be directed to the other leader.	URS examined the relevant policies, technical arrangements, and retained evidence mapped to CC2.2 and assessed the specific requirement that system changes that affect responsibilities or the achievement of the entity's objectives are communicated in a timely manner. Based on the POA description and the referenced evidence, URS determined that objectives, responsibilities, and policy changes are communicated internally through the ISMS documentation, onboarding, periodic e-learning, and direct channels (email, Google Chat) to the Cybersecurity Manager or IT department for reporting suspicious activity or incidents. The Code of Ethics (v1.0, effective 1 Jan 2026) commits to whistleblower protection under Act No.	**No exceptions noted.**

		VDD is also below the statutory headcount threshold (50 employees) at which Act No. 171/2023 Coll. mandates a dedicated internal reporting channel.		
CC2.3	**COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.**			
	Communicates to External Parties—Processes are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties.	External communication of incidents and security/confidentiality-relevant matters is addressed contractually with customers and suppliers and operationally through the Incident Response Plan, which defines notification duties toward affected customers and, where required, the Czech Data Protection Authority within 72 hours. A published Privacy Policy provides external parties with information on data handling and how to raise concerns or exercise their rights.	URS evaluated the governing procedures and referenced evidence mapped to CC2.3 and assessed the specific requirement that processes are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties. Based on the POA description and the referenced evidence, URS found that a published Privacy Policy provides external parties with information on data handling and how to raise concerns or exercise their rights. External communication of incidents and security/confidentiality-relevant matters is addressed contractually with customers and suppliers and operationally through the Incident Response Plan, which defines notification duties toward affected customers	**No exceptions noted.**

			and, where required, the Czech Data Protection Authority within 72 hours	
	Enables Inbound Communications—Open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing management and the board of directors with relevant information.	External communication of incidents and security/confidentiality-relevant matters is addressed contractually with customers and suppliers and operationally through the Incident Response Plan, which defines notification duties toward affected customers and, where required, the Czech Data Protection Authority within 72 hours. A published Privacy Policy provides external parties with information on data handling and how to raise concerns or exercise their rights.	URS verified the process description and evidence identified in the POA mapped to CC2.3 and assessed the specific requirement that open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing management and the board of directors with relevant information. Based on the POA description and the referenced evidence, URS determined that external communication of incidents and security/confidentiality-relevant matters is addressed contractually with customers and suppliers and operationally through the Incident Response Plan, which defines notification duties toward affected customers and, where required, the Czech Data Protection Authority within 72 hours. A published Privacy Policy provides external parties with information on data handling	**No exceptions noted.**

			and how to raise concerns or exercise their rights	
	Communicates with the Board of Directors—Relevant information resulting from assessments conducted by external parties is communicated to the board of directors.	External communication of incidents and security/confidentiality-relevant matters is addressed contractually with customers and suppliers and operationally through the Incident Response Plan, which defines notification duties toward affected customers and, where required, the Czech Data Protection Authority within 72 hours. A published Privacy Policy provides external parties with information on data handling and how to raise concerns or exercise their rights.	URS verified the applicable policy requirements and implementation evidence mapped to CC2.3 and assessed the specific requirement that relevant information resulting from assessments conducted by external parties is communicated to the board of directors. Based on the POA description and the referenced evidence, URS concluded that external communication of incidents and security/confidentiality-relevant matters is addressed contractually with customers and suppliers and operationally through the Incident Response Plan, which defines notification duties toward affected customers and, where required, the Czech Data Protection Authority within 72 hours. A published Privacy Policy provides external parties with information on data handling and how to raise concerns or exercise their rights	**No exceptions noted.**
	Provides Separate Communication Lines— Separate communication channels, such as whistleblower hotlines, are in place and serve as fail-safe	External communication of incidents and security/confidentiality-relevant matters is addressed contractually with customers and	URS evaluated the process description and evidence identified in the POA mapped to CC2.3 and assessed the specific requirement that separate	**No exceptions noted.**

	mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.	suppliers and operationally through the Incident Response Plan, which defines notification duties toward affected customers and, where required, the Czech Data Protection Authority within 72 hours. A published Privacy Policy provides external parties with information on data handling and how to raise concerns or exercise their rights.	communication channels, such as whistleblower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective. Based on the POA description and the referenced evidence, URS found that external communication of incidents and security/confidentiality-relevant matters is addressed contractually with customers and suppliers and operationally through the Incident Response Plan, which defines notification duties toward affected customers and, where required, the Czech Data Protection Authority within 72 hours. A published Privacy Policy provides external parties with information on data handling and how to raise concerns or exercise their rights	
	Selects Relevant Method of Communication—The method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations.	External communication of incidents and security/confidentiality-relevant matters is addressed contractually with customers and suppliers and operationally through the Incident Response Plan, which defines notification	URS examined the control documentation, assigned responsibilities, and available records mapped to CC2.3 and assessed the specific requirement that the method of communication considers the timing, audience, and nature of	**No exceptions noted.**

		duties toward affected customers and, where required, the Czech Data Protection Authority within 72 hours. A published Privacy Policy provides external parties with information on data handling and how to raise concerns or exercise their rights.	the communication and legal, regulatory, and fiduciary requirements and expectations. Based on the POA description and the referenced evidence, URS confirmed that external communication of incidents and security/confidentiality-relevant matters is addressed contractually with customers and suppliers and operationally through the Incident Response Plan, which defines notification duties toward affected customers and, where required, the Czech Data Protection Authority within 72 hours. A published Privacy Policy provides external parties with information on data handling and how to raise concerns or exercise their rights	
	Additional point of focus when using the trust services criteria for confidentiality:			
	Communicates Objectives Related to Confidentiality and Changes to Those Objectives — The entity communicates, to external users, vendors, business partners, and others whose products or services, or both, are part of the system, the entity's objectives related to confidentiality and the protection	External communication of incidents and security/confidentiality-relevant matters is addressed contractually with customers and suppliers and operationally through the Incident Response Plan, which defines notification duties toward affected customers and, where required, the Czech Data Protection Authority within	URS inspected the relevant policies, technical arrangements, and retained evidence mapped to CC2.3 and assessed the specific requirement that the entity communicates, to external users, vendors, business partners, and others whose products or services, or both, are part of the system, the entity's objectives related to confidentiality and the	**No exceptions noted.**

	of confidential information, as well as changes to those objectives.	72 hours. A published Privacy Policy provides external parties with information on data handling and how to raise concerns or exercise their rights.	protection of confidential information, as well as changes to those objectives. Based on the POA description and the referenced evidence, URS verified that external communication of incidents and security/confidentiality-relevant matters is addressed contractually with customers and suppliers and operationally through the Incident Response Plan, which defines notification duties toward affected customers and, where required, the Czech Data Protection Authority within 72 hours. A published Privacy Policy provides external parties with information on data handling and how to raise concerns or exercise their rights	
	Additional points of focus when using the trust services criteria at the system level:			
	Communicates Information About System Operation and Boundaries—The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized external users to permit users to understand their role in the system and the results of system operation.	External communication of incidents and security/confidentiality-relevant matters is addressed contractually with customers and suppliers and operationally through the Incident Response Plan, which defines notification duties toward affected customers and, where required, the Czech Data Protection Authority within	URS assessed the process description and evidence identified in the POA mapped to CC2.3 and assessed the specific requirement that the entity prepares and communicates information about the design and operation of the system and its boundaries to authorized external users to permit users to understand their role in the	**No exceptions noted.**

		72 hours. A published Privacy Policy provides external parties with information on data handling and how to raise concerns or exercise their rights.	system and the results of system operation. Based on the POA description and the referenced evidence, URS verified that a published Privacy Policy provides external parties with information on data handling and how to raise concerns or exercise their rights. External communication of incidents and security/confidentiality-relevant matters is addressed contractually with customers and suppliers and operationally through the Incident Response Plan, which defines notification duties toward affected customers and, where required, the Czech Data Protection Authority within 72 hours	
	Communicates System Objectives—The entity communicates its system objectives to appropriate external users.	External communication of incidents and security/confidentiality-relevant matters is addressed contractually with customers and suppliers and operationally through the Incident Response Plan, which defines notification duties toward affected customers and, where required, the Czech Data Protection Authority within 72 hours. A published Privacy Policy provides external parties	URS reviewed the control documentation, assigned responsibilities, and available records mapped to CC2.3 and assessed the specific requirement that the entity communicates its system objectives to appropriate external users. Based on the POA description and the referenced evidence, URS concluded that external communication of incidents and security/confidentiality-relevant	**No exceptions noted.**

		with information on data handling and how to raise concerns or exercise their rights.	matters is addressed contractually with customers and suppliers and operationally through the Incident Response Plan, which defines notification duties toward affected customers and, where required, the Czech Data Protection Authority within 72 hours. A published Privacy Policy provides external parties with information on data handling and how to raise concerns or exercise their rights	
	Communicates System Responsibilities — External users with responsibility for designing, developing, implementing, operating, maintaining, and monitoring system controls receive information about such responsibilities and have the information necessary to carry out such responsibilities.	External communication of incidents and security/confidentiality-relevant matters is addressed contractually with customers and suppliers and operationally through the Incident Response Plan, which defines notification duties toward affected customers and, where required, the Czech Data Protection Authority within 72 hours. A published Privacy Policy provides external parties with information on data handling and how to raise concerns or exercise their rights.	URS reviewed the relevant policies, technical arrangements, and retained evidence mapped to CC2.3 and assessed the specific requirement that external users with responsibility for designing, developing, implementing, operating, maintaining, and monitoring system controls receive information about such responsibilities and have the information necessary to carry out such responsibilities. Based on the POA description and the referenced evidence, URS concluded that external communication of incidents and security/confidentiality-relevant matters is addressed contractually with customers and	**No exceptions noted.**

			suppliers and operationally through the Incident Response Plan, which defines notification duties toward affected customers and, where required, the Czech Data Protection Authority within 72 hours. A published Privacy Policy provides external parties with information on data handling and how to raise concerns or exercise their rights	
	Communicates Information on Reporting System Failures, Incidents, Concerns, and Other Matters — External users are provided with information on how to report systems failures, incidents, concerns, and other complaints to appropriate entity personnel.	External communication of incidents and security/confidentiality-relevant matters is addressed contractually with customers and suppliers and operationally through the Incident Response Plan, which defines notification duties toward affected customers and, where required, the Czech Data Protection Authority within 72 hours. A published Privacy Policy provides external parties with information on data handling and how to raise concerns or exercise their rights.	URS verified the control documentation, assigned responsibilities, and available records mapped to CC2.3 and assessed the specific requirement that external users are provided with information on how to report systems failures, incidents, concerns, and other complaints to appropriate entity personnel. Based on the POA description and the referenced evidence, URS found that external communication of incidents and security/confidentiality-relevant matters is addressed contractually with customers and suppliers and operationally through the Incident Response Plan, which defines notification duties toward affected customers and, where required, the Czech	**No exceptions noted.**

			Data Protection Authority within 72 hours. A published Privacy Policy provides external parties with information on data handling and how to raise concerns or exercise their rights	

CC3.0 Risk assessment

Criteria		Controls Defined by Big Dig Data s.r.o.	Tests of Controls Performed by URS	Results of Tests
CC3.1	**COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.**			
	Operations Objectives			
	Reflects Management's Choices—Operations objectives reflect management's choices about structure, industry considerations, and performance of the entity.	The Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	URS assessed the documented control design and supporting records mapped to CC3.1 and assessed the specific requirement that operations objectives reflect management's choices about structure, industry considerations, and performance of the entity. Based on the POA description and the referenced evidence, URS established that the Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process	**No exceptions noted.**

	Considers Tolerances for Risk— Management considers the acceptable levels of variation relative to the achievement of operations objectives.	The Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	URS assessed the control documentation, assigned responsibilities, and available records mapped to CC3.1 and assessed the specific requirement that management considers the acceptable levels of variation relative to the achievement of operations objectives. Based on the POA description and the referenced evidence, URS established that the Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	**No exceptions noted.**
	Includes Operations and Financial Performance Goals— The organization reflects the desired level of operations and financial performance for the entity within operations objectives.	The Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to	URS assessed the process description and evidence identified in the POA mapped to CC3.1 and assessed the specific requirement that the organization reflects the desired level of operations and financial	**No exceptions noted.**

		make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	performance for the entity within operations objectives. Based on the POA description and the referenced evidence, URS determined that the Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	
	Forms a Basis for Committing of Resources—Management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance.	The Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	URS reviewed the process description and evidence identified in the POA mapped to CC3.1 and assessed the specific requirement that management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance. Based on the POA description and the referenced evidence, URS confirmed that the Cybersecurity Manager provides management with accurate and	**No exceptions noted.**

			complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	
	External Financial Reporting Objectives			
	Complies with Applicable Accounting Standards—Financial reporting objectives are consistent with accounting principles suitable and available for that entity. The accounting principles selected are appropriate in the circumstances.	The Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	URS evaluated the governing procedures and referenced evidence mapped to CC3.1 and assessed the specific requirement that financial reporting objectives are consistent with accounting principles suitable and available for that entity. The accounting principles selected are appropriate in the circumstances. Based on the POA description and the referenced evidence, URS determined that the Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on	**No exceptions noted.**

			security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	
	Considers Materiality—Management considers materiality in financial statement presentation.	The Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	URS reviewed the documented control design and supporting records mapped to CC3.1 and assessed the specific requirement that management considers materiality in financial statement presentation. Based on the POA description and the referenced evidence, URS established that the Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	**No exceptions noted.**

	Reflects Entity Activities—External reporting reflects the underlying transactions and events to show qualitative characteristics and assertions.	The Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	URS inspected the control documentation, assigned responsibilities, and available records mapped to CC3.1 and assessed the specific requirement that external reporting reflects the underlying transactions and events to show qualitative characteristics and assertions. Based on the POA description and the referenced evidence, URS determined that the Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	**No exceptions noted.**
	External Nonfinancial Reporting Objectives			
	Complies with Externally Established Frameworks—Management establishes objectives consistent with laws and regulations or standards and	The Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment	URS reviewed the relevant policies, technical arrangements, and retained evidence mapped to CC3.1 and assessed the specific requirement that management establishes objectives consistent	**No exceptions noted.**

	frameworks of recognized external organizations.	reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	with laws and regulations or standards and frameworks of recognized external organizations. Based on the POA description and the referenced evidence, URS confirmed that the Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	
	Considers the Required Level of Precision—Management reflects the required level of precision and accuracy suitable for user needs and based on criteria established by third parties in nonfinancial reporting.	The Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and	URS evaluated the documented control design and supporting records mapped to CC3.1 and assessed the specific requirement that management reflects the required level of precision and accuracy suitable for user needs and based on criteria established by third parties in nonfinancial reporting. Based on the POA description and the referenced evidence, URS concluded that the Cybersecurity Manager provides	**No exceptions noted.**

		reviewed at least annually as part of this process.	management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	
	Reflects Entity Activities—External reporting reflects the underlying transactions and events within a range of acceptable limits.	The Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	URS verified the documented control design and supporting records mapped to CC3.1 and assessed the specific requirement that external reporting reflects the underlying transactions and events within a range of acceptable limits. Based on the POA description and the referenced evidence, URS confirmed that the Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment.	**No exceptions noted.**

			ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	
	Internal Reporting Objectives			
	Reflects Management's Choices—Internal reporting provides management with accurate and complete information regarding management's choices and information needed in managing the entity.	The Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	URS evaluated the process description and evidence identified in the POA mapped to CC3.1 and assessed the specific requirement that internal reporting provides management with accurate and complete information regarding management's choices and information needed in managing the entity. Based on the POA description and the referenced evidence, URS established that the Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and	**No exceptions noted.**

			reviewed at least annually as part of this process.	
	Considers the Required Level of Precision—Management reflects the required level of precision and accuracy suitable for user needs in nonfinancial reporting objectives and materiality within financial reporting objectives.	The Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	URS evaluated the control documentation, assigned responsibilities, and available records mapped to CC3.1 and assessed the specific requirement that management reflects the required level of precision and accuracy suitable for user needs in nonfinancial reporting objectives and materiality within financial reporting objectives. Based on the POA description and the referenced evidence, URS concluded that the Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	**No exceptions noted.**

	Reflects Entity Activities—Internal reporting reflects the underlying transactions and events within a range of acceptable limits.	The Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	URS examined the governing procedures and referenced evidence mapped to CC3.1 and assessed the specific requirement that internal reporting reflects the underlying transactions and events within a range of acceptable limits. Based on the POA description and the referenced evidence, URS confirmed that the Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	**No exceptions noted.**
	Compliance Objectives			
	Reflects External Laws and Regulations—Laws and regulations establish minimum standards of conduct, which the entity integrates into compliance objectives.	The Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to	URS evaluated the documented control design and supporting records mapped to CC3.1 and assessed the specific requirement that laws and regulations establish minimum standards of conduct, which the entity	**No exceptions noted.**

		make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	integrates into compliance objectives. Based on the POA description and the referenced evidence, URS established that the Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	
	Considers Tolerances for Risk— Management considers the acceptable levels of variation relative to the achievement of operations objectives.	The Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	URS verified the documented control design and supporting records mapped to CC3.1 and assessed the specific requirement that management considers the acceptable levels of variation relative to the achievement of operations objectives. Based on the POA description and the referenced evidence, URS established that the Cybersecurity Manager provides management with accurate and complete information on the state of the	**No exceptions noted.**

			ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	
	Additional point of focus when using the trust services criteria:			
	Establishes Sub-Objectives for Risk Assessment — Management identifies sub-objectives for use in risk assessment related to Security, Availability and Confidentiality to support the achievement of the entity's objectives.	The Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	URS evaluated the documented control design and supporting records mapped to CC3.1 and assessed the specific requirement that management identifies sub-objectives for use in risk assessment related to Security, Availability and Confidentiality to support the achievement of the entity's objectives. Based on the POA description and the referenced evidence, URS found that the Cybersecurity Manager provides management with accurate and complete information on the state of the ISMS through the annual ISMS review and risk assessment reports, enabling management to make informed decisions on security priorities, resource	**No exceptions noted.**

			allocation, and risk treatment. ISMS objectives are defined in the ISMS Objectives document and reviewed at least annually as part of this process.	
CC3.2	**COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.**			
	Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels—The entity identifies and assesses risk at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives.	An annual, documented risk assessment identifies and evaluates threats and vulnerabilities to information assets, including risks arising from suppliers, business partners, and other third parties with access to company systems, using a defined risk methodology. Risk significance is estimated based on likelihood and impact, and risk owners determine and document the risk response (mitigate, accept, transfer, avoid) in the risk treatment plan.	URS examined the documented control design and supporting records mapped to CC3.2 and assessed the specific requirement that the entity identifies and assesses risk at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives. Based on the POA description and the referenced evidence, URS found that an annual, documented risk assessment identifies and evaluates threats and vulnerabilities to information assets, including risks arising from suppliers, business partners, and other third parties with access to company systems, using a defined risk methodology. Risk significance is estimated based on likelihood and impact, and risk owners determine and document the risk response (mitigate,	**No exceptions noted.**

			accept, transfer, avoid) in the risk treatment plan.	
	Analyzes Internal and External Factors—Risk identification considers both internal and external factors and their impact on the achievement of objectives.	An annual, documented risk assessment identifies and evaluates threats and vulnerabilities to information assets, including risks arising from suppliers, business partners, and other third parties with access to company systems, using a defined risk methodology. Risk significance is estimated based on likelihood and impact, and risk owners determine and document the risk response (mitigate, accept, transfer, avoid) in the risk treatment plan.	URS evaluated the applicable policy requirements and implementation evidence mapped to CC3.2 and assessed the specific requirement that risk identification considers both internal and external factors and their impact on the achievement of objectives. Based on the POA description and the referenced evidence, URS determined that an annual, documented risk assessment identifies and evaluates threats and vulnerabilities to information assets, including risks arising from suppliers, business partners, and other third parties with access to company systems, using a defined risk methodology. Risk significance is estimated based on likelihood and impact, and risk owners determine and document the risk response (mitigate, accept, transfer, avoid) in the risk treatment plan.	**No exceptions noted.**
	Involves Appropriate Levels of Management—The entity puts into	An annual, documented risk assessment identifies and	URS verified the process description and evidence	**No exceptions noted.**

	place effective risk assessment mechanisms that involve appropriate levels of management.	evaluates threats and vulnerabilities to information assets, including risks arising from suppliers, business partners, and other third parties with access to company systems, using a defined risk methodology. Risk significance is estimated based on likelihood and impact, and risk owners determine and document the risk response (mitigate, accept, transfer, avoid) in the risk treatment plan.	identified in the POA mapped to CC3.2 and assessed the specific requirement that the entity puts into place effective risk assessment mechanisms that involve appropriate levels of management. Based on the POA description and the referenced evidence, URS established that an annual, documented risk assessment identifies and evaluates threats and vulnerabilities to information assets, including risks arising from suppliers, business partners, and other third parties with access to company systems, using a defined risk methodology. Risk significance is estimated based on likelihood and impact, and risk owners determine and document the risk response (mitigate, accept, transfer, avoid) in the risk treatment plan.	
	Estimates Significance of Risks Identified—Identified risks are analyzed through a process that includes estimating the potential significance of the risk.	An annual, documented risk assessment identifies and evaluates threats and vulnerabilities to information assets, including risks arising from suppliers, business partners, and other third parties with access to company systems, using a defined	URS reviewed the process description and evidence identified in the POA mapped to CC3.2 and assessed the specific requirement that identified risks are analyzed through a process that includes estimating the potential significance of the risk.	**No exceptions noted.**

		risk methodology. Risk significance is estimated based on likelihood and impact, and risk owners determine and document the risk response (mitigate, accept, transfer, avoid) in the risk treatment plan.	Based on the POA description and the referenced evidence, URS concluded that an annual, documented risk assessment identifies and evaluates threats and vulnerabilities to information assets, including risks arising from suppliers, business partners, and other third parties with access to company systems, using a defined risk methodology. Risk significance is estimated based on likelihood and impact, and risk owners determine and document the risk response (mitigate, accept, transfer, avoid) in the risk treatment plan.	
	Determines How to Respond to Risks—Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.	An annual, documented risk assessment identifies and evaluates threats and vulnerabilities to information assets, including risks arising from suppliers, business partners, and other third parties with access to company systems, using a defined risk methodology. Risk significance is estimated based on likelihood and impact, and risk owners determine and document the risk response (mitigate, accept, transfer, avoid) in the risk treatment plan.	URS inspected the documented control design and supporting records mapped to CC3.2 and assessed the specific requirement that risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk. Based on the POA description and the referenced evidence, URS found that an annual, documented risk assessment identifies and evaluates threats and vulnerabilities to information assets, including risks arising from	**No exceptions noted.**

			suppliers, business partners, and other third parties with access to company systems, using a defined risk methodology. Risk significance is estimated based on likelihood and impact, and risk owners determine and document the risk response (mitigate, accept, transfer, avoid) in the risk treatment plan.	
	Additional points of focus when using the trust services criteria:			
	Identifies Threats to Objectives — The entity identifies threats to the achievement of its objectives from intentional (including malicious) and unintentional acts and environmental events.	An annual, documented risk assessment identifies and evaluates threats and vulnerabilities to information assets, including risks arising from suppliers, business partners, and other third parties with access to company systems, using a defined risk methodology. Risk significance is estimated based on likelihood and impact, and risk owners determine and document the risk response (mitigate, accept, transfer, avoid) in the risk treatment plan.	URS verified the process description and evidence identified in the POA mapped to CC3.2 and assessed the specific requirement that the entity identifies threats to the achievement of its objectives from intentional (including malicious) and unintentional acts and environmental events. Based on the POA description and the referenced evidence, URS found that an annual, documented risk assessment identifies and evaluates threats and vulnerabilities to information assets, including risks arising from suppliers, business partners, and other third parties with access to company systems, using a defined risk methodology. Risk	**No exceptions noted.**

			significance is estimated based on likelihood and impact, and risk owners determine and document the risk response (mitigate, accept, transfer, avoid) in the risk treatment plan.	
	Identifies Vulnerability of System Components — The entity identifies the vulnerabilities of system components, including system processes, infrastructure, software, and other information assets.	An annual, documented risk assessment identifies and evaluates threats and vulnerabilities to information assets, including risks arising from suppliers, business partners, and other third parties with access to company systems, using a defined risk methodology. Risk significance is estimated based on likelihood and impact, and risk owners determine and document the risk response (mitigate, accept, transfer, avoid) in the risk treatment plan.	URS reviewed the documented control design and supporting records mapped to CC3.2 and assessed the specific requirement that the entity identifies the vulnerabilities of system components, including system processes, infrastructure, software, and other information assets. Based on the POA description and the referenced evidence, URS confirmed that an annual, documented risk assessment identifies and evaluates threats and vulnerabilities to information assets, including risks arising from suppliers, business partners, and other third parties with access to company systems, using a defined risk methodology. Risk significance is estimated based on likelihood and impact, and risk owners determine and document the risk response (mitigate,	**No exceptions noted.**

			accept, transfer, avoid) in the risk treatment plan.	
	Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other Parties — The entity's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and other third parties with access to the entity's information systems.	An annual, documented risk assessment identifies and evaluates threats and vulnerabilities to information assets, including risks arising from suppliers, business partners, and other third parties with access to company systems, using a defined risk methodology. Risk significance is estimated based on likelihood and impact, and risk owners determine and document the risk response (mitigate, accept, transfer, avoid) in the risk treatment plan.	URS evaluated the control documentation, assigned responsibilities, and available records mapped to CC3.2 and assessed the specific requirement that the entity's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and other third parties with access to the entity's information systems. Based on the POA description and the referenced evidence, URS concluded that an annual, documented risk assessment identifies and evaluates threats and vulnerabilities to information assets, including risks arising from suppliers, business partners, and other third parties with access to company systems, using a defined risk methodology. Risk significance is estimated based on likelihood and impact, and risk owners determine and document	**No exceptions noted.**

			the risk response (mitigate, accept, transfer, avoid) in the risk treatment plan.	
	Assesses the Significance of the Risks — The entity assesses the significance of the identified risks, including (1) determining the criticality of system components, including information assets, in achieving the objectives; (2) assessing the susceptibility of the identified vulnerabilities to the identified threats (3) assessing the likelihood of the identified risks (4) assessing the magnitude of the effect of potential risks to the achievement of the objectives; (5) considering the potential effects of unidentified threats and vulnerabilities on the assessed risks; (6) developing risk mitigation strategies to address the assessed risks; and (7) evaluating the appropriateness of residual risk (including whether to accept, reduce, or share such risks).	An annual, documented risk assessment identifies and evaluates threats and vulnerabilities to information assets, including risks arising from suppliers, business partners, and other third parties with access to company systems, using a defined risk methodology. Risk significance is estimated based on likelihood and impact, and risk owners determine and document the risk response (mitigate, accept, transfer, avoid) in the risk treatment plan.	URS reviewed the applicable policy requirements and implementation evidence mapped to CC3.2 and assessed the specific requirement that the entity assesses the significance of the identified risks, including (1) determining the criticality of system components, including information assets, in achieving the objectives; (2) assessing the susceptibility of the identified vulnerabilities to the identified threats (3) assessing the likelihood of the identified risks (4) assessing the magnitude of the effect of potential risks to the achievement of the objectives; (5) considering the potential effects of unidentified threats and vulnerabilities on the assessed risks; (6) developing risk mitigation strategies to address the assessed risks; and (7) evaluating the appropriateness of residual risk (including whether to accept, reduce, or share such risks). Based on the POA description and the referenced evidence, URS	**No exceptions noted.**

			determined that an annual, documented risk assessment identifies and evaluates threats and vulnerabilities to information assets, including risks arising from suppliers, business partners, and other third parties with access to company systems, using a defined risk methodology. Risk significance is estimated based on likelihood and impact, and risk owners determine and document the risk response (mitigate, accept, transfer, avoid) in the risk treatment plan.	
CC3.3	**COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.**			
	Considers Various Types of Fraud— The assessment of fraud considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.	Fraud, sabotage, and misuse of assigned authority by an employee (e.g., misappropriation of assets, deliberate damage or disruption, or circumventing approval or control processes) are assessed as part of the risk analysis, using the same threat/vulnerability scoring approach as other risks.	URS examined the applicable policy requirements and implementation evidence mapped to CC3.3 and assessed the specific requirement that the assessment of fraud considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur. Based on the POA description and the referenced evidence, URS confirmed that fraud, sabotage, and misuse of assigned authority by an employee (e.g.,	**No exceptions noted.**

			misappropriation of assets, deliberate damage or disruption, or circumventing approval or control processes) are assessed as part of the risk analysis, using the same threat/vulnerability scoring approach as other risks.	
	Assesses Incentives and Pressures — The assessment of fraud risks considers incentives and pressures.	Fraud, sabotage, and misuse of assigned authority by an employee (e.g., misappropriation of assets, deliberate damage or disruption, or circumventing approval or control processes) are assessed as part of the risk analysis, using the same threat/vulnerability scoring approach as other risks.	URS examined the process description and evidence identified in the POA mapped to CC3.3 and assessed the specific requirement that the assessment of fraud risks considers incentives and pressures. Based on the POA description and the referenced evidence, URS concluded that fraud, sabotage, and misuse of assigned authority by an employee (e.g., misappropriation of assets, deliberate damage or disruption, or circumventing approval or control processes) are assessed as part of the risk analysis, using the same threat/vulnerability scoring approach as other risks.	**No exceptions noted.**
	Assesses Opportunities— The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering the	Fraud, sabotage, and misuse of assigned authority by an employee (e.g., misappropriation of assets, deliberate damage or disruption, or circumventing approval or	URS evaluated the relevant policies, technical arrangements, and retained evidence mapped to CC3.3 and assessed the specific requirement that the assessment	**No exceptions noted.**

	entity's reporting records, or committing other inappropriate acts.	control processes) are assessed as part of the risk analysis, using the same threat/vulnerability scoring approach as other risks.	of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering the entity's reporting records, or committing other inappropriate acts. Based on the POA description and the referenced evidence, URS established that fraud, sabotage, and misuse of assigned authority by an employee (e.g., misappropriation of assets, deliberate damage or disruption, or circumventing approval or control processes) are assessed as part of the risk analysis, using the same threat/vulnerability scoring approach as other risks.	
	Assesses Attitudes and Rationalizations— The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions.	Fraud, sabotage, and misuse of assigned authority by an employee (e.g., misappropriation of assets, deliberate damage or disruption, or circumventing approval or control processes) are assessed as part of the risk analysis, using the same threat/vulnerability scoring approach as other risks.	URS assessed the process description and evidence identified in the POA mapped to CC3.3 and assessed the specific requirement that the assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions. Based on the POA description and the referenced evidence, URS established that fraud, sabotage, and misuse of assigned authority by an employee (e.g.,	**No exceptions noted.**

			misappropriation of assets, deliberate damage or disruption, or circumventing approval or control processes) are assessed as part of the risk analysis, using the same threat/vulnerability scoring approach as other risks.	
	Additional point of focus when using the trust services criteria:			
	Considers the Risks Related to the Use of IT and Access to Information — The assessment of fraud risks includes consideration of internal and external threats and vulnerabilities that arise specifically from the use of IT and access to information.	Fraud, sabotage, and misuse of assigned authority by an employee (e.g., misappropriation of assets, deliberate damage or disruption, or circumventing approval or control processes) are assessed as part of the risk analysis, using the same threat/vulnerability scoring approach as other risks.	URS assessed the documented control design and supporting records mapped to CC3.3 and assessed the specific requirement that the assessment of fraud risks includes consideration of internal and external threats and vulnerabilities that arise specifically from the use of IT and access to information. Based on the POA description and the referenced evidence, URS verified that fraud, sabotage, and misuse of assigned authority by an employee (e.g., misappropriation of assets, deliberate damage or disruption, or circumventing approval or control processes) are assessed as part of the risk analysis, using the same threat/vulnerability scoring approach as other risks.	**No exceptions noted.**

CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
	Assesses Changes in the External Environment—The risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.	The risk assessment and the ISMS documentation are reviewed at least annually, and additionally whenever significant changes occur (new suppliers, technology, leadership, business model, or after significant incidents), to identify new or changed threats and vulnerabilities and update the risk treatment plan accordingly.	URS inspected the governing procedures and referenced evidence mapped to CC3.4 and assessed the specific requirement that the risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates. Based on the POA description and the referenced evidence, URS found that the risk assessment and the ISMS documentation are reviewed at least annually, and additionally whenever significant changes occur (new suppliers, technology, leadership, business model, or after significant incidents), to identify new or changed threats and vulnerabilities and update the risk treatment plan accordingly.	**No exceptions noted.**
	Assesses Changes in the Business Model— The entity considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on	The risk assessment and the ISMS documentation are reviewed at least annually, and additionally whenever significant changes occur (new suppliers, technology, leadership, business model, or after significant incidents), to identify new or changed threats and vulnerabilities and update the risk treatment plan accordingly.	URS evaluated the governing procedures and referenced evidence mapped to CC3.4 and assessed the specific requirement that the entity considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the	**No exceptions noted.**

	foreign geographies, and new technologies.		system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies. Based on the POA description and the referenced evidence, URS concluded that the risk assessment and the ISMS documentation are reviewed at least annually, and additionally whenever significant changes occur (new suppliers, technology, leadership, business model, or after significant incidents), to identify new or changed threats and vulnerabilities and update the risk treatment plan accordingly.	
	Assesses Changes in Leadership— The entity considers changes in management and respective attitudes and philosophies on the system of internal control.	The risk assessment and the ISMS documentation are reviewed at least annually, and additionally whenever significant changes occur (new suppliers, technology, leadership, business model, or after significant incidents), to identify new or changed threats and vulnerabilities and update the risk treatment plan accordingly.	URS verified the applicable policy requirements and implementation evidence mapped to CC3.4 and assessed the specific requirement that the entity considers changes in management and respective attitudes and philosophies on the system of internal control. Based on the POA description and the referenced evidence, URS confirmed that the risk assessment and the ISMS documentation are reviewed at least annually, and additionally whenever significant changes occur (new suppliers, technology,	**No exceptions noted.**

			leadership, business model, or after significant incidents), to identify new or changed threats and vulnerabilities and update the risk treatment plan accordingly.	
	Additional point of focus when using the trust services criteria:			
	Assesses Changes in Systems and Technology— The risk identification process considers changes arising from changes in the entity's systems and changes in the technology environment.	The risk assessment and the ISMS documentation are reviewed at least annually, and additionally whenever significant changes occur (new suppliers, technology, leadership, business model, or after significant incidents), to identify new or changed threats and vulnerabilities and update the risk treatment plan accordingly.	URS reviewed the control documentation, assigned responsibilities, and available records mapped to CC3.4 and assessed the specific requirement that the risk identification process considers changes arising from changes in the entity's systems and changes in the technology environment. Based on the POA description and the referenced evidence, URS verified that the risk assessment and the ISMS documentation are reviewed at least annually, and additionally whenever significant changes occur (new suppliers, technology, leadership, business model, or after significant incidents), to identify new or changed threats and vulnerabilities and update the risk treatment plan accordingly.	**No exceptions noted.**
	Assesses Changes in Vendor and Business Partner Relationships—	The risk assessment and the ISMS documentation are reviewed at	URS verified the control documentation, assigned	**No exceptions noted.**

	The risk identification process considers changes in vendor and business partner relationships.	least annually, and additionally whenever significant changes occur (new suppliers, technology, leadership, business model, or after significant incidents), to identify new or changed threats and vulnerabilities and update the risk treatment plan accordingly.	responsibilities, and available records mapped to CC3.4 and assessed the specific requirement that the risk identification process considers changes in vendor and business partner relationships. Based on the POA description and the referenced evidence, URS determined that the risk assessment and the ISMS documentation are reviewed at least annually, and additionally whenever significant changes occur (new suppliers, technology, leadership, business model, or after significant incidents), to identify new or changed threats and vulnerabilities and update the risk treatment plan accordingly.	
	Assesses Changes in Threats and Vulnerabilities — The risk identification process assesses changes in (1) internal and external threats to and vulnerabilities of the components of the entity's systems and (2) the likelihood and magnitude of the resultant risks to the achievement of the entity's objectives.	The risk assessment and the ISMS documentation are reviewed at least annually, and additionally whenever significant changes occur (new suppliers, technology, leadership, business model, or after significant incidents), to identify new or changed threats and vulnerabilities and update the risk treatment plan accordingly.	URS examined the governing procedures and referenced evidence mapped to CC3.4 and assessed the specific requirement that the risk identification process assesses changes in (1) internal and external threats to and vulnerabilities of the components of the entity's systems and (2) the likelihood and magnitude of the resultant risks to the achievement of the entity's objectives. Based on the POA description and the	**No exceptions noted.**

			referenced evidence, URS verified that the risk assessment and the ISMS documentation are reviewed at least annually, and additionally whenever significant changes occur (new suppliers, technology, leadership, business model, or after significant incidents), to identify new or changed threats and vulnerabilities and update the risk treatment plan accordingly.	

