HECVAT™ Solution Provider Response - *Start Here*

Date Completed	*12/9/2025*

Instructions for Solution Providers

1. Complete the "Start Here" tab and review the "Required Questions" guidance to find the other

2. Complete the "Organization" tab and the applicable questions in each of the next 5 tabs (Produ

3. Guidance in column E may change based on your answers to prompt details in "Additional Info

4. DO NOT complete any fields in the "Evaluation" sheets or the "Analyst Notes" column.

5. Return the completed file to institutions.

* *Denotes critical questions. Critical questions are those deemed most important to institutions by higher edu*

For full instructions, please visit educause.edu/HECVAT

General Information

GNRL-01	Solution Provider Name	*EdInvent Inc. d.b.a. Accre*
GNRL-02	Solution Name	*Accredible*
GNRL-03	Solution Description	*Accredible is a cloud-host modern web browser to d*
GNRL-04	Solution Provider Contact Name	*Alan Heppenstall*
GNRL-05	Solution Provider Contact Title	*CTO*
GNRL-06	Solution Provider Contact Email	*alan@accredible.com*
GNRL-07	Solution Provider Contact Phone Number	*+1 (628) 214-2701*
GNRL-08	Country of Company Headquarters	*United States*

GNRL-09	Employee Work Locations (all)	*Accredible is a globally di* *All employees and contrac*
Company Information		**Answer**
COMP-01	Do you have a dedicated software and system development team(s) (e.g., customer support, implementation, product management, etc.)?*	Yes
COMP-02	Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships.	Yes
COMP-03	Have you operated without unplanned disruptions to this solution in the past 12 months?	Yes
COMP-04	Do you have a dedicated information security staff or office?	No
COMP-05	Use this area to share information about your environment that will assist those who are assessing your company's data security program	
Required Questions		**Answer**
REQU-01	Are you offering either a product or platform, as opposed to only offering a service	Yes

REQU-02	Does your product or service have an interface?	Yes
REQU-03	Are you providing consulting services?	Yes
REQU-04	Does your solution have AI features, or are there plans to implement AI features in the next 12 months?	Yes
REQU-05	Does your solution process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act (HIPAA)?	No
REQU-06	Is the solution designed to process, store, or transmit credit card information?	No
REQU-07	Does operating your solution require the institution to operate a physical or virtual appliance in their own environment or to provide inbound firewall exceptions to allow your employees to remotely administer systems in the institution's environment?	No
REQU-08	Does your solution have access to personal or institutional data?	Yes

Note: The "Organization" tab is required for ALL products and services.

sections are required for your product or service.

ct through Privacy) that apply, based on your answers to the "Req

rmation." If leaving an answer blank, you must also state why in "

cation volunteers.

edible.

ted, shared-tenant Software as a Service solution. As the customer, you are ar
esign, create, deliver and administrate certificates and badges

stributed organization, so employees and contractors outside the US have acce
tors are formally vetted in the same way, with uniform background checking, t

Additional Information
Accredible maintains dedicated teams across engineering, product management, implementation, and customer support. Engineering focuses on platform reliability, integrations, and security. Product management ensures alignment with customer needs and industry trends. Implementation specialists oversee onboarding and rollout, while customer support provides responsive assistance. This structure ensures scalability and high-quality service delivery.
EdInvent Inc. d.b.a. Accredible is a US C-corporation, and has a wholly owned UK subsidiary, Accredible Ltd for it's UK operations
Accredible has delivered continuous service availability with no material unplanned disruptions in the last 12 months. High availability is achieved through cloud redundancy, proactive monitoring, and 24/7 operations support. Service performance
Accredible does not maintain a dedicated, standalone information security office. Instead, security responsibilities are integrated into its broader engineering, infrastructure, and compliance practices
Security is integrated into the software development lifecycle, access management, and infrastructure operations. Controls align with ISO 27001, NIST CSF, and CIS

Additional Information
Accredible provides a SaaS-based digital credentialing platform that enables organizations to issue, manage, and verify digital certificates and badges. Implementation and support services are provided to ensure success but are not the primary offering.

