GUIDE

Driving Data Security in the Automotive Industry

How Cyera Supports TISAX Compliance

cyera

Table of Contents

Introduction 3

Information Security Policies and Organization 4

Human Resources 9

Physical Security 10

Identity and Access Management 10

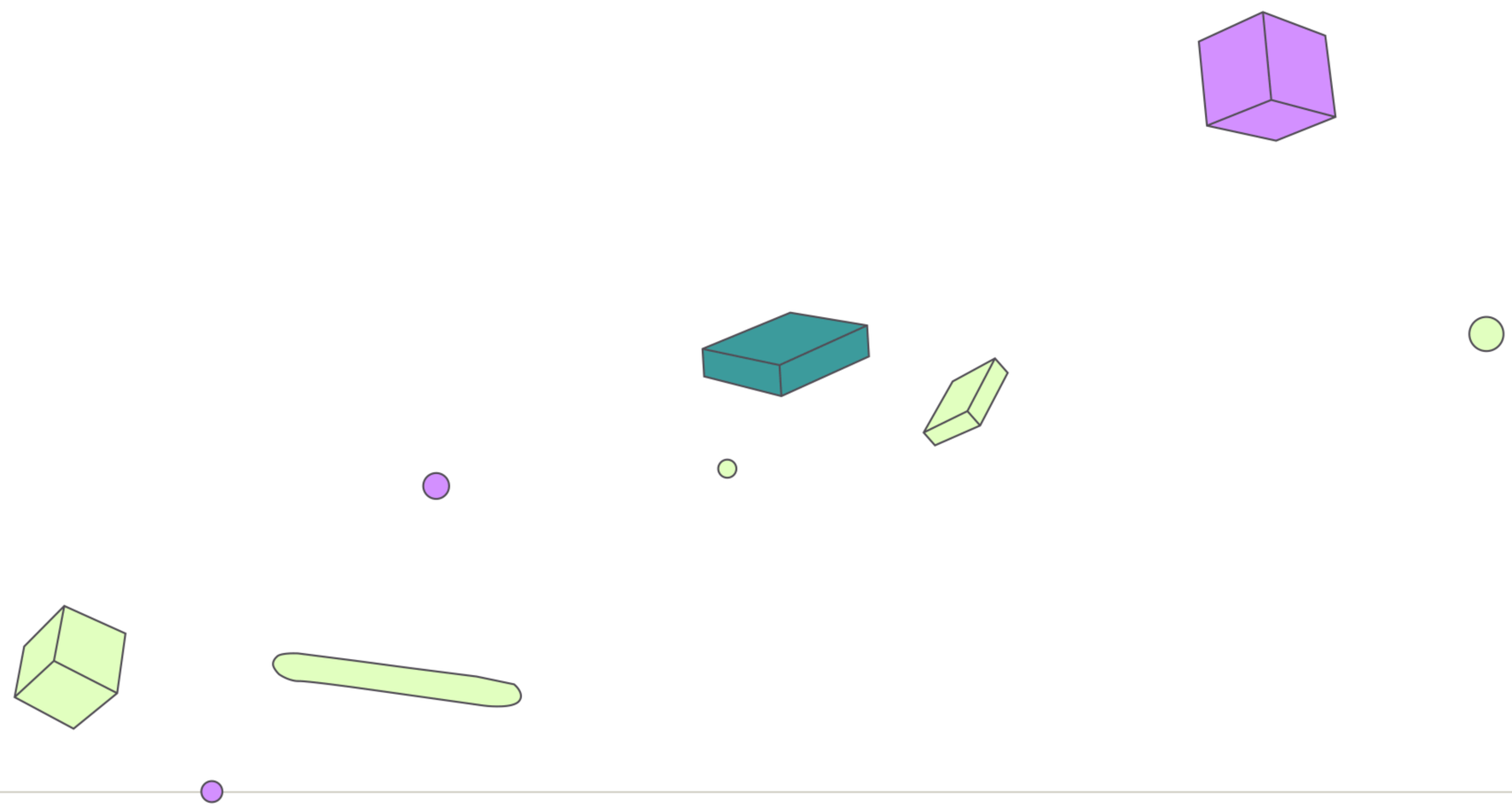
IT Security / Cybersecurity 11

Supplier Relationships 16

Compliance 17

Prototype Protection 17

Data Protection 20



Introduction

About TISAX

The Trusted Information Security Assessment Exchange (TISAX) is a framework developed by the German Association of the Automotive Industry (VDA) to promote a standardized approach to information security in the automotive industry.

Organizations seeking TISAX certification are assessed with respect to nine sets of controls relating to Information Security (Sections 1 through 7), Prototype Protection (Section 8), and Data Protection (Section 9). TISAX recognizes six maturity levels (0 to 5), with a minimum maturity level of 3 needed for certification.