CC4.0 Monitoring Activities

Criteria		Controls Defined by Big Dig Data s.r.o.	Tests of Controls Performed by URS	Results of Tests
CC4.1	**COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.**			
	Considers a Mix of Ongoing and Separate Evaluations—Management includes a balance of ongoing and separate evaluations.	The company combines ongoing evaluations (vulnerability scanning, log monitoring) with periodic separate evaluations (internal cybersecurity audits performed by an independent external auditor at least annually, and penetration testing, which has already been performed) to determine whether ISMS controls are present and functioning, with scope and frequency adjusted based on risk.	URS assessed the process description and evidence identified in the POA mapped to CC4.1 and assessed the specific requirement that management includes a balance of ongoing and separate evaluations. Based on the POA description and the referenced evidence, URS determined that the company combines ongoing evaluations (vulnerability scanning, log monitoring) with periodic separate evaluations (internal cybersecurity audits performed by an independent external auditor at least annually, and penetration testing, which has already been performed) to determine whether ISMS controls are present and functioning, with scope and frequency adjusted based on risk.	**No exceptions noted.**
	Considers Rate of Change—Management considers the rate of change in business and business processes when selecting and	The company combines ongoing evaluations (vulnerability scanning, log monitoring) with periodic separate evaluations (internal cybersecurity audits	URS examined the applicable policy requirements and implementation evidence mapped to CC4.1 and assessed the specific requirement that	**No exceptions noted.**

	developing ongoing and separate evaluations.	performed by an independent external auditor at least annually, and penetration testing, which has already been performed) to determine whether ISMS controls are present and functioning, with scope and frequency adjusted based on risk.	management considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations. Based on the POA description and the referenced evidence, URS established that the company combines ongoing evaluations (vulnerability scanning, log monitoring) with periodic separate evaluations (internal cybersecurity audits performed by an independent external auditor at least annually, and penetration testing, which has already been performed) to determine whether ISMS controls are present and functioning, with scope and frequency adjusted based on risk.	
	Establishes Baseline Understanding—The design and current state of an internal control system are used to establish a baseline for ongoing and separate evaluations.	The company combines ongoing evaluations (vulnerability scanning, log monitoring) with periodic separate evaluations (internal cybersecurity audits performed by an independent external auditor at least annually, and penetration testing, which has already been performed) to determine whether ISMS controls are present and functioning, with	URS evaluated the process description and evidence identified in the POA mapped to CC4.1 and assessed the specific requirement that the design and current state of an internal control system are used to establish a baseline for ongoing and separate evaluations. Based on the POA description and the referenced evidence, URS confirmed that the company combines ongoing	**No exceptions noted.**

		scope and frequency adjusted based on risk.	evaluations (vulnerability scanning, log monitoring) with periodic separate evaluations (internal cybersecurity audits performed by an independent external auditor at least annually, and penetration testing, which has already been performed) to determine whether ISMS controls are present and functioning, with scope and frequency adjusted based on risk.	
	Uses Knowledgeable Personnel—Evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated.	The company combines ongoing evaluations (vulnerability scanning, log monitoring) with periodic separate evaluations (internal cybersecurity audits performed by an independent external auditor at least annually, and penetration testing, which has already been performed) to determine whether ISMS controls are present and functioning, with scope and frequency adjusted based on risk.	URS verified the governing procedures and referenced evidence mapped to CC4.1 and assessed the specific requirement that evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated. Based on the POA description and the referenced evidence, URS concluded that the company combines ongoing evaluations (vulnerability scanning, log monitoring) with periodic separate evaluations (internal cybersecurity audits performed by an independent external auditor at least annually, and penetration testing, which has already been performed) to	**No exceptions noted.**

			determine whether ISMS controls are present and functioning, with scope and frequency adjusted based on risk.	
	Integrates with Business Processes—Ongoing evaluations are built into the business processes and adjust to changing conditions.	The company combines ongoing evaluations (vulnerability scanning, log monitoring) with periodic separate evaluations (internal cybersecurity audits performed by an independent external auditor at least annually, and penetration testing, which has already been performed) to determine whether ISMS controls are present and functioning, with scope and frequency adjusted based on risk.	URS evaluated the control documentation, assigned responsibilities, and available records mapped to CC4.1 and assessed the specific requirement that ongoing evaluations are built into the business processes and adjust to changing conditions. Based on the POA description and the referenced evidence, URS confirmed that the company combines ongoing evaluations (vulnerability scanning, log monitoring) with periodic separate evaluations (internal cybersecurity audits performed by an independent external auditor at least annually, and penetration testing, which has already been performed) to determine whether ISMS controls are present and functioning, with scope and frequency adjusted based on risk.	**No exceptions noted.**
	Adjusts Scope and Frequency—Management varies the scope and	The company combines ongoing evaluations (vulnerability scanning, log monitoring) with	URS assessed the governing procedures and referenced evidence mapped to CC4.1 and	**No exceptions noted.**

	frequency of separate evaluations depending on risk.	periodic separate evaluations (internal cybersecurity audits performed by an independent external auditor at least annually, and penetration testing, which has already been performed) to determine whether ISMS controls are present and functioning, with scope and frequency adjusted based on risk.	assessed the specific requirement that management varies the scope and frequency of separate evaluations depending on risk. Based on the POA description and the referenced evidence, URS found that the company combines ongoing evaluations (vulnerability scanning, log monitoring) with periodic separate evaluations (internal cybersecurity audits performed by an independent external auditor at least annually, and penetration testing, which has already been performed) to determine whether ISMS controls are present and functioning, with scope and frequency adjusted based on risk.	
	Objectively Evaluates— Separate evaluations are performed periodically to provide objective feedback.	The company combines ongoing evaluations (vulnerability scanning, log monitoring) with periodic separate evaluations (internal cybersecurity audits performed by an independent external auditor at least annually, and penetration testing, which has already been performed) to determine whether ISMS controls are present and functioning, with scope and frequency adjusted based on risk.	URS examined the relevant policies, technical arrangements, and retained evidence mapped to CC4.1 and assessed the specific requirement that separate evaluations are performed periodically to provide objective feedback. Based on the POA description and the referenced evidence, URS determined that the company combines ongoing evaluations (vulnerability scanning, log monitoring) with	**No exceptions noted.**

			periodic separate evaluations (internal cybersecurity audits performed by an independent external auditor at least annually, and penetration testing, which has already been performed) to determine whether ISMS controls are present and functioning, with scope and frequency adjusted based on risk.	
	Additional point of focus when using the trust services criteria:			
	Considers Different Types of Ongoing and Separate Evaluations — Management uses a variety of ongoing and separate risk and control evaluations to determine whether internal controls are present and functioning. Depending on the entity's objectives, such risk and control evaluations may include first- and second-line monitoring and control testing, internal audit assessments, compliance assessments, resilience assessments, vulnerability scans, security assessment, penetration testing, and third-party assessments.	The company combines ongoing evaluations (vulnerability scanning, log monitoring) with periodic separate evaluations (internal cybersecurity audits performed by an independent external auditor at least annually, and penetration testing, which has already been performed) to determine whether ISMS controls are present and functioning, with scope and frequency adjusted based on risk.	URS reviewed the governing procedures and referenced evidence mapped to CC4.1 and assessed the specific requirement that management uses a variety of ongoing and separate risk and control evaluations to determine whether internal controls are present and functioning. Depending on the entity's objectives, such risk and control evaluations may include first- and second-line monitoring and control testing, internal audit assessments, compliance assessments, resilience assessments, vulnerability scans, security assessment, penetration testing, and third-party assessments. Based on the POA description and the referenced	**No exceptions noted.**

			evidence, URS confirmed that the company combines ongoing evaluations (vulnerability scanning, log monitoring) with periodic separate evaluations (internal cybersecurity audits performed by an independent external auditor at least annually, and penetration testing, which has already been performed) to determine whether ISMS controls are present and functioning, with scope and frequency adjusted based on risk.	
CC4.2	**COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.**			
	Assesses Results—Management and the board of directors, as appropriate, assess results of ongoing and separate evaluations.	Audit findings and identified deficiencies are documented in the Cybersecurity Audit Report and reported to management, who reviews, approves, and directs corrective action. The Cybersecurity Manager tracks remediation of corrective actions to completion, and results feed into the annual ISMS Management Review Report.	URS reviewed the governing procedures and referenced evidence mapped to CC4.2 and assessed the specific requirement that management and the board of directors, as appropriate, assess results of ongoing and separate evaluations. Based on the POA description and the referenced evidence, URS found that the Cybersecurity Manager tracks remediation of corrective actions to completion, and results feed into the annual ISMS Management Review Report. Audit findings and identified deficiencies are	**No exceptions noted.**

			documented in the Cybersecurity Audit Report and reported to management, who reviews, approves, and directs corrective action.	
	Communicates Deficiencies—Deficiencies are communicated to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate.	Audit findings and identified deficiencies are documented in the Cybersecurity Audit Report and reported to management, who reviews, approves, and directs corrective action. The Cybersecurity Manager tracks remediation of corrective actions to completion, and results feed into the annual ISMS Management Review Report.	URS verified the control documentation, assigned responsibilities, and available records mapped to CC4.2 and assessed the specific requirement that deficiencies are communicated to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate. Based on the POA description and the referenced evidence, URS established that audit findings and identified deficiencies are documented in the Cybersecurity Audit Report and reported to management, who reviews, approves, and directs corrective action. The Cybersecurity Manager tracks remediation of corrective actions to completion, and results feed into the annual ISMS Management Review Report.	**No exceptions noted.**

	Monitors Corrective Action—Management tracks whether deficiencies are remedied on a timely basis.	Audit findings and identified deficiencies are documented in the Cybersecurity Audit Report and reported to management, who reviews, approves, and directs corrective action. The Cybersecurity Manager tracks remediation of corrective actions to completion, and results feed into the annual ISMS Management Review Report.	URS inspected the documented control design and supporting records mapped to CC4.2 and assessed the specific requirement that management tracks whether deficiencies are remedied on a timely basis. Based on the POA description and the referenced evidence, URS confirmed that audit findings and identified deficiencies are documented in the Cybersecurity Audit Report and reported to management, who reviews, approves, and directs corrective action. The Cybersecurity Manager tracks remediation of corrective actions to completion, and results feed into the annual ISMS Management Review Report.	**No exceptions noted.**

CC5.0 Control Activities

Criteria		Controls Defined by Big Dig Data s.r.o.	Tests of Controls Performed by URS	Results of Tests
CC5.1	**COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.**			
	Integrates With Risk Assessment—Control activities help ensure that risk responses that address and mitigate risks are carried out.	Control activities are selected based on the outcome of the risk assessment and the company's size and risk profile. Segregation of incompatible duties is applied where practical (e.g., the Cybersecurity Manager role may not be combined with the Asset Owner role); where full segregation is not feasible given the company's size, compensating controls such as independent review of access rights and activity logging are used.	URS examined the governing procedures and referenced evidence mapped to CC5.1 and assessed the specific requirement that control activities help ensure that risk responses that address and mitigate risks are carried out. Based on the POA description and the referenced evidence, URS concluded that control activities are selected based on the outcome of the risk assessment and the company's size and risk profile. Segregation of incompatible duties is applied where practical (e.g., the Cybersecurity Manager role may not be combined with the Asset Owner role); where full segregation is not feasible given the company's size, compensating controls such as independent review of access rights and activity logging are used.	**No exceptions noted.**
	Considers Entity-Specific Factors—Management considers how the environment, complexity, nature, and scope of	Control activities are selected based on the outcome of the risk assessment and the company's size and risk profile. Segregation of	URS reviewed the governing procedures and referenced evidence mapped to CC5.1 and assessed the specific requirement	**No exceptions noted.**

	its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.	incompatible duties is applied where practical (e.g., the Cybersecurity Manager role may not be combined with the Asset Owner role); where full segregation is not feasible given the company's size, compensating controls such as independent review of access rights and activity logging are used.	that management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities. Based on the POA description and the referenced evidence, URS found that control activities are selected based on the outcome of the risk assessment and the company's size and risk profile. Segregation of incompatible duties is applied where practical (e.g., the Cybersecurity Manager role may not be combined with the Asset Owner role); where full segregation is not feasible given the company's size, compensating controls such as independent review of access rights and activity logging are used.	
	Determines Relevant Business Processes—Management determines which relevant business processes require control activities.	Control activities are selected based on the outcome of the risk assessment and the company's size and risk profile. Segregation of incompatible duties is applied where practical (e.g., the Cybersecurity Manager role may not be combined with the Asset Owner role); where full segregation is not feasible given the company's	URS assessed the applicable policy requirements and implementation evidence mapped to CC5.1 and assessed the specific requirement that management determines which relevant business processes require control activities. Based on the POA description and the referenced evidence, URS found	**No exceptions noted.**

		size, compensating controls such as independent review of access rights and activity logging are used.	that control activities are selected based on the outcome of the risk assessment and the company's size and risk profile. Segregation of incompatible duties is applied where practical (e.g., the Cybersecurity Manager role may not be combined with the Asset Owner role); where full segregation is not feasible given the company's size, compensating controls such as independent review of access rights and activity logging are used.	
	Evaluates a Mix of Control Activity Types—Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.	Control activities are selected based on the outcome of the risk assessment and the company's size and risk profile. Segregation of incompatible duties is applied where practical (e.g., the Cybersecurity Manager role may not be combined with the Asset Owner role); where full segregation is not feasible given the company's size, compensating controls such as independent review of access rights and activity logging are used.	URS evaluated the process description and evidence identified in the POA mapped to CC5.1 and assessed the specific requirement that control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls. Based on the POA description and the referenced evidence, URS determined that control activities are selected based on the outcome of the risk assessment and the company's size and risk profile. Segregation of incompatible duties is applied	**No exceptions noted.**

			where practical (e.g., the Cybersecurity Manager role may not be combined with the Asset Owner role); where full segregation is not feasible given the company's size, compensating controls such as independent review of access rights and activity logging are used.	
	Considers at What Level Activities Are Applied—Management considers control activities at various levels in the entity.	Control activities are selected based on the outcome of the risk assessment and the company's size and risk profile. Segregation of incompatible duties is applied where practical (e.g., the Cybersecurity Manager role may not be combined with the Asset Owner role); where full segregation is not feasible given the company's size, compensating controls such as independent review of access rights and activity logging are used.	URS inspected the applicable policy requirements and implementation evidence mapped to CC5.1 and assessed the specific requirement that management considers control activities at various levels in the entity. Based on the POA description and the referenced evidence, URS verified that control activities are selected based on the outcome of the risk assessment and the company's size and risk profile. Segregation of incompatible duties is applied where practical (e.g., the Cybersecurity Manager role may not be combined with the Asset Owner role); where full segregation is not feasible given the company's size, compensating controls such as independent review of access rights and activity logging are used.	**No exceptions noted.**

	Addresses Segregation of Duties—Management segregates incompatible duties, and where such segregation is not practical, management selects and develops alternative control activities.	Control activities are selected based on the outcome of the risk assessment and the company's size and risk profile. Segregation of incompatible duties is applied where practical (e.g., the Cybersecurity Manager role may not be combined with the Asset Owner role); where full segregation is not feasible given the company's size, compensating controls such as independent review of access rights and activity logging are used.	URS reviewed the relevant policies, technical arrangements, and retained evidence mapped to CC5.1 and assessed the specific requirement that management segregates incompatible duties, and where such segregation is not practical, management selects and develops alternative control activities. Based on the POA description and the referenced evidence, URS determined that segregation of incompatible duties is applied where practical (e.g., the Cybersecurity Manager role may not be combined with the Asset Owner role); where full segregation is not feasible given the company's size, compensating controls such as independent review of access rights and activity logging are used. Control activities are selected based on the outcome of the risk assessment and the company's size and risk profile.	**No exceptions noted.**
CC5.2	**COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.**			
	Determines Dependency Between the Use of Technology in Business Processes and Technology General Controls—Management understands and	General technology controls covering access management and the acquisition, development, and maintenance of IT systems are defined and linked to the	URS evaluated the governing procedures and referenced evidence mapped to CC5.2 and assessed the specific requirement that management understands	**No exceptions noted.**

	determines the dependency and linkage between business processes, automated control activities, and technology general controls.	underlying business processes they support, and are reassessed whenever significant infrastructure or technology changes occur.	and determines the dependency and linkage between business processes, automated control activities, and technology general controls. Based on the POA description and the referenced evidence, URS verified that general technology controls covering access management and the acquisition, development, and maintenance of IT systems are defined and linked to the underlying business processes they support, and are reassessed whenever significant infrastructure or technology changes occur.	
	Establishes Relevant Technology Infrastructure Control Activities—Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.	General technology controls covering access management and the acquisition, development, and maintenance of IT systems are defined and linked to the underlying business processes they support, and are reassessed whenever significant infrastructure or technology changes occur.	URS inspected the documented control design and supporting records mapped to CC5.2 and assessed the specific requirement that management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing. Based on the POA description and the referenced evidence, URS verified that general technology controls covering access management and the acquisition, development, and	**No exceptions noted.**

			maintenance of IT systems are defined and linked to the underlying business processes they support, and are reassessed whenever significant infrastructure or technology changes occur.	
	Establishes Relevant Security Management Process Controls Activities—Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats.	General technology controls covering access management and the acquisition, development, and maintenance of IT systems are defined and linked to the underlying business processes they support, and are reassessed whenever significant infrastructure or technology changes occur.	URS assessed the process description and evidence identified in the POA mapped to CC5.2 and assessed the specific requirement that management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats. Based on the POA description and the referenced evidence, URS established that general technology controls covering access management and the acquisition, development, and maintenance of IT systems are defined and linked to the underlying business processes they support, and are reassessed whenever significant infrastructure or technology changes occur.	**No exceptions noted.**

	Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities—Management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives.	General technology controls covering access management and the acquisition, development, and maintenance of IT systems are defined and linked to the underlying business processes they support, and are reassessed whenever significant infrastructure or technology changes occur.	URS verified the applicable policy requirements and implementation evidence mapped to CC5.2 and assessed the specific requirement that management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives. Based on the POA description and the referenced evidence, URS concluded that general technology controls covering access management and the acquisition, development, and maintenance of IT systems are defined and linked to the underlying business processes they support, and are reassessed whenever significant infrastructure or technology changes occur.	**No exceptions noted.**
CC5.3	**COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.**			
	Establishes Policies and Procedures to Support Deployment of Management 's Directives—Management establishes control activities that are built into business processes and employees' day-to-day activities through policies	Control activities are deployed through a complete, versioned set of ISMS policies (1.01-1.20), with document ownership, review cadence (at least annually), and update procedures defined centrally, so that policies remain	URS reviewed the applicable policy requirements and implementation evidence mapped to CC5.3 and assessed the specific requirement that management establishes control activities that are built into business processes and	**No exceptions noted.**

	establishing what is expected and relevant procedures specifying actions.	relevant and are refreshed as needed.	employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions. Based on the POA description and the referenced evidence, URS determined that control activities are deployed through a complete, versioned set of ISMS policies (1.01-1.20), with document ownership, review cadence (at least annually), and update procedures defined centrally, so that policies remain relevant and are refreshed as needed.	
	Establishes Responsibility and Accountability for Executing Policies and Procedures—Management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside.	Control activities are deployed through a complete, versioned set of ISMS policies (1.01-1.20), with document ownership, review cadence (at least annually), and update procedures defined centrally, so that policies remain relevant and are refreshed as needed.	URS reviewed the relevant policies, technical arrangements, and retained evidence mapped to CC5.3 and assessed the specific requirement that management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside. Based on the POA description and the referenced evidence, URS verified that control activities are deployed through a complete, versioned set of ISMS policies (1.01-1.20), with document ownership, review	**No exceptions noted.**

			cadence (at least annually), and update procedures defined centrally, so that policies remain relevant and are refreshed as needed.	
	Performs in a Timely Manner—Responsible personnel perform control activities in a timely manner as defined by the policies and procedures.	Control activities are deployed through a complete, versioned set of ISMS policies (1.01-1.20), with document ownership, review cadence (at least annually), and update procedures defined centrally, so that policies remain relevant and are refreshed as needed.	URS reviewed the applicable policy requirements and implementation evidence mapped to CC5.3 and assessed the specific requirement that responsible personnel perform control activities in a timely manner as defined by the policies and procedures. Based on the POA description and the referenced evidence, URS verified that control activities are deployed through a complete, versioned set of ISMS policies (1.01-1.20), with document ownership, review cadence (at least annually), and update procedures defined centrally, so that policies remain relevant and are refreshed as needed.	**No exceptions noted.**
	Takes Corrective Action—Responsible personnel investigate and act on matters identified as a result of executing control activities.	Control activities are deployed through a complete, versioned set of ISMS policies (1.01-1.20), with document ownership, review cadence (at least annually), and	URS assessed the applicable policy requirements and implementation evidence mapped to CC5.3 and assessed the specific requirement that	**No exceptions noted.**

		update procedures defined centrally, so that policies remain relevant and are refreshed as needed.	responsible personnel investigate and act on matters identified as a result of executing control activities. Based on the POA description and the referenced evidence, URS confirmed that control activities are deployed through a complete, versioned set of ISMS policies (1.01-1.20), with document ownership, review cadence (at least annually), and update procedures defined centrally, so that policies remain relevant and are refreshed as needed.	
	Performs Using Competent Personnel—Competent personnel with sufficient authority perform control activities with diligence and continuing focus.	Control activities are deployed through a complete, versioned set of ISMS policies (1.01-1.20), with document ownership, review cadence (at least annually), and update procedures defined centrally, so that policies remain relevant and are refreshed as needed.	URS assessed the applicable policy requirements and implementation evidence mapped to CC5.3 and assessed the specific requirement that competent personnel with sufficient authority perform control activities with diligence and continuing focus. Based on the POA description and the referenced evidence, URS concluded that control activities are deployed through a complete, versioned set of ISMS policies (1.01-1.20), with document ownership, review cadence (at least annually), and update	**No exceptions noted.**

			procedures defined centrally, so that policies remain relevant and are refreshed as needed.	
	Reassesses Policies and Procedures—Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary.	Control activities are deployed through a complete, versioned set of ISMS policies (1.01-1.20), with document ownership, review cadence (at least annually), and update procedures defined centrally, so that policies remain relevant and are refreshed as needed.	URS evaluated the applicable policy requirements and implementation evidence mapped to CC5.3 and assessed the specific requirement that management periodically reviews control activities to determine their continued relevance and refreshes them when necessary. Based on the POA description and the referenced evidence, URS concluded that control activities are deployed through a complete, versioned set of ISMS policies (1.01-1.20), with document ownership, review cadence (at least annually), and update procedures defined centrally, so that policies remain relevant and are refreshed as needed.	**No exceptions noted.**

CC6.0 Logical and Physical Access Controls

Criteria		Controls Defined by Big Dig Data s.r.o.	Tests of Controls Performed by URS	Results of Tests
CC6.1	**The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.**			
	Identifies and Manages the Inventory of Information Assets — The entity identifies, inventories, classifies, and manages information assets (for example, infrastructure, software, and data).	Network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	URS verified the process description and evidence identified in the POA mapped to CC6.1 and assessed the specific requirement that the entity identifies, inventories, classifies, and manages information assets (for example, infrastructure, software, and data). Based on the POA description and the referenced evidence, URS found that network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	**No exceptions noted.**
	Assesses New Architectures — The entity identifies new system architectures and assesses their security prior to implementation into the system environment.	Network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's	URS evaluated the process description and evidence identified in the POA mapped to CC6.1 and assessed the specific requirement that the entity	**No exceptions noted.**

		IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	identifies new system architectures and assesses their security prior to implementation into the system environment. Based on the POA description and the referenced evidence, URS confirmed that network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	
	Restricts Logical Access — The entity restricts logical access to information assets, including infrastructure (for example, server, storage, network elements, APIs, and endpoint devices), software, and data (at rest, during processing, or in transmission) through the use of access control software, rule sets, and standard configuration hardening processes.	Network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	URS verified the applicable policy requirements and implementation evidence mapped to CC6.1 and assessed the specific requirement that the entity restricts logical access to information assets, including infrastructure (for example, server, storage, network elements, APIs, and endpoint devices), software, and data (at rest, during processing, or in transmission) through the use of access control software, rule sets, and standard configuration	**No exceptions noted.**

			hardening processes. Based on the POA description and the referenced evidence, URS determined that network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	
	Identifies and Authenticates Users — The entity identifies and authenticates persons, infrastructure, and software prior to accessing information assets, whether locally or remotely. The entity uses more complex or advanced user authentication techniques such as multifactor authentication when such protections are deemed appropriate based on its risk mitigation strategy.	Network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	URS examined the control documentation, assigned responsibilities, and available records mapped to CC6.1 and assessed the specific requirement that the entity identifies and authenticates persons, infrastructure, and software prior to accessing information assets, whether locally or remotely. The entity uses more complex or advanced user authentication techniques such as multifactor authentication when such protections are deemed appropriate based on its risk mitigation strategy. Based on the	**No exceptions noted.**

			POA description and the referenced evidence, URS established that network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	
	Considers Network Segmentation — The entity uses network segmentation, zero trust architectures, and other techniques to isolate unrelated portions of the entity's information technology from each other based on the entity's risk mitigation strategy.	Network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	URS examined the governing procedures and referenced evidence mapped to CC6.1 and assessed the specific requirement that the entity uses network segmentation, zero trust architectures, and other techniques to isolate unrelated portions of the entity's information technology from each other based on the entity's risk mitigation strategy. Based on the POA description and the referenced evidence, URS established that network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to	**No exceptions noted.**

			isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	
	Manages Points of Access— Points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The types of individuals and systems using each point of access are identified, documented, and managed.	Network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	URS examined the relevant policies, technical arrangements, and retained evidence mapped to CC6.1 and assessed the specific requirement that points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The types of individuals and systems using each point of access are identified, documented, and managed. Based on the POA description and the referenced evidence, URS verified that network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	**No exceptions noted.**

	Restricts Access to Information Assets — Combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access control rules and configuration standards for information assets.	Network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	URS verified the documented control design and supporting records mapped to CC6.1 and assessed the specific requirement that combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access control rules and configuration standards for information assets. Based on the POA description and the referenced evidence, URS determined that network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	**No exceptions noted.**
	Manages Identification and Authentication—Identification and authentication requirements are established, documented, and managed for individuals and systems	Network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other.	URS evaluated the relevant policies, technical arrangements, and retained evidence mapped to CC6.1 and assessed the specific requirement that identification and authentication requirements	**No exceptions noted.**

	accessing entity information, infrastructure and software.	Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	are established, documented, and managed for individuals and systems accessing entity information, infrastructure and software. Based on the POA description and the referenced evidence, URS verified that network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	
	Manages Credentials for Infrastructure and Software— New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required or the infrastructure and software are no longer in use.	Network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	URS reviewed the process description and evidence identified in the POA mapped to CC6.1 and assessed the specific requirement that new internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required or the infrastructure and software are	**No exceptions noted.**

			no longer in use. Based on the POA description and the referenced evidence, URS established that network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	
	Uses Encryption to Protect Data — The entity uses encryption to protect data (at rest, during processing, or in transmission), when such protections are deemed appropriate based on the entity's risk mitigation strategy.	Network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	URS assessed the governing procedures and referenced evidence mapped to CC6.1 and assessed the specific requirement that the entity uses encryption to protect data (at rest, during processing, or in transmission), when such protections are deemed appropriate based on the entity's risk mitigation strategy. Based on the POA description and the referenced evidence, URS concluded that network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to	**No exceptions noted.**

			isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	
	Protects Cryptographic Keys — The entity protects cryptographic keys during generation, storage, use, and destruction. Cryptographic modules, algorithms, key lengths, and architectures are appropriate based on the entity's risk mitigation strategy.	Network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	URS assessed the documented control design and supporting records mapped to CC6.1 and assessed the specific requirement that the entity protects cryptographic keys during generation, storage, use, and destruction. Cryptographic modules, algorithms, key lengths, and architectures are appropriate based on the entity's risk mitigation strategy. Based on the POA description and the referenced evidence, URS verified that data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy. Network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other.	**No exceptions noted.**

	Additional point of focus when using the trust services criteria for confidentiality:			
	Restricts Access to and Use of Confidential Information for Identified Purposes —Logical access to and use of confidential information is restricted to identified purposes.	Network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	URS examined the governing procedures and referenced evidence mapped to CC6.1 and assessed the specific requirement that logical access to and use of confidential information is restricted to identified purposes. Based on the POA description and the referenced evidence, URS confirmed that network segmentation and zero-trust principles are applied where technically feasible, particularly for cloud-hosted services, to isolate unrelated portions of the company's IT environment from each other. Data in transit and at rest is encrypted, with cryptographic keys managed under a dedicated policy.	**No exceptions noted.**
CC6.2	**Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.**			
	Creates Access Credentials to Protected Information Assets — The entity creates credentials for accessing protected information assets based on an authorization from the system's asset owner or authorized	Access credentials are disabled no later than the day a user's employment or contract ends, per the documented offboarding procedure, preventing further use of invalid credentials. Access rights are	URS examined the relevant policies, technical arrangements, and retained evidence mapped to CC6.2 and assessed the specific requirement that the entity creates credentials for accessing protected information assets	**No exceptions noted.**

	custodian. Authorization is required for the creation of all types of credentials of individuals (for example, employees, contractors, vendors, and business partner personnel), systems, and software.	also subject to periodic review to confirm they remain valid	based on an authorization from the system's asset owner or authorized custodian. Authorization is required for the creation of all types of credentials of individuals (for example, employees, contractors, vendors, and business partner personnel), systems, and software. Based on the POA description and the referenced evidence, URS found that access credentials are disabled no later than the day a user's employment or contract ends, per the documented offboarding procedure, preventing further use of invalid credentials. Access rights are also subject to periodic review to confirm they remain valid.	
	Reviews Validity of Access Credentials — The entity reviews access credentials on a periodic basis for validity (for example, employees, contractors, vendors, and business partner personnel) and inappropriate system or service accounts.	Access credentials are disabled no later than the day a user's employment or contract ends, per the documented offboarding procedure, preventing further use of invalid credentials. Access rights are also subject to periodic review to confirm they remain valid	URS examined the control documentation, assigned responsibilities, and available records mapped to CC6.2 and assessed the specific requirement that the entity reviews access credentials on a periodic basis for validity (for example, employees, contractors, vendors, and business partner personnel) and	**No exceptions noted.**

			inappropriate system or service accounts. Based on the POA description and the referenced evidence, URS established that access credentials are disabled no later than the day a user's employment or contract ends, per the documented offboarding procedure, preventing further use of invalid credentials. Access rights are also subject to periodic review to confirm they remain valid.	
	Prevents the Use of Credentials When No Longer Valid — Processes are in place to disable, destroy, or otherwise prevent the use of access credentials when no longer valid.	Access credentials are disabled no later than the day a user's employment or contract ends, per the documented offboarding procedure, preventing further use of invalid credentials. Access rights are also subject to periodic review to confirm they remain valid.	URS assessed the process description and evidence identified in the POA mapped to CC6.2 and assessed the specific requirement that processes are in place to disable, destroy, or otherwise prevent the use of access credentials when no longer valid. Based on the POA description and the referenced evidence, URS found that access credentials are disabled no later than the day a user's employment or contract ends, per the documented offboarding procedure, preventing further use of invalid credentials. Access rights are also subject to periodic	**No exceptions noted.**

			review to confirm they remain valid.	
CC6.3	**The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.**			
	Creates or Modifies Access to Protected Information Assets— Processes are in place to create or modify access to protected information assets based on authorization from the asset's owner.	Access rights, including privileged and administrative access, are periodically reviewed by the relevant asset owner to confirm they remain necessary and appropriate for each individual's current role; unnecessary or inappropriate access identified during review is revoked or modified accordingly	URS evaluated the control documentation, assigned responsibilities, and available records mapped to CC6.3 and assessed the specific requirement that processes are in place to create or modify access to protected information assets based on authorization from the asset's owner. Based on the POA description and the referenced evidence, URS determined that access rights, including privileged and administrative access, are periodically reviewed by the relevant asset owner to confirm they remain necessary and appropriate for each individual's current role; unnecessary or inappropriate access identified during review is revoked or modified accordingly.	**No exceptions noted.**
	Removes Access to Protected Information Assets — Processes are in place to remove access to	Access rights, including privileged and administrative access, are periodically reviewed by the relevant	URS assessed the process description and evidence identified in the POA mapped to	**No exceptions noted.**

	protected information assets when no longer required.	asset owner to confirm they remain necessary and appropriate for each individual's current role; unnecessary or inappropriate access identified during review is revoked or modified accordingly	CC6.3 and assessed the specific requirement that processes are in place to remove access to protected information assets when no longer required. Based on the POA description and the referenced evidence, URS verified that access rights, including privileged and administrative access, are periodically reviewed by the relevant asset owner to confirm they remain necessary and appropriate for each individual's current role; unnecessary or inappropriate access identified during review is revoked or modified accordingly.	
	Uses Access Control Structures — The entity uses access control structures, such as role-based access controls, to restrict access to protected information assets, limit privileges, and support segregation of incompatible functions.	Access rights, including privileged and administrative access, are periodically reviewed by the relevant asset owner to confirm they remain necessary and appropriate for each individual's current role; unnecessary or inappropriate access identified during review is revoked or modified accordingly	URS examined the documented control design and supporting records mapped to CC6.3 and assessed the specific requirement that the entity uses access control structures, such as role- based access controls, to restrict access to protected information assets, limit privileges, and support segregation of incompatible functions. Based on the POA description and the referenced evidence, URS concluded that access rights, including privileged	**No exceptions noted.**

			and administrative access, are periodically reviewed by the relevant asset owner to confirm they remain necessary and appropriate for each individual's current role; unnecessary or inappropriate access identified during review is revoked or modified accordingly.	
	Reviews Access Roles and Rules — The appropriateness of access roles and access rules is reviewed on a periodic basis for unnecessary and inappropriate individuals (for example, employees, contractors, vendors, business partner personnel) and inappropriate system or service accounts. Access roles and rules are modified, as appropriate.	Access rights, including privileged and administrative access, are periodically reviewed by the relevant asset owner to confirm they remain necessary and appropriate for each individual's current role; unnecessary or inappropriate access identified during review is revoked or modified accordingly.	URS inspected the control documentation, assigned responsibilities, and available records mapped to CC6.3 and assessed the specific requirement that the appropriateness of access roles and access rules is reviewed on a periodic basis for unnecessary and inappropriate individuals (for example, employees, contractors, vendors, business partner personnel) and inappropriate system or service accounts. Access roles and rules are modified, as appropriate. Based on the POA description and the referenced evidence, URS found that access rights, including privileged and administrative access, are periodically reviewed by the relevant asset owner to confirm	**No exceptions noted.**

			they remain necessary and appropriate for each individual's current role; unnecessary or inappropriate access identified during review is revoked or modified accordingly.	
CC6.4	**The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.**			
	Creates or Modifies Physical Access — Processes are in place to create or modify physical access by employees, contractors, vendors, and business partner personnel to facilities such as data centers, office spaces, and work areas, based on appropriate authorization.	Physical access to offices and protected information assets is restricted to authorized personnel, controlled and monitored per the Physical and Environmental Security Policy; return of keys, access cards, and company devices is required as part of the offboarding process.	URS inspected the process description and evidence identified in the POA mapped to CC6.4 and assessed the specific requirement that processes are in place to create or modify physical access by employees, contractors, vendors, and business partner personnel to facilities such as data centers, office spaces, and work areas, based on appropriate authorization. Based on the POA description and the referenced evidence, URS confirmed that physical access to offices and protected information assets is restricted to authorized personnel, controlled and monitored per the Physical and Environmental Security Policy; return of keys, access cards, and	**No exceptions noted.**

			company devices is required as part of the offboarding process.	
	Removes Physical Access — Processes are in place to remove physical access to facilities and protected information assets when an employee, contractor, vendor, or business partner no longer requires access.	Physical access to offices and protected information assets is restricted to authorized personnel, controlled and monitored per the Physical and Environmental Security Policy; return of keys, access cards, and company devices is required as part of the offboarding process.	URS examined the process description and evidence identified in the POA mapped to CC6.4 and assessed the specific requirement that processes are in place to remove physical access to facilities and protected information assets when an employee, contractor, vendor, or business partner no longer requires access. Based on the POA description and the referenced evidence, URS verified that physical access to offices and protected information assets is restricted to authorized personnel, controlled and monitored per the Physical and Environmental Security Policy; return of keys, access cards, and company devices is required as part of the offboarding process.	**No exceptions noted.**
	Recovers Physical Devices — Processes are in place to recover entity devices (for example, badges, laptops, and mobile devices) when an employee, contractor, vendor,	Physical access to offices and protected information assets is restricted to authorized personnel, controlled and monitored per the Physical and Environmental Security Policy; return of keys, access cards,	URS verified the governing procedures and referenced evidence mapped to CC6.4 and assessed the specific requirement that processes are in place to recover entity devices	**No exceptions noted.**

	or business partner no longer requires access.	and company devices is required as part of the offboarding process.	(for example, badges, laptops, and mobile devices) when an employee, contractor, vendor, or business partner no longer requires access. Based on the POA description and the referenced evidence, URS determined that physical access to offices and protected information assets is restricted to authorized personnel, controlled and monitored per the Physical and Environmental Security Policy; return of keys, access cards, and company devices is required as part of the offboarding process.	
	Reviews Physical Access — Processes are in place to periodically review Physical access to help ensure consistency with job responsibilities.	Physical access to offices and protected information assets is restricted to authorized personnel, controlled and monitored per the Physical and Environmental Security Policy; return of keys, access cards, and company devices is required as part of the offboarding process.	URS inspected the control documentation, assigned responsibilities, and available records mapped to CC6.4 and assessed the specific requirement that processes are in place to periodically review Physical access to help ensure consistency with job responsibilities. Based on the POA description and the referenced evidence, URS confirmed that physical access to offices and protected information assets is restricted to authorized	**No exceptions noted.**