Accredible includes both an administrative interface for issuing and managing credentials, and a recipient-facing interface that allows learners to view, share, and verify credentials easily.
Accredible does not operate as a consulting company. Professional services are provided only to support integration, onboarding, and credential program rollout, always in conjunction with the platform.
Accredible uses AI and machine learning for credential fraud detection, analytics, and usage insights. Future roadmap items also include expanded AI capabilities, all aligned with ethical AI principles such as transparency, fairness, and human oversight.
Accredible is not designed to handle PHI and does not process HIPAA-covered data. The platform is focused on credential and achievement data for education, training, and certification.
Accredible does not store, process, or transmit credit card information. Where billing is required, trusted PCI DSS–compliant third-party payment processors are used.
Accredible is a fully managed SaaS solution. It does not require the institution to operate appliances in their environment or to configure inbound firewall exceptions for Accredible staff.
Accredible processes personal data such as name, email, and credential metadata necessary to issue and manage credentials. Access is controlled, minimized, and governed by GDPR/CCPA-compliant policies. Institutional data is protected through encryption, access controls, and logical segregation.

Version 4.1.0

uired Questions."

'Additional Information".

ı issuer of digital credentials and access a Dashboard web property via a

ess to organization networks, product code or systems.
raining, equipment and access control policies.

Guidance	Analyst Notes
Describe the structure and size of your software and system development teams. (e.g., customer support, implementation, product management, etc.).	
Describe any plans to create an information security office for your organization.	
Share any details that would help information security analysts assess your	

Guidance	Analyst Notes
DO complete the Product and Infrastructure worksheets	

DO complete the IT Accessibility worksheet.	
DO complete the Consulting section in the Case-Specific worksheet	
DO complete the Artificial Intelligence (AI) worksheet	
DO NOT complete the HIPAA section in the Case-Specific worksheet	
DO NOT complete the PCI-DSS section in the Case-Specific worksheet	
DO NOT complete the On-Prem section in the Case-Specific worksheet	
DO complete the Privacy tab	

HECVAT Solution Provider Response - *Organization*

Date Completed	*12/9/2025*

Instructions for Solution Providers

1. Complete the "Start Here" tab and review the "Required Questions" guidance to find the other

2. Complete the "Organization" tab and the applicable questions in each of the next 5 tabs (Produ

3. Guidance in column E may change based on your answers to prompt details in "Additional Info

4. DO NOT complete any fields in the "Evaluation" sheets or the "Analyst Notes" column.

5. Return the completed file to institutions.

* *Denotes critical questions. Critical questions are those deemed most important to institutions by higher edu*

For full instructions, please visit educause.edu/HECVAT

General Information		**Answer**
GNRL-01	Solution Provider Name	*EdInvent Inc. d.b.a. Accre*
GNRL-02	Solution Name	*Accredible*
GNRL-03	Solution Description	*Accredible is a clo*
GNRL-04	Solution Provider Contact Name	*Alan Heppenstall*
GNRL-05	Solution Provider Contact Title	*CTO*
GNRL-06	Solution Provider Contact Email	*alan@accredible.com*
GNRL-07	Solution Provider Contact Phone Number	*+1 (628) 214-2701*
GNRL-08	Country of Company Headquarters	*United States*

Documentation		Answer
DOCU-01	Do you have a well-documented business continuity plan (BCP), with a clear owner, that is tested annually?*	Yes
DOCU-02	Do you have a well-documented disaster recovery plan (DRP), with a clear owner, that is tested annually?*	Yes
DOCU-03	Have you undergone a SSAE 18/SOC 2 audit?	Yes
DOCU-04	Do you conform with a specific industry standard security framework (e.g., NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)?	Yes
DOCU-05	Can you provide overall system and/or application architecture diagrams, including a full description of the data flow for all components of the system?	Yes
DOCU-06	Does your organization have a data privacy policy?	Yes
DOCU-07	Do you have a documented, and currently implemented, employee onboarding and offboarding policy?	Yes

Assessment of Third Parties		Answer
THRD-01	Do you perform security assessments of third-party companies with which you share data (e.g., hosting providers, cloud services, PaaS, IaaS, SaaS)?*	Yes
THRD-02	Do you have contractual language in place with third parties governing access to institutional data?*	Yes
THRD-03	Do the contracts in place with these third parties address liability in the event of a data breach?*	Yes
THRD-04	Do you have an implemented third-party management strategy?*	Yes
THRD-05	Do you have a process and implemented procedures for managing your hardware supply chain (e.g., telecommunications equipment, export licensing, computing devices)?	Yes
Change Management		**Answer**
CHNG-01	Will the institution be notified of major changes to your environment that could impact the institution's security posture?*	Yes