The Information Security controls will be familiar to organizations that comply with the ISO 27001 standard, and while TISAX is not a legal requirement, it is the industry standard for European and global auto manufacturers, their contractors and subcontractors.

About Cyera

Cyera is a unified, AI-native data security platform that empowers businesses to discover, classify and protect data. It allows security leaders to manage sensitive data across highly permissive and widely distributed environments with high precision and efficiency.

The platform's agentless, fully automated data discovery provides a comprehensive inventory of sensitive data across structured and unstructured sources, and across IaaS, SaaS, DBaaS and on-premises environments. This capability enables organizations to address critical data challenges like data proliferation and drift. Powered by AI-native classification, Cyera goes beyond traditional methods by also understanding context, intent, and nuance - decoding data down to the DNA level. This deep insight helps uncover ghost data, reveal sensitive data risks, reduce false positives, and mitigate threats like data breaches and ransomware — areas where conventional data loss prevention and data governance tools fall short.

By combining advanced technology with ease of use, and scale from its cloud-delivered backbone, Cyera empowers organizations to confidently secure their data, maintain compliance, and unlock the full potential of their data to drive innovation.

1. Information Security Policies and Organization

1.1 Information Security Policies

1.1.1 To what extent are information security policies available?

Organizations must have a documented information security policy adapted to the needs of the organization and communicated to its employees. The policy must explain the objectives and significance of information security within the organization.

Cyera can help your organization better understand its information security needs and objectives.

Cyera's AI-native **DSPM** discovers and classifies all of your organization's data, across SaaS, PaaS, IaaS, and DBaaS services, as well as all on-prem systems. As a result, Cyera can map the scope and contours of your organization's attack surface with granularity and precision.

1.2 Organization of Information Security

1.2.1 To what extent is information security managed within the organization?

Organizations must have some kind of information security management system (ISMS) with clearly defined goals and structure. The ISMS must implement information security controls and its effectiveness must be regularly tested.

1.2.2 To what extent are information security responsibilities organized?

Information security roles and responsibilities are clearly defined and communicated to internal and external stakeholders. Resources necessary for fulfilling information security responsibilities are furnished.

Cyera continuously monitors your entire data estate, logging data events and alerting on policy violations or the occurrence of anomalous or suspicious activity. Cyera also integrates with third party tools like identity providers and SIEM tools to support your organization's data governance policies, as well as automate the handling of processes like incident response or the remediation of access misconfigurations.

Cyera's **AI Security Posture Management (AISPM)** discovers and inventories Shadow AI tools and AI-capable SaaS apps used in the environment, ensuring unauthorized AI systems are not storing or processing sensitive prototype or manufacturing data.

1.2 Organization of Information Security

1.2.3 To what extent are information security requirements considered in projects?

Projects are classified according to their security requirements.

Cyera can help your organization ensure that project data is correctly classified according to its security requirements.

Cyera's AI-native **DSPM** doesn't just classify data by looking at superficial fingerprints or fixed patterns. It grasps the import of data from its context, allowing it to understand the nature of unstructured data and to correctly classify that data with 95 percent precision.

In addition to pre-trained classifiers aligned with many different control frameworks, Cyera's DSPM can learn to recognize new patterns that are unique to your organization.

1.2.4 To what extent are the responsibilities between external IT service providers and the organization defined?

External IT service providers are identified and their security requirements are determined.

The assignment of responsibilities for information security is clearly defined and communicated, and mechanisms are in place to verify compliance.

Cyera **Omni DLP** can trace your data through users and applications, giving you a better picture of which applications are handling the largest volumes of data, and which are handling the most sensitive data, including unmanaged "Shadow IT" apps and services.

Cyera's **Identity Access** catalogs all the entities that have access to your organization's data, whether internal or external, human or non-human. Together, **Omni DLP** and **Identity Access** can be used to verify that external IT service providers are adhering to information security responsibilities such as requiring strong passphrases or multi-factor authentication.

Finally, Cyera's **Agent Guardian** can help identify AI applications in use in your environment, including Shadow AI, and can monitor AI usage to prevent abusive prompts or data leakage.

1.3 Asset Management

1.3.1 To what extent are information assets identified and recorded?

Organizations must inventory their data assets as well as the supporting assets required for their processing. Organizations must appoint a person responsible for their data assets and supporting assets.

Cyera's AI-native **DSPM** can identify your data across cloud, on-prem, and hybrid environments and classify them with 95 percent precision. Pre-trained classifiers can assign data to categories aligned with major regulatory frameworks and industry standards.

Additionally, Cyera's **DSPM** can learn to recognize classification schemas unique to your organization's environment. These schemas are particularly useful for identifying and protecting intellectual property such as trade secrets.