			personnel, controlled and monitored per the Physical and Environmental Security Policy; return of keys, access cards, and company devices is required as part of the offboarding process.	
CC6.5	**The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.**			
	Removes Data and Software for Disposal — Procedures are in place to remove, delete, or otherwise render data and software inaccessible from physical assets and other devices owned by the entity, its vendors, and employees when the data and software are no longer required on the asset or the asset will no longer be under the control of the entity.	Data and software are securely removed from devices and media before disposal or re-use, with disposal method (deletion, overwrite, or physical destruction) determined by the classification of the information involved, and cloud provider certified secure-deletion mechanisms used for cloud storage.	URS inspected the relevant policies, technical arrangements, and retained evidence mapped to CC6.5 and assessed the specific requirement that procedures are in place to remove, delete, or otherwise render data and software inaccessible from physical assets and other devices owned by the entity, its vendors, and employees when the data and software are no longer required on the asset or the asset will no longer be under the control of the entity. Based on the POA description and the referenced evidence, URS found that data and software are securely removed from devices and media before disposal or re-use, with disposal method (deletion, overwrite, or physical destruction) determined by the classification of the information	**No exceptions noted.**

			involved, and cloud provider certified secure-deletion mechanisms used for cloud storage.	
CC6.6	**The entity implements logical access security measures to protect against threats from sources outside its system boundaries.**			
	Restricts Access—The types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted.	Transmission, movement, and removal of information is restricted to authorized users and processes and protected in transit via encryption (TLS 1.2+ or stronger; weak protocols such as SSL and TLS 1.0/1.1 are prohibited); handling rules for information transfer, portable media, and removal of assets are classification-dependent	URS evaluated the governing procedures and referenced evidence mapped to CC6.6 and assessed the specific requirement that the types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted. Based on the POA description and the referenced evidence, URS verified that boundary protection (firewalls, network segmentation, and monitoring at the network perimeter) is implemented to protect against threats originating outside the company's system boundary; cloud environments are additionally protected through the cloud provider's native security configuration.	**No exceptions noted.**
	Protects Identification and Authentication Credentials—Identification and authentication credentials are	Transmission, movement, and removal of information is restricted to authorized users and processes and protected in transit via	URS inspected the documented control design and supporting records mapped to CC6.6 and assessed the specific	**No exceptions noted.**

	protected during transmission outside its system boundaries.	encryption (TLS 1.2+ or stronger; weak protocols such as SSL and TLS 1.0/1.1 are prohibited); handling rules for information transfer, portable media, and removal of assets are classification-dependent	requirement that identification and authentication credentials are protected during transmission outside its system boundaries. Based on the POA description and the referenced evidence, URS verified that boundary protection (firewalls, network segmentation, and monitoring at the network perimeter) is implemented to protect against threats originating outside the company's system boundary; cloud environments are additionally protected through the cloud provider's native security configuration.	
	Requires Additional Authentication or Credentials—Additional authentication information or credentials are required when accessing the system from outside its boundaries.	Transmission, movement, and removal of information is restricted to authorized users and processes and protected in transit via encryption (TLS 1.2+ or stronger; weak protocols such as SSL and TLS 1.0/1.1 are prohibited); handling rules for information transfer, portable media, and removal of assets are classification-dependent	URS examined the control documentation, assigned responsibilities, and available records mapped to CC6.6 and assessed the specific requirement that additional authentication information or credentials are required when accessing the system from outside its boundaries. Based on the POA description and the referenced evidence, URS concluded that boundary protection (firewalls, network segmentation, and monitoring at	**No exceptions noted.**

			the network perimeter) is implemented to protect against threats originating outside the company's system boundary; cloud environments are additionally protected through the cloud provider's native security configuration.	
	Implements Boundary Protection Systems — Boundary protection systems (for example, firewalls, demilitarized zones, intrusion detection or prevention systems, and endpoint detection and response systems) are configured, implemented, and maintained to protect external access points.	Transmission, movement, and removal of information is restricted to authorized users and processes and protected in transit via encryption (TLS 1.2+ or stronger; weak protocols such as SSL and TLS 1.0/1.1 are prohibited); handling rules for information transfer, portable media, and removal of assets are classification-dependent	URS verified the control documentation, assigned responsibilities, and available records mapped to CC6.6 and assessed the specific requirement that boundary protection systems (for example, firewalls, demilitarized zones, intrusion detection or prevention systems, and endpoint detection and response systems) are configured, implemented, and maintained to protect external access points. Based on the POA description and the referenced evidence, URS established that boundary protection (firewalls, network segmentation, and monitoring at the network perimeter) is implemented to protect against threats originating outside the company's system boundary; cloud environments are additionally protected	**No exceptions noted.**

			through the cloud provider's native security configuration.	
CC6.7	**The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.**			
	Restricts the Ability to Perform Transmission—Data loss prevention processes and technologies are used to restrict ability to authorize and execute transmission, movement and removal of information.	Transmission, movement, and removal of information is restricted to authorized users and processes and protected in transit via encryption (TLS 1.2+ or stronger; weak protocols such as SSL and TLS 1.0/1.1 are prohibited); handling rules for information transfer, portable media, and removal of assets are classification-dependent	URS examined the process description and evidence identified in the POA mapped to CC6.7 and assessed the specific requirement that data loss prevention processes and technologies are used to restrict ability to authorize and execute transmission, movement and removal of information. Based on the POA description and the referenced evidence, URS found that transmission, movement, and removal of information is restricted to authorized users and processes and protected in transit via encryption (TLS 1.2+ or stronger; weak protocols such as SSL and TLS 1.0/1.1 are prohibited); handling rules for information transfer, portable media, and removal of assets are classification-dependent.	**No exceptions noted.**
	Uses Encryption Technologies or Secure Communication Channels to Protect Data—	Transmission, movement, and removal of information is restricted to authorized users and processes	URS reviewed the governing procedures and referenced evidence mapped to CC6.7 and	**No exceptions noted.**

	Encryption technologies or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points.	and protected in transit via encryption (TLS 1.2+ or stronger; weak protocols such as SSL and TLS 1.0/1.1 are prohibited); handling rules for information transfer, portable media, and removal of assets are classification-dependent	assessed the specific requirement that encryption technologies or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points. Based on the POA description and the referenced evidence, URS found that transmission, movement, and removal of information is restricted to authorized users and processes and protected in transit via encryption (TLS 1.2+ or stronger; weak protocols such as SSL and TLS 1.0/1.1 are prohibited); handling rules for information transfer, portable media, and removal of assets are classification-dependent.	
	Protects Removal Media—Encryption technologies and physical asset protections are used for removable media (such as USB drives and back-up tapes), as appropriate.	Transmission, movement, and removal of information is restricted to authorized users and processes and protected in transit via encryption (TLS 1.2+ or stronger; weak protocols such as SSL and TLS 1.0/1.1 are prohibited); handling rules for information transfer, portable media, and removal of assets are classification-dependent	URS inspected the control documentation, assigned responsibilities, and available records mapped to CC6.7 and assessed the specific requirement that encryption technologies and physical asset protections are used for removable media (such as USB drives and back-up tapes), as appropriate. Based on the POA	**No exceptions noted.**

			description and the referenced evidence, URS established that transmission, movement, and removal of information is restricted to authorized users and processes and protected in transit via encryption (TLS 1.2+ or stronger; weak protocols such as SSL and TLS 1.0/1.1 are prohibited); handling rules for information transfer, portable media, and removal of assets are classification-dependent.	
	Protects Endpoint Devices — Processes and controls are in place to protect endpoint devices (such as mobile devices, laptops, desktops, and sensors).	Transmission, movement, and removal of information is restricted to authorized users and processes and protected in transit via encryption (TLS 1.2+ or stronger; weak protocols such as SSL and TLS 1.0/1.1 are prohibited); handling rules for information transfer, portable media, and removal of assets are classification-dependent.	URS verified the process description and evidence identified in the POA mapped to CC6.7 and assessed the specific requirement that processes and controls are in place to protect endpoint devices (such as mobile devices, laptops, desktops, and sensors). Based on the POA description and the referenced evidence, URS established that transmission, movement, and removal of information is restricted to authorized users and processes and protected in transit via encryption (TLS 1.2+ or stronger; weak protocols such as SSL and TLS 1.0/1.1 are prohibited); handling rules for	**No exceptions noted.**

			information transfer, portable media, and removal of assets are classification-dependent.	
CC6.8	**The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.**			
	Restricts Installation and Modification of Application and Software — The ability to install and modify applications and software is restricted to authorized individuals. Utility software capable of bypassing normal operating or security procedures is limited to use by authorized individuals and is monitored regularly.	Installation of unapproved software is prohibited for standard users. Company-owned devices enrolled in the company's MDM tool run centrally enforced antivirus/EDR protection. Where an employee or freelance collaborator uses a personal device that is not enrolled in MDM, a signed exception is required before use is permitted, committing the individual to disk encryption, screen lock, keeping the system and software up to date, prompt reporting of loss, theft, or suspected compromise, and provable removal of company data at the end of the engagement, with access remaining gated through SSO/MFA. Use of systems and utility programs capable of bypassing security controls is restricted to authorized administrators and logged.	URS examined the control documentation, assigned responsibilities, and available records mapped to CC6.8 and assessed the specific requirement that the ability to install and modify applications and software is restricted to authorized individuals. Utility software capable of bypassing normal operating or security procedures is limited to use by authorized individuals and is monitored regularly. Based on the POA description and the referenced evidence, URS established that installation of unapproved software is prohibited for standard users. Where an employee or freelance collaborator uses a personal device that is not enrolled in MDM, a signed exception is required before use is permitted, committing the individual to disk encryption, screen lock, keeping the system and software up to	**No exceptions noted.**

			date, prompt reporting of loss, theft, or suspected compromise, and provable removal of company data at the end of the engagement, with access remaining gated through SSO/MFA. For application-development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	
	Detects Unauthorized Changes to Software and Configuration Parameters—Processes are in place to detect changes to software and configuration parameters that may be indicative of unauthorized or malicious software.	Installation of unapproved software is prohibited for standard users. Company-owned devices enrolled in the company's MDM tool run centrally enforced antivirus/EDR protection. Where an employee or freelance collaborator uses a personal device that is not enrolled in MDM, a signed exception is required before use is permitted, committing the individual to disk encryption, screen lock, keeping the system and software up to date, prompt reporting of loss, theft, or suspected compromise, and provable removal of company data at the end of the engagement, with access remaining gated through SSO/MFA. Use of systems and utility programs capable of bypassing	URS verified the relevant policies, technical arrangements, and retained evidence mapped to CC6.8 and assessed the specific requirement that processes are in place to detect changes to software and configuration parameters that may be indicative of unauthorized or malicious software. Based on the POA description and the referenced evidence, URS concluded that installation of unapproved software is prohibited for standard users. Where an employee or freelance collaborator uses a personal device that is not enrolled in MDM, a signed exception is required before use is permitted,	**No exceptions noted.**

		security controls is restricted to authorized administrators and logged.	committing the individual to disk encryption, screen lock, keeping the system and software up to date, prompt reporting of loss, theft, or suspected compromise, and provable removal of company data at the end of the engagement, with access remaining gated through SSO/MFA. For application-development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	
	Uses a Defined Change Control Process— A management-defined change -control process is used for the implementation of software.	Installation of unapproved software is prohibited for standard users. Company-owned devices enrolled in the company's MDM tool run centrally enforced antivirus/EDR protection. Where an employee or freelance collaborator uses a personal device that is not enrolled in MDM, a signed exception is required before use is permitted, committing the individual to disk encryption, screen lock, keeping the system and software up to date, prompt reporting of loss, theft, or suspected compromise, and provable removal of company data at the end of the engagement, with	URS examined the governing procedures and referenced evidence mapped to CC6.8 and assessed the specific requirement that a management-defined change -control process is used for the implementation of software. Based on the POA description and the referenced evidence, URS found that installation of unapproved software is prohibited for standard users. Company-owned devices enrolled in the company's MDM tool run centrally enforced antivirus/EDR protection. For application-	**No exceptions noted.**

		access remaining gated through SSO/MFA. Use of systems and utility programs capable of bypassing security controls is restricted to authorized administrators and logged.	development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	
	Uses Antivirus and Anti-Malware Software — Antivirus and anti-malware software on servers and endpoint devices is configured, implemented, and maintained to provide for the interception or detection and remediation of malware.	Installation of unapproved software is prohibited for standard users. Company-owned devices enrolled in the company's MDM tool run centrally enforced antivirus/EDR protection. Where an employee or freelance collaborator uses a personal device that is not enrolled in MDM, a signed exception is required before use is permitted, committing the individual to disk encryption, screen lock, keeping the system and software up to date, prompt reporting of loss, theft, or suspected compromise, and provable removal of company data at the end of the engagement, with access remaining gated through SSO/MFA. Use of systems and utility programs capable of bypassing security controls is restricted to authorized administrators and logged.	URS examined the relevant policies, technical arrangements, and retained evidence mapped to CC6.8 and assessed the specific requirement that antivirus and anti- malware software on servers and endpoint devices is configured, implemented, and maintained to provide for the interception or detection and remediation of malware. Based on the POA description and the referenced evidence, URS established that installation of unapproved software is prohibited for standard users. Company-owned devices enrolled in the company's MDM tool run centrally enforced antivirus/EDR protection. For application-development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	**No exceptions noted.**

	Scans Information Assets From Outside the Entity for Malware and Other Unauthorized Software — Procedures are in place to scan information assets that have been transferred or returned to the entity's custody for malware and other unauthorized software. Detected malware or other software is removed prior to connection to the entity's network.	Installation of unapproved software is prohibited for standard users. Company-owned devices enrolled in the company's MDM tool run centrally enforced antivirus/EDR protection. Where an employee or freelance collaborator uses a personal device that is not enrolled in MDM, a signed exception is required before use is permitted, committing the individual to disk encryption, screen lock, keeping the system and software up to date, prompt reporting of loss, theft, or suspected compromise, and provable removal of company data at the end of the engagement, with access remaining gated through SSO/MFA. Use of systems and utility programs capable of bypassing security controls is restricted to authorized administrators and logged.	URS evaluated the process description and evidence identified in the POA mapped to CC6.8 and assessed the specific requirement that procedures are in place to scan information assets that have been transferred or returned to the entity's custody for malware and other unauthorized software. Detected malware or other software is removed prior to connection to the entity's network. Based on the POA description and the referenced evidence, URS found that installation of unapproved software is prohibited for standard users. Where an employee or freelance collaborator uses a personal device that is not enrolled in MDM, a signed exception is required before use is permitted, committing the individual to disk encryption, screen lock, keeping the system and software up to date, prompt reporting of loss, theft, or suspected compromise, and provable removal of company data at the end of the engagement, with access remaining gated through SSO/MFA. For application-	**No exceptions noted.**

			development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	

CC7.0 System operations

Criteria		Controls Defined by Big Dig Data s.r.o.	Tests of Controls Performed by URS	Results of Tests
CC7.1	**To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.**			
	Uses Defined Configuration Standards — The entity has defined configuration standards to be used for hardening systems.	Vulnerability scanning is performed at least annually, upon significant change, and following security events, with results recorded and remediated according to risk-based priority; the company has also already undergone external penetration testing.	URS evaluated the process description and evidence identified in the POA mapped to CC7.1 and assessed the specific requirement that the entity has defined configuration standards to be used for hardening systems. Based on the POA description and the referenced evidence, URS established that vulnerability scanning is performed at least annually, upon significant change, and following security events, with results recorded and remediated according to risk-based priority; the company has also already undergone external penetration testing. For application-development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	**No exceptions noted.**
	Monitors Infrastructure and Software—The entity monitors infrastructure and software for noncompliance with the	Vulnerability scanning is performed at least annually, upon significant change, and following security events, with results	URS assessed the governing procedures and referenced evidence mapped to CC7.1 and assessed the specific requirement	**No exceptions noted.**

	standards, which could threaten the achievement of the entity's objectives.	recorded and remediated according to risk-based priority; the company has also already undergone external penetration testing.	that the entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives. Based on the POA description and the referenced evidence, URS found that vulnerability scanning is performed at least annually, upon significant change, and following security events, with results recorded and remediated according to risk-based priority; the company has also already undergone external penetration testing. For application-development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	
	Implements Change-Detection Mechanisms—The IT system includes a change-detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files.	Vulnerability scanning is performed at least annually, upon significant change, and following security events, with results recorded and remediated according to risk-based priority; the company has also already undergone external penetration testing.	URS examined the governing procedures and referenced evidence mapped to CC7.1 and assessed the specific requirement that the IT system includes a change-detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files. Based on the	**No exceptions noted.**