CHNG-02	Does the system support client customizations from one release to another?*	Yes
CHNG-03	Do you have an implemented system configuration management process (e.g.,secure "gold" images, etc.)?*	Yes
CHNG-04	Do you have a documented change management process?	Yes
CHNG-05	Does your change management process minimally include authorization, impact analysis, testing, and validation before moving changes to production?	Yes
CHNG-06	Does your change management process verify that all required third-party libraries and dependencies are still supported with each major change?	Yes
CHNG-07	Do you have policy and procedure, currently implemented, managing how critical patches are applied to all systems and applications?	Yes
CHNG-08	Have you implemented policies and procedures that guide how security risks are mitigated until patches can be applied?	Yes
CHNG-09	Do clients have the option to not participate in or postpone an upgrade to a new release?	No

CHNG-10	Do you have a fully implemented solution support strategy that defines how many concurrent versions you support?	Yes
CHNG-11	Do you have a release schedule for product updates?	Yes
CHNG-12	Do you have a technology roadmap, for at least the next two years, for enhancements and bug fixes for the solution being assessed?	Yes
CHNG-13	Can solution updates be completed without institutional involvement (i.e., technically or organizationally)?	Yes
CHNG-14	Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?	Yes
CHNG-15	Do procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval)?	Yes
CHNG-16	Do you have a systems management and configuration strategy that encompasses servers, appliances, cloud services, applications, and mobile devices (company and employee owned)?	Yes
Policies, Processes, and Procedures		**Answer**
PPPR-01	Do you have a documented patch management process?*	Yes
PPPR-02	Can your organization comply with institutional policies on privacy and data protection with regard to users of institutional systems, if required?*	Yes

PPPR-03	Is your company subject to the institution's geographic region's laws and regulations?*	Yes
PPPR-04	Can you accommodate encryption requirements using open standards?	Yes
PPPR-05	Do you have a documented systems development life cycle (SDLC)?	Yes
PPPR-06	Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?	Yes
PPPR-07	Do you require new employees to fill out agreements and review policies?	Yes
PPPR-08	Do you have a documented information security policy?	Yes
PPPR-09	Are information security principles designed into the product lifecycle?	Yes
PPPR-10	Will you comply with applicable breach notification laws?	Yes
PPPR-11	Do you have an information security awareness program?	Yes
PPPR-12	Is security awareness training mandatory for all employees?	Yes
PPPR-13	Do you have process and procedure(s) documented, and currently followed, that require a review and update of the access list(s) for privileged accounts?	Yes
PPPR-14	Do you have documented, and currently implemented, internal audit processes and procedures?	Yes

PPPR-15	Does your organization have physical security controls and policies in place?	Yes

sections are required for your product or service.

ct through Privacy) that apply, based on your answers to the "Req

rmation." If leaving an answer blank, you must also state why in "

cation volunteers.

edible.

ud-hosted, shared-tenant Software as a Service solution. As the customer, you
modern web browser to design, create, deliver and a

Additional Information
Accredible maintains a comprehensive Business Continuity Plan reviewed and tested annually, ensuring service continuity in the event of disruption.
Accredible operates a documented Disaster Recovery Plan with defined recovery time objectives and periodic testing
Accredible is SOC2 Type 2 certified tested annually with a copy available under NDA; SOC3 is available here https://www.accredible.com/trust-center
Accredible aligns its security practices with established industry standards and frameworks. While Accredible does not currently maintain a formal ISO 27001 certification, the platform's policies and controls are designed to be consistent with widely recognized security frameworks such as ISO 27001, the NIST Cybersecurity
Diagrams are available here https://www.accredible.com/trust-center
https://www.accredible.com/legal/privacy-policy
Accredible maintains formal employee onboarding and offboarding policies as part of its internal security and compliance program. These policies govern account provisioning, role-based access control, device management, and the timely removal of access upon employee departure. Supporting documentation includes procedural checklists for onboarding (such as background checks, confidentiality agreements, and assignment of appropriate access)

Additional Information
Accredible conducts risk assessments before engaging with any third-party service provider, focusing on security, privacy, and recoverability. Reviews are refreshed periodically based on vendor criticality.
Accredible requires contractual obligations for confidentiality, security practices, incident reporting, and business continuity. These are standard terms in all third-party agreements.
Accredible maintains ongoing oversight of third parties, including periodic security reviews, evidence requests, and monitoring of compliance with contractual obligations. Vendors are re-assessed when scope or services change.
Accredible enforces the principle of least privilege. Third parties are granted access only to the data and systems required to deliver their contracted services. Access is time-bound, monitored, and revoked promptly when no longer required.
Accredible contracts mandate that third parties uphold security and confidentiality programs aligned with recognized industry standards (such as SOC 2, ISO 27001, or equivalent). Vendors must provide evidence of compliance during onboarding and renewal.