1.3.2 To what extent are information assets classified and managed in terms of their protection needs?

Organizations must devise and consistently implement a classification scheme for information assets based on their protection needs. Rules regarding the handling of information assets based on their assigned classification must be established and enforced.

Cyera's **Omni DLP** protects structured, unstructured, and AI-generated data in motion, and Cyera's **Agent Guardian** prevents sensitive data from being shared with or by AI tools.

1.3.3 To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets?

External IT services are not onboarded without first conducting a risk assessment that considers legal, regulatory, and contractual requirements, as well as the protection needs of the data those services would have access to.

Cyera's AI-native **DSPM** discovers and classifies your entire data estate, giving visibility into what data you have, its nature and sensitivity, where it's going and who has access to it.

Cyera's **Omni DLP** tracks data in motion, and can prevent data from being shared with unapproved apps and services.

And Cyera's **Identity Access** shows you all the entities, internal or external, that have access to your data, again helping you keep track of external services that may be accessing your data.

1.3.4 To what extent is it ensured that only evaluated and approved software is used for processing the organization's information assets?

Software must be approved prior to installation or use. The approval process should consider the source and reputation of the software, use rights and licensing, whether its use should be limited to specific use cases or roles, and whether use of the software would be consistent with the organization's information security requirements.

With Cyera's **AISPM**, organizations can track usage of unauthorized generative AI apps or unvetted browser plugins used by engineers or designers, supporting TISAX's requirement to only allow pre-approved applications.

Cyera's **Agent Guardian** monitors AI usage for data leakage and prevents sensitive data from being used in LLM prompts.

1.4 Information Security Risk Management

1.4.1 To what extent are information security risks managed?

Risk assessments are carried out on a regular basis and in response to security events. Information risks are documented, and a responsible person is assigned to each information security risk.

Cyera's **Data Risk Assessment** service provides your security officials with a virtual, CISO-led evaluation of your organization's data security posture relative to more than 30 controls from frameworks such as ISO 27001 and NIST CSF. The service provides actionable intelligence that can help you immediately shrink your attack surface, gain greater visibility into potential threats, and develop a plan for improving your security posture going forward, including timelines and milestones.

1.5 Assessments

1.5.1 To what extent is compliance with information security ensured in procedures and processes?

Organizations must verify compliance with information security policies and requirements, and initiate and pursue measures for correcting deviations from those requirements.

Information security policies and requirements are reviewed on a regular basis, and the results of those reviews are recorded and retained.

Cyera's AI-native **DSPM** discovers and classifies your organization's data across cloud, on-prem, and hybrid environments. Many customers discover far greater stores of data than they anticipated, helping them to securely delete redundant, obsolete, and trivial (ROT) data, thereby ensuring compliance with minimization requirements and data retention policies.

Cyera monitors your data estate and alerts on violations of information security policies, such as the discovery of unencrypted sensitive data. It can send alerts to data owners via email, Slack, or other channels with instructions for remediation, and can also integrate with third-party SIEM tools to automate incident response. Audit log retention supports compliance testing.

1.5.2 To what extent is the information security management system reviewed by an independent authority?

Information security policies and requirements are reviewed by an independent and competent body at regular intervals, and measures for correcting deviations between policy requirements and practices must be initiated and pursued.

Cyera's **Data Risk Assessment** service provides a virtual, CISO-led evaluation of your organization's information security posture that can help you define the scope of your attack surface, identify gaps between policy requirements and security practices, and provide specific, actionable guidance for improving your data security posture moving forward.

1.6 Incident and Crisis Management

1.6.1 To what extent are information security relevant events or observations reported?

Definitions for reportable security events are established and communicated to employees and other stakeholders.

Mechanisms for reporting events are implemented and communicated to all potential reporters, and adequate communication channels with event reporters are established.

Cyera monitors your data estate, logs all data events and alerts on violations of data security policies. Alerts can be sent to data owners via email, Slack, or other channels with instructions for remediation. Cyera also integrates with third-party SIEM tools to facilitate automated incident response and remediation.

Access Trail creates an auditable, time-stamped record of who accessed sensitive data, what they did, and when.

Cyera's **DataWatcher** provides continuous, expert-led monitoring of sensitive data activity and risk. It alerts owners when something looks off (for example, unusual downloads or shares), helping employees recognize and report events early.

1.6.2 To what extent are reported security events managed?

Reported events are processed and responded to in a timely manner. Lessons learned are incorporated into the ISMS for continuous improvement.

1.6.3 To what extent is the organization prepared to handle crisis situations?

Organizations must have a disaster recovery and business continuity plan. Roles and responsibilities for disaster recovery and business continuity are assigned to appropriate personnel, and adequate resources are furnished for the carrying out of their duties.