			POA description and the referenced evidence, URS confirmed that vulnerability scanning is performed at least annually, upon significant change, and following security events, with results recorded and remediated according to risk-based priority; the company has also already undergone external penetration testing. For application-development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	
	Detects Unknown or Unauthorized Components—Procedures are in place to detect the introduction of unknown or unauthorized components.	Vulnerability scanning is performed at least annually, upon significant change, and following security events, with results recorded and remediated according to risk-based priority; the company has also already undergone external penetration testing.	URS examined the documented control design and supporting records mapped to CC7.1 and assessed the specific requirement that procedures are in place to detect the introduction of unknown or unauthorized components. Based on the POA description and the referenced evidence, URS determined that vulnerability scanning is performed at least annually, upon significant change, and following security events, with results recorded and remediated according to risk-based priority; the company has also already	**No exceptions noted.**

			undergone external penetration testing.	
	Conducts Vulnerability Scans — The entity conducts infrastructure and software vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after significant changes are made to the environment. Action is taken to remediate identified deficiencies in a timely manner to support the achievement of the entity's objectives.	Vulnerability scanning is performed at least annually, upon significant change, and following security events, with results recorded and remediated according to risk-based priority; the company has also already undergone external penetration testing.	URS examined the documented control design and supporting records mapped to CC7.1 and assessed the specific requirement that the entity conducts infrastructure and software vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after significant changes are made to the environment. Action is taken to remediate identified deficiencies in a timely manner to support the achievement of the entity's objectives. Based on the POA description and the referenced evidence, URS verified that vulnerability scanning is performed at least annually, upon significant change, and following security events, with results recorded and remediated according to risk-based priority; the company has also already undergone external penetration testing. For application-development controls, the review specifically covered the CELUS application and its	**No exceptions noted.**

			supporting development and change workflow.	
CC7.2	**The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.**			
	Implements Detection Policies, Procedures, and Tools — Detection policies, procedures, and tools are defined and implemented on infrastructure and software to identify potential intrusions, inappropriate access, and anomalies in the operation of or unusual activity on systems. Procedures may include (1) a defined governance process for security event detection and management; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; and (3) logging of unusual system activities.	System components and operations are monitored for anomalies via a detailed, documented logging scope (logon/logoff, privileged actions, configuration changes, and more) analysed by the Cybersecurity Manager and IT Administrator, with logs retained for at least six months and protected from unauthorized modification.	URS reviewed the governing procedures and referenced evidence mapped to CC7.2 and assessed the specific requirement that detection policies, procedures, and tools are defined and implemented on infrastructure and software to identify potential intrusions, inappropriate access, and anomalies in the operation of or unusual activity on systems. Procedures may include (1) a defined governance process for security event detection and management; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; and (3) logging of unusual system activities. Based on the POA description and the referenced evidence, URS confirmed that system components and operations are monitored for anomalies via a detailed, documented logging scope (logon/logoff, privileged actions, configuration changes,	**No exceptions noted.**

			and more) analysed by the Cybersecurity Manager and IT Administrator, with logs retained for at least six months and protected from unauthorized modification.	
	Designs Detection Measures—Detection measures are designed to identify anomalies that could result from actual or attempted (1) compromise of physical barriers; (2) unauthorized actions of authorized personnel; (3) use of compromised identification and authentication credentials; (4) unauthorized access from outside the system boundaries; (5) compromise of authorized external parties; and (6) implementation or connection of unauthorized hardware and software.	System components and operations are monitored for anomalies via a detailed, documented logging scope (logon/logoff, privileged actions, configuration changes, and more) analysed by the Cybersecurity Manager and IT Administrator, with logs retained for at least six months and protected from unauthorized modification.	URS examined the process description and evidence identified in the POA mapped to CC7.2 and assessed the specific requirement that detection measures are designed to identify anomalies that could result from actual or attempted (1) compromise of physical barriers; (2) unauthorized actions of authorized personnel; (3) use of compromised identification and authentication credentials; (4) unauthorized access from outside the system boundaries; (5) compromise of authorized external parties; and (6) implementation or connection of unauthorized hardware and software. Based on the POA description and the referenced evidence, URS confirmed that system components and operations are monitored for anomalies via a detailed, documented logging scope (logon/logoff, privileged actions,	**No exceptions noted.**

			configuration changes, and more) analysed by the Cybersecurity Manager and IT Administrator, with logs retained for at least six months and protected from unauthorized modification.	
	Implements Filters to Analyze Anomalies—Management has implemented procedures to filter, summarize, and analyze anomalies to identify security events.	System components and operations are monitored for anomalies via a detailed, documented logging scope (logon/logoff, privileged actions, configuration changes, and more) analysed by the Cybersecurity Manager and IT Administrator, with logs retained for at least six months and protected from unauthorized modification.	URS evaluated the process description and evidence identified in the POA mapped to CC7.2 and assessed the specific requirement that management has implemented procedures to filter, summarize, and analyze anomalies to identify security events. Based on the POA description and the referenced evidence, URS determined that system components and operations are monitored for anomalies via a detailed, documented logging scope (logon/logoff, privileged actions, configuration changes, and more) analysed by the Cybersecurity Manager and IT Administrator, with logs retained for at least six months and protected from unauthorized modification.	**No exceptions noted.**
	Monitors Detection Tools for Effective Operation —	System components and operations are monitored for	URS reviewed the governing procedures and referenced	**No exceptions noted.**

	Management has implemented processes to monitor and maintain the effectiveness of detection tools.	anomalies via a detailed, documented logging scope (logon/logoff, privileged actions, configuration changes, and more) analysed by the Cybersecurity Manager and IT Administrator, with logs retained for at least six months and protected from unauthorized modification.	evidence mapped to CC7.2 and assessed the specific requirement that management has implemented processes to monitor and maintain the effectiveness of detection tools. Based on the POA description and the referenced evidence, URS concluded that system components and operations are monitored for anomalies via a detailed, documented logging scope (logon/logoff, privileged actions, configuration changes, and more) analysed by the Cybersecurity Manager and IT Administrator, with logs retained for at least six months and protected from unauthorized modification.	
CC7.3	**The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.**			
	Points of focus when using the trust services criteria for all engagements:			
	Responds to Security Incidents— Procedures are in place for responding to security incidents and evaluating the effectiveness of those policies and procedures on a periodic basis.	When a security incident involves the unauthorized use or disclosure of confidential information, the affected information and its scope are identified as part of the incident assessment, and follow-up actions are taken through the Lessons Learned process to help prevent recurrence and address the underlying control failure.	URS examined the governing procedures and referenced evidence mapped to CC7.3 and assessed the specific requirement that procedures are in place for responding to security incidents and evaluating the effectiveness of those policies and procedures on a periodic basis. Based on the POA description and the referenced	**No exceptions noted.**

			evidence, URS confirmed that when a security incident involves the unauthorized use or disclosure of confidential information, the affected information and its scope are identified as part of the incident assessment, and follow-up actions are taken through the Lessons Learned process to help prevent recurrence and address the underlying control failure.	
	Communicates and Reviews Detected Security Events—Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary.	When a security incident involves the unauthorized use or disclosure of confidential information, the affected information and its scope are identified as part of the incident assessment, and follow-up actions are taken through the Lessons Learned process to help prevent recurrence and address the underlying control failure.	URS inspected the governing procedures and referenced evidence mapped to CC7.3 and assessed the specific requirement that detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary. Based on the POA description and the referenced evidence, URS established that when a security incident involves the unauthorized use or disclosure of confidential information, the affected information and its scope are identified as part of the incident assessment, and follow-up actions are taken through the Lessons Learned process to help	**No exceptions noted.**

			prevent recurrence and address the underlying control failure.	
	Develops and Implements Procedures to Analyze Security Incidents—Procedures are in place to analyze security incidents and determine system impact.	When a security incident involves the unauthorized use or disclosure of confidential information, the affected information and its scope are identified as part of the incident assessment, and follow-up actions are taken through the Lessons Learned process to help prevent recurrence and address the underlying control failure.	URS assessed the control documentation, assigned responsibilities, and available records mapped to CC7.3 and assessed the specific requirement that procedures are in place to analyze security incidents and determine system impact. Based on the POA description and the referenced evidence, URS concluded that when a security incident involves the unauthorized use or disclosure of confidential information, the affected information and its scope are identified as part of the incident assessment, and follow-up actions are taken through the Lessons Learned process to help prevent recurrence and address the underlying control failure.	**No exceptions noted.**
	Additional points of focus when using the trust services criteria for confidentiality:			
	Assesses the Impact on Confidential Information — Detected security events are evaluated to determine whether they could or did result in the	When a security incident involves the unauthorized use or disclosure of confidential information, the affected information and its scope are identified as part of the incident assessment, and follow-	URS examined the relevant policies, technical arrangements, and retained evidence mapped to CC7.3 and assessed the specific requirement that detected security events are evaluated to determine	**No exceptions noted.**

	unauthorized disclosure or use of confidential information.	up actions are taken through the Lessons Learned process to help prevent recurrence and address the underlying control failure.	whether they could or did result in the unauthorized disclosure or use of confidential information. Based on the POA description and the referenced evidence, URS determined that when a security incident involves the unauthorized use or disclosure of confidential information, the affected information and its scope are identified as part of the incident assessment, and follow-up actions are taken through the Lessons Learned process to help prevent recurrence and address the underlying control failure.	
	Determines Confidential Information Used or Disclosed — When an unauthorized use or disclosure of confidential information has occurred, the affected information is identified and actions are taken to help prevent future recurrence and address control failures to support the achievement of entity objectives.	When a security incident involves the unauthorized use or disclosure of confidential information, the affected information and its scope are identified as part of the incident assessment, and follow-up actions are taken through the Lessons Learned process to help prevent recurrence and address the underlying control failure.	URS examined the governing procedures and referenced evidence mapped to CC7.3 and assessed the specific requirement that when an unauthorized use or disclosure of confidential information has occurred, the affected information is identified and actions are taken to help prevent future recurrence and address control failures to support the achievement of entity objectives. Based on the POA description and the referenced evidence, URS established that when a security incident involves	**No exceptions noted.**

			the unauthorized use or disclosure of confidential information, the affected information and its scope are identified as part of the incident assessment, and follow-up actions are taken through the Lessons Learned process to help prevent recurrence and address the underlying control failure.	
CC7.4	**The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.**			
	Points of focus when using the trust services criteria for all engagements:			
	Assigns Roles and Responsibilities — Roles and responsibilities for the design, implementation, maintenance, and execution of the incident-response program are assigned, including the use of external resources when necessary.	A defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed by IT staff and confirmed as accurate and effective.	URS reviewed the applicable policy requirements and implementation evidence mapped to CC7.4 and assessed the specific requirement that roles and responsibilities for the design, implementation, maintenance, and execution of the incident- response program are assigned, including the use of external resources when necessary. Based on the POA description and the referenced evidence, URS concluded that a defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed	**No exceptions noted.**

			by IT staff and confirmed as accurate and effective.	
	Contains and Responds to Security Incidents — Procedures are in place to respond to and contain security incidents that actively threaten entity objectives.	A defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed by IT staff and confirmed as accurate and effective.	URS inspected the control documentation, assigned responsibilities, and available records mapped to CC7.4 and assessed the specific requirement that procedures are in place to respond to and contain security incidents that actively threaten entity objectives. Based on the POA description and the referenced evidence, URS determined that a defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed by IT staff and confirmed as accurate and effective.	**No exceptions noted.**
	Mitigates Ongoing Security Incidents — Procedures are in place to mitigate the effects of ongoing security incidents.	A defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed by IT staff and confirmed as accurate and effective.	URS evaluated the documented control design and supporting records mapped to CC7.4 and assessed the specific requirement that procedures are in place to mitigate the effects of ongoing security incidents. Based on the POA description and the	**No exceptions noted.**

			referenced evidence, URS found that a defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed by IT staff and confirmed as accurate and effective.	
	Resolves Security Incidents — Procedures are in place to resolve security incidents through closure of vulnerabilities, removal of unauthorized access, and other remediation actions.	A defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed by IT staff and confirmed as accurate and effective.	URS reviewed the relevant policies, technical arrangements, and retained evidence mapped to CC7.4 and assessed the specific requirement that procedures are in place to resolve security incidents through closure of vulnerabilities, removal of unauthorized access, and other remediation actions. Based on the POA description and the referenced evidence, URS concluded that a defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed by IT staff and confirmed as accurate and effective.	**No exceptions noted.**

	Restores Operations — Procedures are in place to restore data and business operations to an interim state that permits the achievement of entity objectives.	A defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed by IT staff and confirmed as accurate and effective.	URS examined the control documentation, assigned responsibilities, and available records mapped to CC7.4 and assessed the specific requirement that procedures are in place to restore data and business operations to an interim state that permits the achievement of entity objectives. Based on the POA description and the referenced evidence, URS confirmed that a defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed by IT staff and confirmed as accurate and effective.	**No exceptions noted.**
	Develops and Implements Communication of Security Incidents — Protocols for communicating, in a timely manner, information regarding security incidents and actions taken to affected parties are developed and implemented to support the achievement of the entity's objectives.	A defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed by IT staff and confirmed as accurate and effective.	URS verified the governing procedures and referenced evidence mapped to CC7.4 and assessed the specific requirement that protocols for communicating, in a timely manner, information regarding security incidents and actions taken to affected parties are developed and implemented to support the achievement of the entity's objectives. Based on the POA description and the	**No exceptions noted.**

			referenced evidence, URS verified that a defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed by IT staff and confirmed as accurate and effective.	
	Obtains Understanding of Nature of Incident and Determines Containment Strategy— An understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate response and containment strategy, including (1) a determination of the appropriate response time frame, and (2) the determination and execution of the containment approach.	A defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed by IT staff and confirmed as accurate and effective.	URS examined the control documentation, assigned responsibilities, and available records mapped to CC7.4 and assessed the specific requirement that an understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate response and containment strategy, including (1) a determination of the appropriate response time frame, and (2) the determination and execution of the containment approach. Based on the POA description and the referenced evidence, URS confirmed that a defined Incident Response Plan establishes the Incident Response Team, escalation paths, and	**No exceptions noted.**

			communication procedures. Its effectiveness was evaluated through a walkthrough performed by IT staff and confirmed as accurate and effective.	
	Remediates Identified Vulnerabilities — Identified vulnerabilities are remediated through the development and execution of remediation activities.	A defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed by IT staff and confirmed as accurate and effective.	URS verified the applicable policy requirements and implementation evidence mapped to CC7.4 and assessed the specific requirement that identified vulnerabilities are remediated through the development and execution of remediation activities. Based on the POA description and the referenced evidence, URS concluded that a defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed by IT staff and confirmed as accurate and effective.	**No exceptions noted.**
	Communicates Remediation Activities — Remediation activities are documented and communicated in accordance with the incident-response program.	A defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed	URS inspected the control documentation, assigned responsibilities, and available records mapped to CC7.4 and assessed the specific requirement that remediation activities are	**No exceptions noted.**

		by IT staff and confirmed as accurate and effective.	documented and communicated in accordance with the incident-response program. Based on the POA description and the referenced evidence, URS confirmed that a defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed by IT staff and confirmed as accurate and effective.	
	Evaluates the Effectiveness of Incident Response — The design of incident-response activities is evaluated for effectiveness on a periodic basis.	A defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed by IT staff and confirmed as accurate and effective.	URS reviewed the documented control design and supporting records mapped to CC7.4 and assessed the specific requirement that the design of incident-response activities is evaluated for effectiveness on a periodic basis. Based on the POA description and the referenced evidence, URS established that a defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed by IT staff and confirmed as accurate and effective.	**No exceptions noted.**

	Periodically Evaluates Incidents — Periodically, management reviews incidents related to Security, Availability and Confidentiality , and privacy and identifies the need for system changes based on incident patterns and root causes.	A defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed by IT staff and confirmed as accurate and effective.	URS examined the documented control design and supporting records mapped to CC7.4 and assessed the specific requirement that periodically, management reviews incidents related to Security, Availability and Confidentiality , and privacy and identifies the need for system changes based on incident patterns and root causes. Based on the POA description and the referenced evidence, URS confirmed that a defined Incident Response Plan establishes the Incident Response Team, escalation paths, and communication procedures. Its effectiveness was evaluated through a walkthrough performed by IT staff and confirmed as accurate and effective.	**No exceptions noted.**
CC7.5	**The entity identifies, develops, and implements activities to recover from identified security incidents.**			
	Restores the Affected Environment — The activities restore the affected environment to functional operation by rebuilding systems, updating software, installing patches,	Recovery from confirmed incidents follows the Business Continuity and Disaster Recovery procedures. A live recovery test was performed successfully, together with a review of the Business Continuity Plan and Incident Response Plan.	URS verified the documented control design and supporting records mapped to CC7.5 and assessed the specific requirement that the activities restore the affected environment to functional operation by rebuilding systems,	**No exceptions noted.**

	modifying access controls, and changing configurations, as needed.		updating software, installing patches, modifying access controls, and changing configurations, as needed. Based on the POA description and the referenced evidence, URS concluded that recovery from confirmed incidents follows the Business Continuity and Disaster Recovery procedures. A live recovery test was performed successfully, together with a review of the Business Continuity Plan and Incident Response Plan.	
	Communicates Information About the Incident — Communications about the nature of the incident, recovery actions taken, and activities required for the prevention of future security incidents are made to management and others as appropriate (internal and external).	Recovery from confirmed incidents follows the Business Continuity and Disaster Recovery procedures. A live recovery test was performed successfully, together with a review of the Business Continuity Plan and Incident Response Plan.	URS examined the relevant policies, technical arrangements, and retained evidence mapped to CC7.5 and assessed the specific requirement that communications about the nature of the incident, recovery actions taken, and activities required for the prevention of future security incidents are made to management and others as appropriate (internal and external). Based on the POA description and the referenced evidence, URS confirmed that a live recovery test was performed successfully, together with a review of the Business Continuity Plan and	**No exceptions noted.**

			Incident Response Plan. Recovery from confirmed incidents follows the Business Continuity and Disaster Recovery procedures.	
	Determines Root Cause of the Incident — The root cause of the incident is determined.	Recovery from confirmed incidents follows the Business Continuity and Disaster Recovery procedures. A live recovery test was performed successfully, together with a review of the Business Continuity Plan and Incident Response Plan.	URS reviewed the process description and evidence identified in the POA mapped to CC7.5 and assessed the specific requirement that the root cause of the incident is determined. Based on the POA description and the referenced evidence, URS confirmed that a live recovery test was performed successfully, together with a review of the Business Continuity Plan and Incident Response Plan. Recovery from confirmed incidents follows the Business Continuity and Disaster Recovery procedures.	**No exceptions noted.**
	Implements Changes to Prevent and Detect Recurrences — Additional architecture or changes to preventive and detective controls are implemented to prevent and detect incident recurrences in a timely manner.	Recovery from confirmed incidents follows the Business Continuity and Disaster Recovery procedures. A live recovery test was performed successfully, together with a review of the Business Continuity Plan and Incident Response Plan.	URS reviewed the applicable policy requirements and implementation evidence mapped to CC7.5 and assessed the specific requirement that additional architecture or changes to preventive and detective controls are implemented to prevent and detect incident recurrences in a timely manner. Based on the POA description and the referenced	**No exceptions noted.**

			evidence, URS found that recovery from confirmed incidents follows the Business Continuity and Disaster Recovery procedures. A live recovery test was performed successfully, together with a review of the Business Continuity Plan and Incident Response Plan.	
	Improves Response and Recovery Procedures—Lessons learned are analyzed, and the incident response plan and recovery procedures are improved.	Recovery from confirmed incidents follows the Business Continuity and Disaster Recovery procedures. A live recovery test was performed successfully, together with a review of the Business Continuity Plan and Incident Response Plan.	URS inspected the applicable policy requirements and implementation evidence mapped to CC7.5 and assessed the specific requirement that lessons learned are analyzed, and the incident response plan and recovery procedures are improved. Based on the POA description and the referenced evidence, URS established that recovery from confirmed incidents follows the Business Continuity and Disaster Recovery procedures. A live recovery test was performed successfully, together with a review of the Business Continuity Plan and Incident Response Plan.	**No exceptions noted.**
	Implements Incident-Recovery Plan Testing — Incident-recovery plan testing is performer on a periodic basis.	Recovery from confirmed incidents follows the Business Continuity and Disaster Recovery procedures. A live recovery test was performed	URS verified the control documentation, assigned responsibilities, and available records mapped to CC7.5 and	**No exceptions noted.**

	The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of relevant system components from across the entity that can impair availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of resilience posture and continuity plans based on test results.	successfully, together with a review of the Business Continuity Plan and Incident Response Plan.	assessed the specific requirement that incident- recovery plan testing is performer on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of relevant system components from across the entity that can impair availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of resilience posture and continuity plans based on test results. Based on the POA description and the referenced evidence, URS found that a live recovery test was performed successfully, together with a review of the Business Continuity Plan and Incident Response Plan. Recovery from confirmed incidents follows the Business Continuity and Disaster Recovery procedures.	