Additional Information
Accredible maintains a change communication process for material updates that could impact security posture or customer integrations. Notices are sent in advance through the customer communication channels and release notes, with timelines, impact

Accredible preserves customer configurations and white-label settings across releases. Backward compatibility is maintained for documented APIs and webhooks, and feature toggles minimize disruption. Deprecations follow an advance-notice process with guidance for transition.
Accredible uses infrastructure-as-code and hardened base images with baseline configurations, patching standards, and least-privilege access. Changes to system configurations follow peer review and approval prior to deployment.
Accredible's SDLC and change control procedures cover planning, risk assessment, approval, testing, deployment, and post-deployment verification, with records retained for audit
All non-emergency changes require documented approval, impact and rollback analysis, test evidence in staging, and validation/monitoring in production. Production access is limited and logged.
Dependency management, automated scanning for vulnerabilities and end-of-support risks, and upgrade gates during CI/CD to prevent deployment of unsafe or unsupported components.
Accredible applies security patches according to severity-based SLAs. Critical patches are prioritized and may be deployed outside normal windows following expedited review and verification.
When immediate patching is not possible, compensating controls are implemented, such as configuration changes, WAF rules, network segmentation, and enhanced monitoring until remediation is complete.
As a managed SaaS platform, Accredible applies platform updates to maintain security and reliability. Where feasible, changes are backward compatible and communicated in advance. Customers may use feature flags, sandbox testing, and documented deprecation timelines to manage transitions; critical security patches are

Accredible operates a single current production version with API/version compatibility policies and documented deprecation timelines. Older interfaces are supported for a defined period with advance-notice and migration guidance.

Accredible follows a regular release cadence for enhancements and fixes, publishes release notes, and maintains a change calendar. Out-of-band releases are used for urgent security or stability updates.

Accredible maintains a forward-looking roadmap and quarterly plans.

As a SaaS provider, Accredible deploys updates without requiring customer action. For changes that may affect integrations or user experience, Accredible provides advance notice, guidance, and testing options.

Planned changes are executed during maintenance windows or using zero-/low-downtime deployment techniques. Customer-facing impact is minimized and communicated in advance where applicable.

An expedited emergency change procedure permits rapid remediation with immediate documentation, post-implementation review, and formal after-the-fact approval.

Accredible’s strategy covers cloud infrastructure, applications, and corporate devices. Cloud resources are defined via infrastructure-as-code with baseline controls; endpoints are managed with MDM for company-owned devices and policy-based controls, aligned to least-privilege and secure configuration standards.

Additional Information

Accredible conducts background checks on employees and contractors prior to granting access to systems, networks, or sensitive data. This includes identity verification, employment history, and criminal background screening in accordance with local laws.

All employees and contractors are required to sign confidentiality agreements as part of the onboarding process, committing them to safeguarding company and customer data during and after employment.

Accredible provides mandatory onboarding and annual refresher training on data security, privacy, and acceptable use. Additional targeted training is delivered when policies or risks change.
Accredible maintains an Acceptable Use Policy covering use of systems, data handling, prohibited activities, and user responsibilities. Compliance is mandatory for all personnel and reinforced through regular training.
Accredible enforces remote work security policies, including requirements for VPN usage, MFA, device encryption, and endpoint protection. Personal devices are restricted unless approved by IT/security
Accredible has a documented onboarding and offboarding process, including
Access is provisioned on a least-privilege basis, tied to role requirements. Access rights are reviewed periodically and adjusted based on job changes or terminations.
Accredible conducts scheduled access reviews for all critical systems to ensure access remains appropriate. Unused or unnecessary accounts are disabled promptly.
Accredible maintains a comprehensive set of security and privacy policies, including information security, data classification, incident response, access control, acceptable use, and vendor management. Policies are reviewed and updated annually.
Employees must acknowledge policies annually to ensure understanding and compliance. A record of acceptance is maintained as part of HR compliance tracking.
Accredible maintains a documented incident response plan covering detection, escalation, containment, investigation, remediation, and customer notification. The plan is reviewed
Accredible operates a disaster recovery program designed to restore critical systems and services within defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).
Accredible maintains a business continuity plan that identifies critical business functions, responsible owners, recovery strategies, and communication protocols. The plan ensures services can continue during unexpected disruptions.
Accredible’s information security program is formally approved and sponsored by senior management. Executive oversight ensures alignment with business objectives and resource allocation for ongoing improvements