Through its integration with Cohesity, Cyera helps organizations prioritize backup cadences based on the sensitivity and criticality of data, so organizations can bounce back quickly after an incident.

2. Human Resources

2.1.1 To what extent is the qualification of employees for sensitive work fields ensured?

Organizations must identify which work fields or jobs involve access to sensitive data, and what responsibilities those jobs or work fields entail. Organizations must also perform due diligence before onboarding new staff, including verifying identities and performing background checks.

Cyera's AI-native **DSPM** discovers and classifies all of your data, across the cloud and on-prem, and can identify which users have access to which data and what they're doing with it. This can be incredibly useful in identifying insider threats.

Cyera can discover and alert on suspicious or anomalous user behavior such as the downloading or sharing of large numbers of sensitive files. And Cyera's **Omni DLP** can prevent insiders from sharing sensitive information outside the organization in violation of their non-disclosure agreements.

2.1.2 To what extent are all staff contractually bound to comply with information security policies?

Employees must agree to be bound by non-disclosure agreements and the organization's information security policy.

And Cyera's **Identity Access** can discover when stale identities (such as ex-employees) still have access to your organization's data. It also surfaces over-permissioned identities and identities that have not enabled multifactor authentication.

2.1.3 To what extent are staff made aware of and trained with respect to the risks arising from the handling of information?

Employees must undergo information security awareness training.

Alerts generated by Cyera include sending a message to the data owner via email, Slack, or other channels, along with instructions for remediation.

Cyera's **Email Engagement** feature enables targeted, branded outreach to employees or contractors who own sensitive data—promoting proactive remediation and reinforcing secure data handling policies.

In this way, Cyera "democratizes" the process of data security, extending awareness and responsibility for data security beyond the SOC team to every data owner in your organization.

2.1.4 To what extent is mobile work regulated?

Organizations must have a teleworking policy that covers the secure handling of information assets by employees working remotely, especially in public settings.

Remote workers must use a secure connection (such as a VPN) to connect to the organization's network, and strong authentication processes must be in place.

Cyera can support your organization's secure remote work policy. Cyera's AI-native **DSPM** discovers and classifies all your organization's sensitive data, and can identify and alert on unencrypted data in transit.

Cyera's **Omni DLP** can prevent organizational data from being shared with unmanaged applications and services, and Cyera's **Identity Access** gives you visibility into which users are accessing which data, and whether secure authentication and access management policies are being adhered to.

3. Physical Security

Cyera does not provide physical security services

4. Identity and Access Management

4.1 Identity Management

4.1.1 To what extent is use of identification means managed?

Organizations must determine the requirements for handling the means of identification throughout their lifecycle.

4.1.2 To what extent is the user access to IT services and IT systems secured?

Procedures for user authentication must be selected based on a risk assessment that includes possible attack scenarios, and must use state of the art technology.

4.1.3 To what extent are user accounts and login information securely managed and applied?

Organizations must create unique and personalized user accounts (collective accounts should be restricted to clearly defined circumstances).

User accounts must be reviewed regularly, and accounts must be disabled immediately when a user leaves the organization.

The organization must have a secure policy for the handling of login credentials from the creation of the user account until its disablement.

Cyera can assist your organization in implementing and verifying secure procedures for user authentication.

Cyera integrates with third party identity providers like Okta and Ping to provide context about which users have had access to which data, whether they're still employed by the organization or have changed roles, which departments they're in, and their appropriate access and privileges.

Cyera's **Identity Access** product catalogs entities with access to your organization's data, whether internal or external, human or non-human. Identity Access can identify stale identities (such as former employees) whose accounts should have been disabled. It can also verify whether users are adhering to secure authentication policies such as length requirements for passphrases or the use of multi-factor authentication.

4.2 Access Management

4.2.1 To what extent are access rights assigned and managed?

Organizations must establish and adhere to requirements for the management of access rights.

Access rights must conform to the principle of least privilege.

Cyera integrates with third party identity providers like Okta and Ping to provide context about which users have had access to which data, whether they're still employed by the organization or have changed roles, which departments they're in, and their appropriate access and privileges.

With **Access Trail**, access reviews don't rely on guesswork. Teams can see actual usage of sensitive data by each identity and align privileges to least-privilege expectations, with exportable, audit-ready evidence.

5. IT Security / Cybersecurity

5.1 Cryptography

5.1.1 To what extent is the use of cryptographic procedures managed?

Cryptographic procedures must conform to the current industry standard.

Cyera can alert on the discovery of data that ought to be encrypted according to organizational policy, and can provide guidance for remediation or integrate with SIEM tools to automate remediation workflows. Cyera can also be configured to take action directly to protect exposed data by, for example, auto-masking sensitive data in DBaaS products like Snowflake.