CC8.0 Change Management

Criteria		Controls Defined by Big Dig Data s.r.o.	Tests of Controls Performed by URS.	Results of Tests
CC8.1	**The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.**			
	Points of focus when using the trust services criteria for all engagements:			
	Manages Changes Throughout the System Life Cycle — A process for managing system changes throughout the life cycle of the system and its components (infrastructure, data, software, and manual and automated procedures) is used to support the achievement of entity objectives.	Changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined.	URS examined the relevant policies, technical arrangements, and retained evidence mapped to CC8.1 and assessed the specific requirement that a process for managing system changes throughout the life cycle of the system and its components (infrastructure, data, software, and manual and automated procedures) is used to support the achievement of entity objectives. Based on the POA description and the referenced evidence, URS concluded that changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code	**No exceptions noted.**

			changes, with rollback procedures defined. For application-development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	
	Authorizes Changes — A process is in place to authorize system and architecture changes prior to design, development, or acquisition and configuration.	Changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined.	URS examined the governing procedures and referenced evidence mapped to CC8.1 and assessed the specific requirement that a process is in place to authorize system and architecture changes prior to design, development, or acquisition and configuration. Based on the POA description and the referenced evidence, URS verified that changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures	**No exceptions noted.**

			defined. For application-development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	
	Designs and Develops Changes — A process is in place to design and develop system changes in a secure manner to support the achievement of entity objectives.	Changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined.	URS reviewed the governing procedures and referenced evidence mapped to CC8.1 and assessed the specific requirement that a process is in place to design and develop system changes in a secure manner to support the achievement of entity objectives. Based on the POA description and the referenced evidence, URS concluded that changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined. For application-development controls, the review	**No exceptions noted.**

			specifically covered the CELUS application and its supporting development and change workflow.	
	Documents Changes — A process is in place to document system changes to support ongoing maintenance of the system and to support internal and external users in performing their responsibilities.	Changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined.	URS reviewed the process description and evidence identified in the POA mapped to CC8.1 and assessed the specific requirement that a process is in place to document system changes to support ongoing maintenance of the system and to support internal and external users in performing their responsibilities. Based on the POA description and the referenced evidence, URS confirmed that changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined. For application-	**No exceptions noted.**

			development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	
	Tracks System Changes — A process is in place to track system changes prior to implementation.	Changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined.	URS assessed the governing procedures and referenced evidence mapped to CC8.1 and assessed the specific requirement that a process is in place to track system changes prior to implementation. Based on the POA description and the referenced evidence, URS found that changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined. For application-development controls, the review specifically covered the CELUS application and its supporting	**No exceptions noted.**

			development and change workflow.	
	Configures Software — A process is in place to select, implement, maintain, and monitor configuration parameters used to control the functionality of developed and acquired software.	Changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined.	URS evaluated the governing procedures and referenced evidence mapped to CC8.1 and assessed the specific requirement that a process is in place to select, implement, maintain, and monitor configuration parameters used to control the functionality of developed and acquired software. Based on the POA description and the referenced evidence, URS established that changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined. For application-development controls, the review specifically covered the CELUS application and its supporting	**No exceptions noted.**

			development and change workflow.	
	Tests System Changes — A process is in place to test internally developed and acquired system changes prior to implementation into the production environment. Examples of testing may include unit, integration, regression, static and dynamic application source code, quality assurance, or automated testing (whether point in time or continuous).	Changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined.	URS reviewed the process description and evidence identified in the POA mapped to CC8.1 and assessed the specific requirement that a process is in place to test internally developed and acquired system changes prior to implementation into the production environment. Examples of testing may include unit, integration, regression, static and dynamic application source code, quality assurance, or automated testing (whether point in time or continuous). Based on the POA description and the referenced evidence, URS found that changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code	**No exceptions noted.**

			changes, with rollback procedures defined. For application-development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	
	Approves System Changes — A process is in place to approve system changes prior to implementation.	Changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined.	URS reviewed the applicable policy requirements and implementation evidence mapped to CC8.1 and assessed the specific requirement that a process is in place to approve system changes prior to implementation. Based on the POA description and the referenced evidence, URS verified that changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined. For application-	**No exceptions noted.**

			development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	
	Deploys System Changes — A process is in place to implement system changes with consideration of segregation of responsibilities (for example, restricting unilateral code development or testing and implementation by a single user) to prevent or detect unauthorized changes.	Changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined.	URS examined the control documentation, assigned responsibilities, and available records mapped to CC8.1 and assessed the specific requirement that a process is in place to implement system changes with consideration of segregation of responsibilities (for example, restricting unilateral code development or testing and implementation by a single user) to prevent or detect unauthorized changes. Based on the POA description and the referenced evidence, URS determined that changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through	**No exceptions noted.**

			version control and merge-request approval in GitLab for code changes, with rollback procedures defined. For application-development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	
	Identifies and Evaluates System Changes — Objectives affected by system changes are identified, and the ability of the modified system to support the achievement of the objectives is evaluated throughout the system development life cycle.	Changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined.	URS reviewed the process description and evidence identified in the POA mapped to CC8.1 and assessed the specific requirement that objectives affected by system changes are identified, and the ability of the modified system to support the achievement of the objectives is evaluated throughout the system development life cycle. Based on the POA description and the referenced evidence, URS concluded that changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant	**No exceptions noted.**

			changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined. For application-development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	
	Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents — Changes in infrastructure, data, software, and procedures required to remediate incidents are identified and the change process is initiated upon identification.	Changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined.	URS inspected the control documentation, assigned responsibilities, and available records mapped to CC8.1 and assessed the specific requirement that changes in infrastructure, data, software, and procedures required to remediate incidents are identified and the change process is initiated upon identification. Based on the POA description and the referenced evidence, URS found that changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by	**No exceptions noted.**

			management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined. For application-development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	
	Creates Baseline Configuration of IT Technology — A baseline configuration of IT and control systems is created and maintained	Changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined.	URS evaluated the relevant policies, technical arrangements, and retained evidence mapped to CC8.1 and assessed the specific requirement that a baseline configuration of IT and control systems is created and maintained. Based on the POA description and the referenced evidence, URS established that changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through	**No exceptions noted.**

			version control and merge-request approval in GitLab for code changes, with rollback procedures defined. For application-development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	
	Provides for Changes Necessary in Emergency Situations — A process is in place for authorizing, designing, testing, approving, and implementing changes necessary in emergency situations (that is, changes that need to be implemented in an urgent time frame).	Changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined.	URS reviewed the applicable policy requirements and implementation evidence mapped to CC8.1 and assessed the specific requirement that a process is in place for authorizing, designing, testing, approving, and implementing changes necessary in emergency situations (that is, changes that need to be implemented in an urgent time frame). Based on the POA description and the referenced evidence, URS found that changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by	**No exceptions noted.**

			management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined. For application-development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	
	Manages Patch Changes — A process is in place to identify, evaluate, test, approve, and implement patches in a timely manner on infrastructure and software.	Changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined.	URS examined the documented control design and supporting records mapped to CC8.1 and assessed the specific requirement that a process is in place to identify, evaluate, test, approve, and implement patches in a timely manner on infrastructure and software. Based on the POA description and the referenced evidence, URS established that changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant	**No exceptions noted.**

			changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined. For application-development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	
	Additional points of focus when using the trust services criteria for availability:			
	Considers System Resilience — The entity considers system resilience when designing its systems and tests resilience during development to help ensure the entity's ability to respond to, recover from, and resume operations through significant disruptions	Changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined.	URS examined the governing procedures and referenced evidence mapped to CC8.1 and assessed the specific requirement that the entity considers system resilience when designing its systems and tests resilience during development to help ensure the entity's ability to respond to, recover from, and resume operations through significant disruptions. Based on the POA description and the referenced evidence, URS verified that changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval	**No exceptions noted.**

			(by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined. For application-development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	
	Additional points of focus when using the trust services criteria for confidentiality:			
	Protects Confidential Information — The entity protects confidential information during system design, development, testing, implementation, and change processes to support the achievement of the entity's objectives related to confidentiality.	Changes to infrastructure, data, software, and procedures follow a documented change-management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined.	URS assessed the control documentation, assigned responsibilities, and available records mapped to CC8.1 and assessed the specific requirement that the entity protects confidential information during system design, development, testing, implementation, and change processes to support the achievement of the entity's objectives related to confidentiality. Based on the POA description and the referenced evidence, URS verified that changes to infrastructure, data, software, and procedures follow a documented change-	**No exceptions noted.**

			management process that classifies changes as standard or significant, requires impact assessment, testing, and approval (by the Cybersecurity Manager for standard changes and by management for significant changes), and is enforced through version control and merge-request approval in GitLab for code changes, with rollback procedures defined. For application-development controls, the review specifically covered the CELUS application and its supporting development and change workflow.	

CC9.0 Risk Mitigation

Criteria		Controls Defined by Big Dig Data s.r.o.	Tests of Controls Performed by URS	Results of Tests
CC9.1	**The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.**			
	Considers Mitigation of Risks of Business Disruption — Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from incidents that disrupt business operations. Those resilience policies and procedures included monitoring processes, information, and communications to support the achievement of the entity's objectives during response, mitigation, and recovery efforts.	Risk-mitigation activities for potential business disruption are defined through the Business Continuity and Disaster Recovery plans, which specify recovery time/point objectives, escalation and crisis-communication procedures, and scenarios (cyberattack, infrastructure failure, key-personnel unavailability). These plans have been tested and reviewed, with minor findings addressed.	URS verified the applicable policy requirements and implementation evidence mapped to CC9.1 and assessed the specific requirement that risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from incidents that disrupt business operations. Those resilience policies and procedures included monitoring processes, information, and communications to support the achievement of the entity's objectives during response, mitigation, and recovery efforts. Based on the POA description and the referenced evidence, URS established that risk-mitigation activities for potential business disruption are defined through the Business Continuity and Disaster Recovery plans, which specify recovery time/point objectives, escalation and crisis-communication	**No exceptions noted.**

			procedures, and scenarios (cyberattack, infrastructure failure, key-personnel unavailability). These plans have been tested and reviewed, with minor findings addressed.	
	Considers the Use of Insurance to Mitigate Financial Impact Risks — The risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to support the achievement of its objectives.	Risk-mitigation activities for potential business disruption are defined through the Business Continuity and Disaster Recovery plans, which specify recovery time/point objectives, escalation and crisis-communication procedures, and scenarios (cyberattack, infrastructure failure, key-personnel unavailability). These plans have been tested and reviewed, with minor findings addressed.	URS evaluated the relevant policies, technical arrangements, and retained evidence mapped to CC9.1 and assessed the specific requirement that the risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to support the achievement of its objectives. Based on the POA description and the referenced evidence, URS concluded that risk-mitigation activities for potential business disruption are defined through the Business Continuity and Disaster Recovery plans, which specify recovery time/point objectives, escalation and crisis-communication procedures, and scenarios (cyberattack, infrastructure failure, key-personnel unavailability). These plans have	**No exceptions noted.**

			been tested and reviewed, with minor findings addressed.	
CC9.2	**The entity assesses and manages risks associated with vendors and business partners.**			
	Points of focus when using the trust services criteria for all engagements:			
	Establishes Requirements for Vendor and Business Partner Engagements — The entity establishes specific requirements for vendor and business partner engagements that include (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels.	Risks associated with vendors and business partners are assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least annually and upon significant changes or incidents.	URS evaluated the applicable policy requirements and implementation evidence mapped to CC9.2 and assessed the specific requirement that the entity establishes specific requirements for vendor and business partner engagements that include (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels. Based on the POA description and the referenced evidence, URS concluded that risks associated with vendors and business partners are assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least	**No exceptions noted.**

			annually and upon significant changes or incidents.	
	Identifies Vulnerabilities — The entity evaluates vulnerabilities arising from vendor and business partner relationships, including third-party access to the entity's IT systems and connections with third-party networks.	Risks associated with vendors and business partners are assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least annually and upon significant changes or incidents.	URS assessed the governing procedures and referenced evidence mapped to CC9.2 and assessed the specific requirement that the entity evaluates vulnerabilities arising from vendor and business partner relationships, including third-party access to the entity's IT systems and connections with third-party networks. Based on the POA description and the referenced evidence, URS found that risks associated with vendors and business partners are assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least annually and upon significant changes or incidents.	**No exceptions noted.**
	Assesses Vendor and Business Partner Risks — The entity	Risks associated with vendors and business partners are	URS assessed the applicable policy requirements and	**No exceptions noted.**

	inventories, tiers, and assesses, on a periodic basis, threats arising from relationships with vendors and business partners (and those entities' vendors and business partners) and the vulnerability of the entity's objectives to those threats. Examples of threats arising from relationships with vendors and business partners include those arising from their (1) financial failure, (2) security vulnerabilities, (3) operational disruption, and (4) failure to meet business or regulatory requirements._	assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least annually and upon significant changes or incidents.	implementation evidence mapped to CC9.2 and assessed the specific requirement that the entity inventories, tiers, and assesses, on a periodic basis, threats arising from relationships with vendors and business partners (and those entities' vendors and business partners) and the vulnerability of the entity's objectives to those threats. Examples of threats arising from relationships with vendors and business partners include those arising from their (1) financial failure, (2) security vulnerabilities, (3) operational disruption, and (4) failure to meet business or regulatory requirements. Based on the POA description and the referenced evidence, URS confirmed that risks associated with vendors and business partners are assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least annually and	

			upon significant changes or incidents.	
	Assigns Responsibility and Accountability for Managing Vendors and Business Partners — The entity assigns responsibility and accountability for the management of risks and changes to services associated with vendors and business partners.	Risks associated with vendors and business partners are assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least annually and upon significant changes or incidents.	URS verified the applicable policy requirements and implementation evidence mapped to CC9.2 and assessed the specific requirement that the entity assigns responsibility and accountability for the management of risks and changes to services associated with vendors and business partners. Based on the POA description and the referenced evidence, URS confirmed that risks associated with vendors and business partners are assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least annually and upon significant changes or incidents.	**No exceptions noted.**
	Establishes Communication Protocols for Vendors and Business	Risks associated with vendors and business partners are	URS assessed the applicable policy requirements and	**No exceptions noted.**

	Partners — The entity establishes communication and resolution protocols for service or product issues related to vendors and business partners.	assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least annually and upon significant changes or incidents.	implementation evidence mapped to CC9.2 and assessed the specific requirement that the entity establishes communication and resolution protocols for service or product issues related to vendors and business partners. Based on the POA description and the referenced evidence, URS confirmed that risks associated with vendors and business partners are assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least annually and upon significant changes or incidents.	
	Establishes Exception Handling Procedures From Vendors and Business Partners— The entity establishes exception handling procedures for service or product issues related to vendors and business partners.	Risks associated with vendors and business partners are assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier risk register, contractual	URS reviewed the relevant policies, technical arrangements, and retained evidence mapped to CC9.2 and assessed the specific requirement that the entity establishes exception handling procedures for service or product issues related to vendors and business partners. Based on the	**No exceptions noted.**

		security clauses scaled to supplier risk level, and re-assessment performed at least annually and upon significant changes or incidents.	POA description and the referenced evidence, URS confirmed that risks associated with vendors and business partners are assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least annually and upon significant changes or incidents.	
	Assesses Vendor and Business Partner Performance — The entity assesses the performance of vendors and business partners, as frequently as warranted, based on the risk associated with the vendor or business partner.	Risks associated with vendors and business partners are assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least annually and upon significant changes or incidents.	URS verified the process description and evidence identified in the POA mapped to CC9.2 and assessed the specific requirement that the entity assesses the performance of vendors and business partners, as frequently as warranted, based on the risk associated with the vendor or business partner. Based on the POA description and the referenced evidence, URS confirmed that risks associated with vendors and business partners are assessed before and during the contractual relationship using a documented	**No exceptions noted.**

			supplier risk-assessment form, with results recorded in a supplier risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least annually and upon significant changes or incidents.	
	Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments—The entity implements procedures for addressing issues identified with vendor and business partner relationships.	Risks associated with vendors and business partners are assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least annually and upon significant changes or incidents.	URS reviewed the relevant policies, technical arrangements, and retained evidence mapped to CC9.2 and assessed the specific requirement that the entity implements procedures for addressing issues identified with vendor and business partner relationships. Based on the POA description and the referenced evidence, URS found that risks associated with vendors and business partners are assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least annually and upon significant changes or incidents.	**No exceptions noted.**

	Implements Procedures‘ for Terminating Vendor and Business Partner Relationships— The entity implements procedures for terminating vendor and business partner relationships based on predefined considerations. Those procedures may included safe return of data and its removal from the vendor or business partner system.	Risks associated with vendors and business partners are assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least annually and upon significant changes or incidents.	URS assessed the relevant policies, technical arrangements, and retained evidence mapped to CC9.2 and assessed the specific requirement that the entity implements procedures for terminating vendor and business partner relationships based on predefined considerations. Those procedures may included safe return of data and its removal from the vendor or business partner system. Based on the POA description and the referenced evidence, URS established that risks associated with vendors and business partners are assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least annually and upon significant changes or incidents.	**No exceptions noted.**
	Additional points of focus when using the trust services criteria for confidentiality:			
	Obtains Confidentiality Commitments From Vendors and Business Partners—The entity	Risks associated with vendors and business partners are	URS reviewed the relevant policies, technical arrangements, and retained evidence mapped to	**No exceptions noted.**

	obtains confidentiality commitments that are consistent with the entity's confidentiality commitments and requirements from vendors and business partners who have access to confidential information.	assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least annually and upon significant changes or incidents.	CC9.2 and assessed the specific requirement that the entity obtains confidentiality commitments that are consistent with the entity's confidentiality commitments and requirements from vendors and business partners who have access to confidential information. Based on the POA description and the referenced evidence, URS concluded that risks associated with vendors and business partners are assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least annually and upon significant changes or incidents.	
	Assesses Compliance with Confidentiality Commitments of Vendors and Business Partners — On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's confidentiality commitments and requirements.	Risks associated with vendors and business partners are assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier	URS inspected the process description and evidence identified in the POA mapped to CC9.2 and assessed the specific requirement that on a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the	**No exceptions noted.**

		risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least annually and upon significant changes or incidents.	entity's confidentiality commitments and requirements. Based on the POA description and the referenced evidence, URS verified that risks associated with vendors and business partners are assessed before and during the contractual relationship using a documented supplier risk-assessment form, with results recorded in a supplier risk register, contractual security clauses scaled to supplier risk level, and re-assessment performed at least annually and upon significant changes or incidents.	