Accredible has a designated security lead responsible for coordinating security policies, risk management, compliance, and incident response. This role ensures security is integrated across engineering, product, and operations.

Version 4.1.0

uired Questions."

'Additional Information".

u are an issuer of digital credentials and access a Dashboard web property via a
dministrate certificates and badges

Guidance	Analyst Notes
Provide the date of assessment and include a SOC 2 Type 2 (preferred) or SOC 3 report. If you have a SOC 3 report, state how to obtain a copy. Indicate if your hosting provider was the subject of the audit.	
Provide documentation on how your organization conforms to your chosen framework and indicate current certification levels, where appropriate	
Provide your diagrams (or a valid link to it) upon submission.	
Provide your data privacy document (or a valid link to it) upon submission.	
Provide a reference to your employee onboarding and offboarding policy and supporting documentation or submit it along with this fully populated HECVAT.	

Guidance	Analyst Notes
Provide a summary of your practices that assures that the third party will be subject to the appropriate standards regarding security, service recoverability, and confidentiality.	
List each third party and why institutional data is shared with them. Format example: [Third Party Name] - Reason	
Provide additional information that may help analysts better understand your environment and how it relates to third-party solutions.	
State what countries and/or regions this process is compliant with.	

Guidance	Analyst Notes
State how and when the institution will be notified of major changes to your environment.	

Describe or provide reference to your solution support strategy in regard to maintaining client customizations from one release to another.	
Summarize your implemented system configuration management precess.	
Summarize your current change management process.	
Indicate all procedures that are implemented in your change management process. (a) An impact analysis of the upgrade is performed. (b) The change is	
Please describe your program to track these dependancies.	
Summarize the policy and procedure(s) managing how critical patches are applied to systems and applications.	
Summarize the policy and procedure(s) guiding risk mitigation practices before critical patches can be applied.	
Summarize why clients do not have alternative release options.	

Describe or provide a reference to your solution support strategy in regard to maintaining software currency (i.e., how many concurrent versions are you willing to run and support?).	
Provide a reference to this solution's release schedule.	
Provide a reference to your technology roadmap.	
Define current off-peak hours, including time zones as necessary.	
Summarize implemented procedures ensuring that emergency changes are documented and authorized.	
ppp	

Guidance	Analyst Notes
State that you have reviewed the institution's IT policies with regards to user privacy and data protection.	

Briefly summarize your SDLC or provide a link or attachment.	
Summarize your background check practices.	
Summarize the required agreements and reviewed policies.	
Provide a reference to your information security policy or submit documentation with this fully populated HECVAT.	
Summarize the information security principles designed into the product lifecycle.	
State how quickly the institution will be notified of a data breach or security	
Summarize your information security awareness program.	
Summarize your security awareness training content and state how frequently	
Provide a brief summary and the implement review interval.	
Summarize your internal audit processes and procedures.	

Provide a copy of your physical security controls and policies along with this document (link or attached).	

HECVAT Solution Provider Response - *Product*

Date Completed	*12/9/2025*

Instructions for Solution Providers

1. Complete the "Start Here" tab and review the "Required Questions" guidance to find the other

2. Complete the "Organization" tab and the applicable questions in each of the next 5 tabs (Produ

3. Guidance in column E may change based on your answers to prompt details in "Additional Info

4. DO NOT complete any fields in the "Evaluation" sheets or the "Analyst Notes" column.

5. Return the completed file to institutions.

** Denotes critical questions. Critical questions are those deemed most important to institutions by higher edu*

For full instructions, please visit educause.edu/HECVAT

General Information		Answer
GNRL-01	Solution Provider Name	*EdInvent Inc. d.b.a. Accre*
GNRL-02	Solution Name	*Accredible*
GNRL-03	Solution Description	*Accredible is a clo*
GNRL-08	Country of Company Headquarters	*United States*