5.1.2 To what extent is information protected during transfer?

Organizations must identify and document all network services used to transfer information, must define and implement classification requirements for the use of those services, and must implement measures to prevent unauthorized access to information during transfer.

Omni DLP can block sensitive IP and prototype files uploaded to unmanaged apps or transmitted via AI prompts or outputs.

DataPort allows customers to query Cyera's data intelligence to identify where sensitive data may be exposed or transferred through unapproved channels.

5.2 Operations Security

5.2.1 To what extent are changes managed?

Information security requirements for changes to the organization, business processes, and IT systems are determined and applied.

Cyera's AI-native **DSPM** can identify and classify data across your IT ecosystem, giving visibility into who has access, what kind of access they have, and where they are using data.

In this way, Cyera can help you identify unmanaged apps and services touching sensitive data. And Cyera's **Identity Access** feature can help you see when users who have changed roles or left the organization still have access to data from their previous roles.

5.2.2 To what extent are development and testing environments separated from operational environments?

Organizations must perform a risk assessment to determine the necessity of separating IT systems into testing, development, and production environments. Segmentation must be implemented on the basis of that risk analysis.

Cyera's **Data Risk Assessment** can assist your organization in determining the necessity of separating systems into testing, development, and production environments.

Cyera's AI-native discovery and classification capability can then ascertain the nature and sensitivity of all data in the environment. This allows Cyera to determine whether data that is required to be in a specific network segment has migrated elsewhere, or whether data that ought to be encrypted has been discovered in an exposed state.

5.2.3 To what extent are IT systems protected against malware?

Requirements for protection against malware are determined, and technical and organizational measures for protection against malware are defined and implemented.

While Cyera does not detect malware directly, it may be able to indirectly observe the indicia of a malware infection by, for example, detecting anomalous usage by a specific user who was a victim of a phishing attack. Cyera can alert on suspicious or anomalous behavior, allowing administrators to intervene before a malware infection causes a material breach or other serious incident.

5.2 Operations Security

5.2.4 To what extent are event logs recorded and analyzed?

Organizations must determine and fulfill the security requirements for the logging of activities and the handling of event logs.

IT systems must be assessed based on the necessity of logging, and when assessing external IT systems, organizations must consider information about monitoring options those systems afford.

Event logs must be checked regularly for rule violations or other anomalous events/ behavior.

Cyera logs and retains all data access events, classification changes, and policy violations, allowing administrators to detect anomalies and engage in forensic analysis of events.

Access Trail centralizes and enriches access activity with data sensitivity and identity context, retains records for a year by default, and supports export to your SIEM for ongoing analysis and audits.

Cyera also supports this requirement through its integrations with other logging and monitoring tools. Cyera's AI-native data discovery and classification capability enables much richer analysis of logs and reports.

5.2.5 To what extent are vulnerabilities identified and addressed?

Organizations must gather and evaluate information on technical vulnerabilities in their IT systems, and potentially affected systems and software must be identified and the vulnerabilities addressed.

Cyera identifies and helps remediate data exposures resulting from misconfigured S3 buckets, open internal shares, stale access policies, or insecure AI tool usage.

DataWatcher accelerates risk reduction by guiding and driving remediation of data exposures (e.g., over-broad sharing, public links, risky app usage) so issues are addressed quickly and consistently.

5.2.6 To what extent are IT systems and services technically checked?

Organizations must determine the scope and requirements for performing audits of IT systems, and coordinate the performance of audits with operators or users of those systems.

Results of audits must be stored in a traceable manner and shared with appropriate management, and measures must be derived from the results.

Cyera's **Data Risk Assessment** service provides your security officials with a virtual, CISO-led evaluation of your organization's data security posture relative to more than 30 controls from frameworks such as ISO 27001 and NIST CSF. The service provides actionable intelligence that can help you immediately shrink your attack surface, gain greater visibility into potential threats, and develop a plan for improving your security posture going forward, including timelines and milestones.

5.2 Operations Security

5.2.7 To what extent is the network of the organization managed?

Requirements for the management, control, and segmentation of networks must be determined and fulfilled.

Cyera's AI-native discovery and classification capability can ascertain the nature and sensitivity of data in the environment, allowing Cyera to determine whether data that is required to be in a specific network segment has migrated elsewhere, or whether data that ought to be encrypted has been discovered in an exposed state.

Additionally, **DataPort** gives security and compliance teams visibility into data flow patterns across their cloud and SaaS environments. By querying Cyera's dataset, teams can detect potential data movement outside approved regions or services.

Furthermore, Cyera's **Identity Access** gives you visibility into which entities have access to your data, anywhere in your IT ecosystem. This includes human and non-human users, internal and external, and users that may once have been employed by your organization or otherwise authorized to access data, but who shouldn't be now.