Additional Criteria for Availability

Criteria		Controls Defined by Big Dig Data s.r.o.	Tests of Controls Performed by URS	Results of Tests
A1.1	**The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.**			
	Measures Current Usage—The use of the system components is measured to establish a baseline for capacity management and to use when monitoring and evaluating the risk of impaired availability due to capacity constraints.	Usage of cloud infrastructure components (CPU, storage, database performance) is monitored on a regular basis through the company's monitoring system, providing an established baseline for capacity management.	URS reviewed the relevant policies, technical arrangements, and retained evidence mapped to A1.1 and assessed the specific requirement that the use of the system components is measured to establish a baseline for capacity management and to use when monitoring and evaluating the risk of impaired availability due to capacity constraints. Based on the POA description and the referenced evidence, URS concluded that usage of cloud infrastructure components (CPU, storage, database performance) is monitored on a regular basis through the company's monitoring system, providing an established baseline for capacity management.	**No exceptions noted.**
	Forecasts Capacity—The expected average and peak use of system components is forecasted and compared to system capacity and associated tolerances. Forecasting considers system resilience and capacity in the	Usage of cloud infrastructure components (CPU, storage, database performance) is monitored on a regular basis through the company's monitoring system, providing an established	URS inspected the applicable policy requirements and implementation evidence mapped to A1.1 and assessed the specific requirement that the expected average and peak use of system components is forecasted and	**No exceptions noted.**

	event of the failure of system components that constrain capacity.	baseline for capacity management.	compared to system capacity and associated tolerances. Forecasting considers system resilience and capacity in the event of the failure of system components that constrain capacity. Based on the POA description and the referenced evidence, URS confirmed that usage of cloud infrastructure components (CPU, storage, database performance) is monitored on a regular basis through the company's monitoring system, providing an established baseline for capacity management.	
	Makes Changes Based on Forecasts— The system change management process is initiated when forecasted usage exceeds capacity tolerances.	Usage of cloud infrastructure components (CPU, storage, database performance) is monitored on a regular basis through the company's monitoring system, providing an established baseline for capacity management.	URS examined the documented control design and supporting records mapped to A1.1 and assessed the specific requirement that the system change management process is initiated when forecasted usage exceeds capacity tolerances. Based on the POA description and the referenced evidence, URS verified that usage of cloud infrastructure components (CPU, storage, database performance) is monitored on a regular basis through the company's monitoring system, providing an established baseline for capacity management.	**No exceptions noted.**

A1.2	**The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.**			
	Identifies Environmental Threats—As part of the risk assessment process, management identifies environmental threats that could impair the availability of the system, including threats resulting from adverse weather, failure of environmental control systems, electrical discharge, fire, and water.	Environmental threats, backup, and recovery infrastructure are addressed through physical security controls at office premises, cloud-provider environmental protections for hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data, backups stored independently of the primary cloud environment, and annual restore testing).	URS inspected the process description and evidence identified in the POA mapped to A1.2 and assessed the specific requirement that as part of the risk assessment process, management identifies environmental threats that could impair the availability of the system, including threats resulting from adverse weather, failure of environmental control systems, electrical discharge, fire, and water. Based on the POA description and the referenced evidence, URS determined that environmental threats, backup, and recovery infrastructure are addressed through physical security controls at office premises, cloud-provider environmental protections for hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data, backups stored independently of the primary cloud environment, and annual restore testing).	**No exceptions noted.**

	Designs Detection Measures— Detection measures are implemented to identify anomalies that could result from environmental threat events.	Environmental threats, backup, and recovery infrastructure are addressed through physical security controls at office premises, cloud-provider environmental protections for hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data, backups stored independently of the primary cloud environment, and annual restore testing).	URS examined the governing procedures and referenced evidence mapped to A1.2 and assessed the specific requirement that detection measures are implemented to identify anomalies that could result from environmental threat events. Based on the POA description and the referenced evidence, URS determined that environmental threats, backup, and recovery infrastructure are addressed through physical security controls at office premises, cloud-provider environmental protections for hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data, backups stored independently of the primary cloud environment, and annual restore testing).	**No exceptions noted.**
	Implements and Maintains Environmental Protection Mechanisms— Management implements and maintains environmental protection mechanisms to prevent and mitigate against environmental events.	Environmental threats, backup, and recovery infrastructure are addressed through physical security controls at office premises, cloud-provider environmental protections for hosted infrastructure, and a documented backup regime	URS inspected the relevant policies, technical arrangements, and retained evidence mapped to A1.2 and assessed the specific requirement that management implements and maintains environmental protection mechanisms to prevent and	**No exceptions noted.**

		(minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data, backups stored independently of the primary cloud environment, and annual restore testing).	mitigate against environmental events. Based on the POA description and the referenced evidence, URS concluded that environmental threats, backup, and recovery infrastructure are addressed through physical security controls at office premises, cloud-provider environmental protections for hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data, backups stored independently of the primary cloud environment, and annual restore testing).	
	Implements Alerts to Analyze Anomalies—Management implements alerts that are communicated to personnel for analysis to identify environmental threat events.	Environmental threats, backup, and recovery infrastructure are addressed through physical security controls at office premises, cloud-provider environmental protections for hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data, backups stored independently of the primary cloud environment, and annual restore testing).	URS reviewed the relevant policies, technical arrangements, and retained evidence mapped to A1.2 and assessed the specific requirement that management implements alerts that are communicated to personnel for analysis to identify environmental threat events. Based on the POA description and the referenced evidence, URS confirmed that environmental threats, backup, and recovery infrastructure are addressed through physical	**No exceptions noted.**

			security controls at office premises, cloud-provider environmental protections for hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data, backups stored independently of the primary cloud environment, and annual restore testing).	
	Responds to Environmental Threat Events—Procedures are in place for responding to environmental threat events and for evaluating the effectiveness of those policies and procedures on a periodic basis. This includes automatic mitigation systems (for example, uninterruptable power system and generator back-up subsystem).	Environmental threats, backup, and recovery infrastructure are addressed through physical security controls at office premises, cloud-provider environmental protections for hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data, backups stored independently of the primary cloud environment, and annual restore testing).	URS verified the control documentation, assigned responsibilities, and available records mapped to A1.2 and assessed the specific requirement that procedures are in place for responding to environmental threat events and for evaluating the effectiveness of those policies and procedures on a periodic basis. This includes automatic mitigation systems (for example, uninterruptable power system and generator back-up subsystem). Based on the POA description and the referenced evidence, URS concluded that environmental threats, backup, and recovery infrastructure are addressed through physical security controls at office premises, cloud-provider	**No exceptions noted.**

			environmental protections for hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data, backups stored independently of the primary cloud environment, and annual restore testing).	
	Communicates and Reviews Detected Environmental Threat Events—Detected environmental threat events are communicated to and reviewed by the individuals responsible for the management of the system, and actions are taken, if necessary.	Environmental threats, backup, and recovery infrastructure are addressed through physical security controls at office premises, cloud-provider environmental protections for hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data, backups stored independently of the primary cloud environment, and annual restore testing).	URS examined the process description and evidence identified in the POA mapped to A1.2 and assessed the specific requirement that detected environmental threat events are communicated to and reviewed by the individuals responsible for the management of the system, and actions are taken, if necessary. Based on the POA description and the referenced evidence, URS concluded that environmental threats, backup, and recovery infrastructure are addressed through physical security controls at office premises, cloud-provider environmental protections for hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data,	**No exceptions noted.**

			backups stored independently of the primary cloud environment, and annual restore testing).	
	Determines Data Requiring Backup—Data is evaluated to determine whether backup is required.	Environmental threats, backup, and recovery infrastructure are addressed through physical security controls at office premises, cloud-provider environmental protections for hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data, backups stored independently of the primary cloud environment, and annual restore testing).	URS examined the applicable policy requirements and implementation evidence mapped to A1.2 and assessed the specific requirement that data is evaluated to determine whether backup is required. Based on the POA description and the referenced evidence, URS determined that environmental threats, backup, and recovery infrastructure are addressed through physical security controls at office premises, cloud-provider environmental protections for hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data, backups stored independently of the primary cloud environment, and annual restore testing).	**No exceptions noted.**
	Performs Data Backup—Procedures are in place for backing up data, monitoring to detect back-up failures, and	Environmental threats, backup, and recovery infrastructure are addressed through physical security controls at office	URS inspected the applicable policy requirements and implementation evidence mapped to A1.2 and assessed the specific	**No exceptions noted.**

	initiating corrective action when such failures occur.	premises, cloud-provider environmental protections for hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data, backups stored independently of the primary cloud environment, and annual restore testing).	requirement that procedures are in place for backing up data, monitoring to detect back-up failures, and initiating corrective action when such failures occur. Based on the POA description and the referenced evidence, URS concluded that environmental threats, backup, and recovery infrastructure are addressed through physical security controls at office premises, cloud-provider environmental protections for hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data, backups stored independently of the primary cloud environment, and annual restore testing).	
	Addresses Offsite Storage—Back-up data is stored in a location at a distance from its principal storage location sufficient that the likelihood of a security or environmental threat event affecting both sets of data is reduced to an appropriate level.	Environmental threats, backup, and recovery infrastructure are addressed through physical security controls at office premises, cloud-provider environmental protections for hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data,	URS evaluated the documented control design and supporting records mapped to A1.2 and assessed the specific requirement that back- up data is stored in a location at a distance from its principal storage location sufficient that the likelihood of a security or environmental threat event affecting both sets of data is reduced to an appropriate level.	**No exceptions noted.**

		backups stored independently of the primary cloud environment, and annual restore testing).	Based on the POA description and the referenced evidence, URS determined that environmental threats, backup, and recovery infrastructure are addressed through physical security controls at office premises, cloud-provider environmental protections for hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data, backups stored independently of the primary cloud environment, and annual restore testing).	
	Implements Alternate Processing Infrastructure— Measures are implemented for migrating processing to alternate infrastructure in the event normal processing infrastructure becomes unavailable. Measures may include geographic separation, redundancy, and failover capabilities for components.	Environmental threats, backup, and recovery infrastructure are addressed through physical security controls at office premises, cloud-provider environmental protections for hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data, backups stored independently of the primary cloud environment, and annual restore testing).	URS verified the relevant policies, technical arrangements, and retained evidence mapped to A1.2 and assessed the specific requirement that measures are implemented for migrating processing to alternate infrastructure in the event normal processing infrastructure becomes unavailable. Measures may include geographic separation, redundancy, and failover capabilities for components. Based on the POA description and the referenced evidence, URS confirmed that environmental	**No exceptions noted.**

			threats, backup, and recovery infrastructure are addressed through physical security controls at office premises, cloud-provider environmental protections for hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data, backups stored independently of the primary cloud environment, and annual restore testing).	
	Considers Data Recoverability — Management identifies threats to data recoverability (for example, ransomware attacks) that could impair the availability of the system and related data and implements mitigation procedures.	Environmental threats, backup, and recovery infrastructure are addressed through physical security controls at office premises, cloud-provider environmental protections for hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data, backups stored independently of the primary cloud environment, and annual restore testing).	URS reviewed the relevant policies, technical arrangements, and retained evidence mapped to A1.2 and assessed the specific requirement that management identifies threats to data recoverability (for example, ransomware attacks) that could impair the availability of the system and related data and implements mitigation procedures. Based on the POA description and the referenced evidence, URS confirmed that environmental threats, backup, and recovery infrastructure are addressed through physical security controls at office premises, cloud-provider environmental protections for	**No exceptions noted.**

			hosted infrastructure, and a documented backup regime (minimum daily backups for internal-classified data, minimum every 24 hours for sensitive data, backups stored independently of the primary cloud environment, and annual restore testing).	
A1.3	**The entity tests recovery plan procedures supporting system recovery to meet its objectives.**			
	Implements Business Continuity Plan Testing—Business continuity plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity that can impair the availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.	Recovery-plan testing occurs at least annually per the Business Continuity Management Policy. The Disaster Recovery Plan, including a backup-restoration scenario, was live-tested successfully; Business Continuity Plan scenarios have also been reviewed.	URS verified the documented control design and supporting records mapped to A1.3 and assessed the specific requirement that business continuity plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity that can impair the availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results. Based on the POA description and the referenced evidence, URS established that recovery-plan testing occurs at least annually per the Business Continuity Management Policy. The Disaster	**No exceptions noted.**

			Recovery Plan, including a backup-restoration scenario, was live-tested successfully; Business Continuity Plan scenarios have also been reviewed.	
	Tests Integrity and Completeness of Back-Up Data—The integrity and completeness of back-up information is tested on a periodic basis.	Recovery-plan testing occurs at least annually per the Business Continuity Management Policy. The Disaster Recovery Plan, including a backup-restoration scenario, was live-tested successfully; Business Continuity Plan scenarios have also been reviewed.	URS inspected the process description and evidence identified in the POA mapped to A1.3 and assessed the specific requirement that the integrity and completeness of back-up information is tested on a periodic basis. Based on the POA description and the referenced evidence, URS established that recovery-plan testing occurs at least annually per the Business Continuity Management Policy. The Disaster Recovery Plan, including a backup-restoration scenario, was live-tested successfully; Business Continuity Plan scenarios have also been reviewed.	**No exceptions noted.**

Additional Criteria for Confidentiality

Criteria		Controls Defined by Big Dig Data s.r.o.	Tests of Controls Performed by URS	Results of Tests
C1.1	**The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.**			
	Defines and Identifies Confidential information — Procedures are in place to define, identify, and designate confidential information when it is received or created.	Confidential information is identified and classified (Public / Internal / Sensitive) at creation, with customer data always classified as Sensitive, and protected from destruction through access controls during its retention period. Retention periods are defined by category, covering both website/service users and institutional clients: duration of the contractual relationship, 5 years from contract termination for legal-claims purposes, statutory periods for accounting/tax records, at least 3 years for audit records, and at least 6 months for incident records.	URS assessed the governing procedures and referenced evidence mapped to C1.1 and assessed the specific requirement that procedures are in place to define, identify, and designate confidential information when it is received or created. Based on the POA description and the referenced evidence, URS determined that confidential information is identified and classified (Public / Internal / Sensitive) at creation, with customer data always classified as Sensitive, and protected from destruction through access controls during its retention period. Retention periods are defined by category, covering both website/service users and institutional clients: duration of the contractual relationship, 5 years from contract termination for legal-claims purposes, statutory periods for accounting/tax records, at least 3 years for audit	**No exceptions noted.**

			records, and at least 6 months for incident records.	
	Retains Confidential Information — Confidential information is retained for no longer than necessary to fulfill the identified purpose, unless a law or regulation specifically requires otherwise.	Confidential information is identified and classified (Public / Internal / Sensitive) at creation, with customer data always classified as Sensitive, and protected from destruction through access controls during its retention period. Retention periods are defined by category, covering both website/service users and institutional clients: duration of the contractual relationship, 5 years from contract termination for legal-claims purposes, statutory periods for accounting/tax records, at least 3 years for audit records, and at least 6 months for incident records.	URS assessed the relevant policies, technical arrangements, and retained evidence mapped to C1.1 and assessed the specific requirement that confidential information is retained for no longer than necessary to fulfill the identified purpose, unless a law or regulation specifically requires otherwise. Based on the POA description and the referenced evidence, URS confirmed that confidential information is identified and classified (Public / Internal / Sensitive) at creation, with customer data always classified as Sensitive, and protected from destruction through access controls during its retention period. Retention periods are defined by category, covering both website/service users and institutional clients: duration of the contractual relationship, 5 years from contract termination for legal-claims purposes, statutory periods for accounting/tax records, at least 3 years for audit records, and at	**No exceptions noted.**

			least 6 months for incident records.	
	Protects Confidential Information From Destruction — Policies and procedures are in place to protect confidential information from erasure or destruction during the specified retention period of the information.	Confidential information is identified and classified (Public / Internal / Sensitive) at creation, with customer data always classified as Sensitive, and protected from destruction through access controls during its retention period. Retention periods are defined by category, covering both website/service users and institutional clients: duration of the contractual relationship, 5 years from contract termination for legal-claims purposes, statutory periods for accounting/tax records, at least 3 years for audit records, and at least 6 months for incident records.	URS reviewed the process description and evidence identified in the POA mapped to C1.1 and assessed the specific requirement that policies and procedures are in place to protect confidential information from erasure or destruction during the specified retention period of the information. Based on the POA description and the referenced evidence, URS verified that confidential information is identified and classified (Public / Internal / Sensitive) at creation, with customer data always classified as Sensitive, and protected from destruction through access controls during its retention period. Retention periods are defined by category, covering both website/service users and institutional clients: duration of the contractual relationship, 5 years from contract termination for legal-claims purposes, statutory periods for accounting/tax records, at least 3 years for audit records, and at	**No exceptions noted.**

			least 6 months for incident records.	
C1.2	**The entity disposes of confidential information to meet the entity's objectives related to confidentiality.**			
	Identifies Confidential Information for Destruction — Procedures are in place to identify confidential information requiring destruction when the end of the retention period is reached.	Confidential information identified for destruction is disposed of according to classification-based rules ranging from secure deletion to physical destruction of media, with cloud providers required to use certified secure-erasure methods (in line with ISO/IEC 21964) before re-use or disposal of storage media. Identification of when information reaches the end of its retention period follows the retention framework defined by category (see C1.1).	URS assessed the applicable policy requirements and implementation evidence mapped to C1.2 and assessed the specific requirement that procedures are in place to identify confidential information requiring destruction when the end of the retention period is reached. Based on the POA description and the referenced evidence, URS confirmed that confidential information identified for destruction is disposed of according to classification-based rules ranging from secure deletion to physical destruction of media, with cloud providers required to use certified secure-erasure methods (in line with ISO/IEC 21964) before re-use or disposal of storage media. Identification of when information reaches the end of its retention period follows the retention framework defined by category (see C1.1).	**No exceptions noted.**

	Destroys Confidential Information — Policies and procedures are in place to automatically or manually erase or otherwise destroy confidential information that has been identified for destruction.	Confidential information identified for destruction is disposed of according to classification-based rules ranging from secure deletion to physical destruction of media, with cloud providers required to use certified secure-erasure methods (in line with ISO/IEC 21964) before re-use or disposal of storage media. Identification of when information reaches the end of its retention period follows the retention framework defined by category (see C1.1).	URS reviewed the governing procedures and referenced evidence mapped to C1.2 and assessed the specific requirement that policies and procedures are in place to automatically or manually erase or otherwise destroy confidential information that has been identified for destruction. Based on the POA description and the referenced evidence, URS determined that confidential information identified for destruction is disposed of according to classification-based rules ranging from secure deletion to physical destruction of media, with cloud providers required to use certified secure-erasure methods (in line with ISO/IEC 21964) before re-use or disposal of storage media. Identification of when information reaches the end of its retention period follows the retention framework defined by category (see C1.1).	**No exceptions noted.**