Required Questions		Answer
REQU-01	Are you offering either a product or platform, as opposed to only offering a service	Yes

Authentication, Authorization, and Account Management		Answer
AAAI-01	Does your solution support single sign-on (SSO) protocols for user and administrator authentication?*	Yes
AAAI-02	For customers not using SSO, does your solution support local authentication protocols for user and administrator authentication?*	Yes

AAAI-03	For customers not using SSO, can you enforce password/passphrase complexity requirements (provided by the institution)?*	Yes
AAAI-04	For customers not using SSO, does the system have password complexity or length limitations and/or restrictions?*	Yes
AAAI-05	For customers not using SSO, do you have documented password/passphrase reset procedures that are currently implemented in the system and/or customer support?*	Yes
AAAI-06	Does your organization participate in InCommon or another eduGAIN-affiliated trust federation?*	Yes
AAAI-07	Are there any passwords/passphrases hard-coded into your systems or solutions?*	No
AAAI-08	Are you storing any passwords in plaintext?*	No
AAAI-09	Are audit logs available that include AT LEAST all of the following: login, logout, actions performed, and source IP address?*	Yes
AAAI-10	Describe or provide a reference to the (a) system capability to log security/authorization changes, as well as user and administrator security events (i.e., physical or electronic), such as login failures, access denied, changes accepted; and (b) all requirements necessary to implement logging and monitoring on the system. Include (c) information about SIEM/log collector usage.*	Yes
AAAI-11	Can you provide the institution documentation regarding the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how)?*	Yes
AAAI-12	For customers not using SSO, does your application support integration with other authentication and authorization systems?	Yes

AAAI-13	Do you allow the customer to specify attribute mappings for any needed information beyond a user identifier? (e.g., Reference eduPerson, ePPA/ePPN/ePE)	Yes
AAAI-14	For customers not using SSO, does your application support directory integration for user accounts?	Yes
AAAI-15	Does your solution support any of the following web SSO standards: SAML2 (with redirect flow), OIDC, CAS, or other?	Yes
AAAI-16	Do you support differentiation between email address and user identifier?	Yes
AAAI-17	For customers not using SSO, does your application and/or user frontend/portal support multifactor authentication (e.g., Duo, Google Authenticator, OTP, etc.)?	Yes
AAAI-18	Does your application automatically lock the session or log out an account after a period of inactivity?	Yes
Data		**Answer**
DATA-01	Will the institution's data be stored on any devices (database servers, file servers, SAN, NAS, etc.) configured with non-RFC 1918/4193 (i.e., publicly routable) IP addresses?*	No
DATA-02	Is the transport of sensitive data encrypted using security protocols/algorithms (e.g., system-to-client)?*	Yes
DATA-03	Is the storage of sensitive data encrypted using security protocols/algorithms (e.g., disk encryption, at-rest, files, and within a running database)?*	Yes
DATA-04	Do all cryptographic modules in use in your solution conform to the Federal Information Processing Standards (FIPS PUB 140-2 or 140-3)?*	Yes

DATA-05	Will the institution's data be available within the system for a period of time at the completion of this contract?*	Yes
DATA-06	Are these rights retained even through a provider acquisition or bankruptcy event?*	Yes
DATA-07	Do backups containing the institution's data ever leave the institution's data zone either physically or via network routing?*	No
DATA-08	Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?*	Yes
DATA-09	At the completion of this contract, will data be returned to the institution and/or deleted from all your systems and archives?	Yes
DATA-10	Can the institution extract a full or partial backup of data?	Yes
DATA-11	Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?	Yes
DATA-12	Are you performing off-site backups (i.e., digitally moved off site)?	Yes
DATA-13	Are physical backups taken off-site (i.e., physically moved off site)?	No
DATA-14	Are data backups encrypted?	Yes
DATA-15	Do you have a media handling process that is documented and currently implemented that meets established business needs and regulatory requirements, including end-of-life, repurposing, and data-sanitization procedures?	Yes
DATA-16	Does the process described in DATA-15 adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?	Yes