5.2.8 To what extent is continuity planning for IT services in place?

Organizations must identify critical IT services and assess the business impact of any disruption to those services.

Relevant stakeholders must understand and fulfill their responsibilities for the continuity and recovery of those IT services.

Cyera can help you understand which IT services are most critical to your organization. Cyera's AI-native **DSPM** and **Omni DLP** identify, classify, and trace your data across users and applications, letting you see where your data resides and who's using it. This visibility allows you to determine which apps and services are most heavily used by your organization, and by whom. It also assists in identifying unmanaged (Shadow) IT services that may also be critical to your operations.

5.2.9 To what extent is the backup and recovery of data and IT services ensured?

Organizations must define and implement appropriate protective measures to ensure the confidentiality, integrity, and availability of backups, and must have in place a plan for the recovery of relevant IT services.

Cyera supports the implementation of your organization's data backup plan. Cyera's unparalleled data discovery and classification capabilities help define the scope of necessary backups. And by partnering with backup technology provider Cohesity, Cyera enhances your cyber resilience by helping your organization prioritize backup cadences based on the sensitivity and criticality of data.

5.3 Systems acquisition, requirement management, and development

5.3.1 To what extent is information security considered in new or further developed IT systems?

Organizations must determine the information security requirements associated with the design, development, acquisition, extension, and changes to the IT system.

By providing a clear and thorough picture of your organization's data, Cyera helps you reduce the exposure of sensitive data, enforce access controls and prevent access misconfigurations, and prevent data from being shared outside of development or testing environments. Cyera can even detect when sensitive data has been used in code, and can alert administrators to take remedial action.

DataPort helps organizations identify where data related to offboarded services or vendors still resides. Teams can query and export relevant data maps to ensure complete data removal and validate cleanup efforts.

5.3.2 To what extent are requirements for network services defined?

Requirements regarding the information security of network services are determined and fulfilled.

5.3.3 To what extent is the return and secure removal of information assets from external IT services regulated?

A procedure for the return and secure removal of information assets from each external IT service is defined and implemented.

5.3.4 To what extent is information protected in shared external IT resources?

The organization utilizes network segregation to prevent unauthorized users from external organizations from accessing internal data.

6. Supplier Relationships

6.1.1 To what extent is information security ensured among contractors and cooperation partners?

Contractors and cooperation partners must be subjected to a risk assessment with respect to information security, and an appropriate level of information security is ensured through the use of contractual obligations.

Contractual agreements with respect to information security must be passed on to subcontractors where appropriate, and compliance with contractual provisions for information security must be verified.

6.1.2 To what extent is non-disclosure regarding the exchange of information contractually agreed?

Organizations must put in place valid non-disclosure agreements with relevant parties before transferring sensitive information.

Members of the organization must understand when non-disclosure agreements are required, and those requirements must be reviewed and updated on a regular basis.

Cyera can help validate appropriate information security vis-a-vis contractors and cooperation partners. Cyera's **DSPM** and **Omni DLP** give administrators visibility into where your data resides, who has access to it, and what they're doing with it.

Cyera's **Identity Access** feature lets you see all entities, whether internal or external, human or non-human, who have access to your data. It can also provide insights such as whether external users have adopted secure authentication procedures such as requiring long passphrases or multi-factor authentication.

DataPort supports oversight of third-party data handling by allowing customers to analyze how partner-related data is distributed across systems and regions. These insights make it easier to verify supplier compliance and document corrective actions.

7. Compliance

7.1.1 To what extent is compliance with regulatory and contractual provisions ensured?

At regular intervals, organizations must determine the legal, regulatory, and contractual provisions applicable to information security, and must define, implement, and communicate policies for compliance with those provisions.

7.1.2 To what extent is the protection of personally identifiable data considered when implementing information security?

Legal, regulatory, and contractual provisions regarding the secure handling of personally identifiable information are determined and communicated to entrusted persons.

Processes and procedures for the protection of personally identifiable information are incorporated into the ISMS.

Cyera's AI-native **DSPM** comes equipped with pre-trained classifiers aligned with major regulatory frameworks such as the GDPR. It can also learn new categories of sensitive data based on your unique environment. This can be especially helpful in recognizing intellectual property and trade secrets, or data that's been shared with or from specific contractors or cooperation partners.

Cyera can recognize personally identifiable information and can orchestrate redaction or masking via policies and integrations. It also sends alerts to data owners with instructions for remediation, and integrates with third-party SIEM tools to automate remediation workflows.

Access Trail streamlines assessments by generating compliance records in seconds—showing who accessed which data, what changed, and when—so evidence collection doesn't stall projects.

8. Prototype Protection

8.1 Physical and Environmental Security

Cyera does not provide physical security services

8.2 Organizational Requirements

8.2.1 To what extent are valid non-disclosure agreements/obligations in effect?

Organizations must put in place valid non-disclosure agreements between contractors and customers, and with all relevant employees and project members, before transferring prototype data.

Cyera's AI-native **DSPM** can assist with this requirement by learning to recognize sensitive categories of data that are unique to your organization. An important use case for this capability is the recognition and protection of intellectual property and trade secrets such as prototype data.

Cyera's **Omni DLP** can be configured to prevent the egress of prototype data with much greater precision than traditional DLP solutions, greatly reducing false positives.

8.2.2 To what extent are requirements for commissioning subcontractors known and fulfilled?

Subject to the approval of the customer, valid non-disclosure agreements must be put in place with subcontractors, and their compliance with those agreements must be verified.

DataPort helps organizations verify that prototype and confidential project data remains within approved systems. Queries can surface potential leaks or unintended storage.

8.2.3 To what extent do employees and project members evidently participate in training and awareness measures regarding the handling of prototypes?

Organizations must ensure the execution of training and awareness measures by management.

Employees and project members must participate in regular, mandatory training and awareness programs with respect to the security requirements for handling prototype data, and completion of those programs must be documented.

Cyera can help raise awareness of data security in your organization by sending alerts directly to data owners and providing them with instructions for remediating vulnerabilities such as access misconfigurations or the exposure of unencrypted data. In this way, Cyera "democratizes" data security responsibilities beyond the SOC team, helping employees and project members understand their role in securely handling prototype data.

8.2.4 To what extent are security classifications of the project and the resulting security measures known?

Organizations must ensure the security classification and requirements in relation to the project progress are understood and adhered to by each project member.

8.2 Organizational Requirements

8.2.5 To what extent is a process defined for granting access to security areas?

Responsibilities for access authorization are clearly specified and documented, and a process must exist for assigning, changing, and revoking access rights.

This requirement pertains to the securing of physical premises. Cyera does not provide physical security services.

8.2.6 To what extent are regulations for image recording and handling of created image material defined?

Organizations must have in place a policy for the approval of image recordings, and the classification, secure storage, secure transmission, and secure deletion of image recordings.

Cyera can assist with this requirement by discovering image and video files, and alerting administrators when image or video files are discovered outside of dedicated environments.

8.2.7 To what extent is a process for carrying along and using mobile video and photography devices into defined security areas established?

Organizations must have in place a policy for the secure carrying along and use of mobile video and photography devices.

This is the responsibility of the organization.

8.5 Requirements for events and shootings

8.5.1 To what extent are security requirements for presentations and events involving vehicles, components, or parts classified as requiring protection known?

Organizations must describe and implement a process for obtaining customer-specific requirements for the classification of protected information relating to presentations and events involving vehicle, components, or parts.

Cyera's AI-native **DSPM** can learn classification schemas unique to your organization, including file-level classifications relating to things like specific products, presentations, or customers.

This capability can be leveraged to create DLP policies that align with customer requirements for the classification of protected information.

8.5.2 To what extent are the protective measures for film and photo shootings involving vehicles, components, or parts classified as requiring protection known?

Organizations must describe and implement a process for obtaining customer-specific requirements for the classification of protected information relating to film and photo shootings involving vehicles, components, and parts.

9. Data Protection

9.1 Data Protection Policies

9.1.1 To what extent do data protection policies exist?

A data protection policy must be created, regularly updated, and approved by management.

Cyera provides a **Data Risk Assessment** service that can inform future updates to your data protection policy. The Data Risk Assessment service provides your security officials with a virtual, CISO-led evaluation of your organization's data security posture relative to more than 30 controls from frameworks such as ISO 27001 and NIST CSF. The service provides actionable intelligence that can help you immediately shrink your attack surface, gain greater visibility into potential threats, and develop a plan for improving your security posture going forward, including timelines and milestones.

9.2 Organization of Data Protection

9.2.1 To what extent are the responsibilities for data protection organized?

Organizations must appoint a qualified data protection officer, and the role of the DPO must be integrated into the organization's structure.

This is the responsibility of the organization.

9.3 Processing Directory

9.3.1 To what extent are processing activities identified and recorded?

If required by law (eg GDPR), organizations must maintain a register of processing activities.

Cyera continuously monitors your data estate and logs all data events, and its AI-native **DSPM** can identify protected classes of data such as personal data as defined by the GDPR.

Access Trail links access events to specific identities, datasets, and systems, providing a searchable record of processing activity that simplifies RoPA documentation.

9.4 Data Protection Impact Assessment

9.4.1 To what extent is adequate handling of high-risk processing activities ensured (data protection impact assessment)?

Organizations must determine which data processing activities require data protection impact assessments, and must define and communicate to the responsible parties their duties in carrying out data protection impact assessments.

Cyera's **Privacy Assessments** module provides DPIA and PIA workflows with auto-populated context drawn from Cyera's data discovery and classification, reducing manual effort and improving audit readiness across recurring DPIAs. The module integrates with the **Privacy Risk Register** to centralize tracking of identified risks and mitigations.

Agent Guardian supports DPIAs involving AI by identifying sensitive data entering AI tools, blocking regulated content in prompts/outputs, and helping enforce controls on AI usage.

For high-risk processing activities, **DataPort** enables teams to surface and analyze data flows, assess where sensitive data is stored or transferred, and document findings that feed into the Data Protection Impact Assessment (DPIA) process.

9.5 Data Transfers

9.5.1 To what extent is the transfer of data managed?

Organizations must implement appropriate processes and workflows for the transmission of data, including ensuring the consent or right of objection of the person responsible for subcontracting.

9.5.2 To what extent are contractual obligations passed through to and enforced by subcontractors and cooperation partners?

Organizations must ensure that applicable contractual provisions to clients are passed on to subcontractors, and review compliance with those contractual provisions.

9.5.3 To what extent are data transfers to third countries managed?

Organizations must systematically record all data transfers to third countries, and when required must obtain the consent of the data subjects whose data is transferred to third countries, or perform data transfer impact assessments (DTIAs) prior to transfer.

Cyera's AI-native **DSPM** can classify your data by type and sensitivity, and apply policies to encrypt, mask, or tokenize unencrypted data. It can also identify personal data as defined by regulatory frameworks like the GDPR, helping to facilitate data subject access requests.

Cyera's **Identity Access** feature catalogs all entities that have access to your data, whether internal or external. This can be useful in identifying contractors or subcontractors who have access to your data ecosystem. Identity Access can help you manage access privileges for external users, and confirm whether external users have complied with data protection policies such as the implementation of secure authentication methods like strong passphrases or multi-factor authentication.

DataPort provides visibility into how and where sensitive data moves across systems. By querying your Cyera data, teams can identify transfer risks and confirm that corrective actions—such as encryption, deletion, or policy enforcement—have been completed in connected platforms.

Finally, Cyera gives you visibility into where your data resides and where it's processed, facilitating compliance with data localization requirements.

9.6 Handling Requests and Incidents

9.6.1 To what extent are data subject requests processed?

Organizations must process requests from data subjects in a timely manner, including training employees in handling subject access requests and providing support to data controllers in fulfilling subject access requests.

DSR Automation locates a requester's personal data across SaaS, IaaS, DBaaS, and on-prem systems; guides approvals; and produces a consistent, auditable response package, completing a week's worth of manual work in minutes.

9.6 Handling Requests and Incidents

9.6.2 To what extent are data protection incidents processed?

Organizations must establish and adhere to a plan for processing data protection incidents in a timely manner, including documenting procedures for notifying responsible parties, documenting incident response activities, training employees, and supporting data controllers in their response to data protection incidents.

Cyera continuously monitors your data estate, logging data events and alerting on policy violations or the occurrence of anomalous or suspicious activity.

Cyera also integrates with third party tools like identity providers and SIEM tools to support your organization's data governance policies, as well as automate the handling of processes like incident response or the remediation of access misconfigurations.

Access Trail supplies the incident timeline—who accessed which records, what changed, and when—while DataWatcher drives and verifies remediation to close exposures and document resolution.

9.7 Human Resources

9.7.1 To what extent are employees obliged to maintain confidentiality?

Employees whose tasks involve the processing of personal data are obliged to maintain confidentiality and to comply with applicable data protection laws. This obligation must be documented.

Cyera can assist in raising information security awareness across your organization.

Cyera monitors your data estate, logs data events, and alerts on violations of information security policies. Alerts generated by Cyera include sending a message to the data owner via email, Slack, or other channels, along with instructions for remediation.

9.7.2 To what extent are employees trained in data protection?

Employees are given appropriate data security training specific to their work, and the scope, frequency, and content of training must be determined according to the protection needs of the data in question.

In this way, Cyera "democratizes" the process of data security, extending awareness and responsibility for data security beyond the SOC team to every data owner in your organization.

9.8 Instructions

9.8.1 To what extent are instructions of processing relationships handled?

Organizations must put in place procedures and measures to ensure that instructions by data controllers regarding the processing of personal data are documented and implemented, and that data is separated by client and specific order or project.

In addition to pre-trained classifiers aligned with common regulatory frameworks, Cyera's AI-native **DSPM** can also learn to recognize categories of data specific to your organization's unique environment. This capability can assist your organization with the implementation of policies to protect personal data, as well as associating data with specific clients, orders, or projects.