DATA-17	Does your staff (or third party) have access to institutional data (e.g., financial, PHI, or other sensitive information) through any means?	Limited and controlled
DATA-18	Do you have a documented and currently implemented strategy for securing employee workstations when they work remotely (i.e., not in a trusted computing environment)?	Yes
DATA-19	Does the environment provide for dedicated single-tenant capabilities? If not, describe how your solution or environment separates data from different customers (e.g., logically, physically, single tenancy, multi-tenancy).	Logical separation
DATA-20	Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?	Yes
DATA-21	In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide 90 days for customers to get their data out of the system and migrate applications?	Yes
DATA-22	Are involatile backup copies made according to predefined schedules and securely stored and protected?	Yes
DATA-23	Do you have a cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement) that is documented and currently implemented, for all system components (e.g., database, system, web, etc.)?	Yes

sections are required for your product or service.
ct through Privacy) that apply, based on your answers to the "Req
rmation." If leaving an answer blank, you must also state why in "

cation volunteers.

edible.

ud-hosted, shared-tenant Software as a Service solution. As the customer, you
modern web browser to design, create, deliver and a

Accredible provides a SaaS-based digital credentialing platform that enables organizations to issue, manage, and verify digital certificates and badges. Implementation and support services are provided to ensure success but are not the primary offering.

Additional Information

Accredible supports SAML 2.0 and OAuth/OIDC for SSO, enabling secure and seamless authentication for both administrators and end users.

Local authentication is supported with username/password login for customers not implementing SSO.

Password policies can be configured to align with institutional requirements, including minimum length, character mix, and expiration.
Passwords must meet minimum complexity requirements. Accredible enforces strong password standards by default.
Accredible provides automated password reset capabilities and documented support processes to ensure secure recovery.
Accredible supports integration with InCommon and other eduGAIN federations for academic institutions.
Hard-coded passwords are prohibited by policy and verified by code review and automated scanning.
Accredible never stores plaintext passwords. All passwords are salted and hashed with strong algorithms (e.g., bcrypt).
Detailed audit logs capture authentication and authorization events, user activity, and originating IP addresses.
Accredible logs login failures, access denied, and security changes. Logs can be exported to a SIEM or log collector for monitoring.
Logs are retained per policy, protected by encryption and access controls, and may be made available to customers under NDA.
Accredible supports directory and identity system integrations via SAML, OIDC, and SCIM.

Accredible supports attribute mapping, including eduPerson attributes (e.g., ePPN, ePE) where required.
Directory integration with LDAP/AD and similar services is supported through SAML/OIDC.
Accredible supports SAML 2.0, OAuth/OIDC, and other federation protocols for secure SSO.
Accredible can differentiate identifiers from email addresses, enabling flexible authentication design.
MFA is supported using TOTP-based authenticators and institutional SSO integrations with MFA enforcement.
Session timeouts and inactivity auto-logout are enforced according to best practices.

Additional Information
Accredible's data is hosted in secure VPCs within AWS using private RFC 1918 address space. Data is never stored on publicly routable IP devices.
All transport of sensitive data uses TLS 1.2+ encryption between clients and systems, and system-to-system integrations.
All data at rest is encrypted with AES-256 encryption, including files, disks, and databases.
Accredible uses FIPS 140-2/3 validated modules through AWS KMS and TLS libraries.

Accredible provides customers with a defined period of access to export their data at the end of a contract.
Accredible contracts guarantee customer ownership rights in the event of acquisition or bankruptcy.
Backups remain within the designated AWS region. Data is not moved outside its hosting zone.
Data is stored in redundant, environmentally controlled AWS facilities with strong physical security.
Accredible securely returns data to customers and deletes all data from systems and backups in compliance with NIST 800-88.
Customers can export full or partial datasets through APIs and administrative tools.
Backups include the application and data layers needed to restore service.
Accredible replicates backups across AWS availability zones and regions.
Accredible does not transport physical media. Backups are cloud-native only.
All backups are encrypted in transit and at rest using AES-256.
Accredible maintains a documented process for data lifecycle management, including secure wiping, repurposing, and destruction of data media.
Data sanitization follows NIST SP 800-88 and DoD 5220.22-M standards.

Access is strictly limited to authorized personnel under least privilege. All access is logged and monitored, and vendors are bound by contractual security requirements.
Accredible enforces security for remote employees through VPN, MFA, device encryption, endpoint protection, and MDM.
Accredible operates a multi-tenant SaaS platform with strict logical data separation, encryption, and access controls per tenant.
Customers retain full ownership of their data at all times. Accredible does not claim rights over inputs, outputs, or metadata.
Accredible provides customers at least 90 days to retrieve and migrate data in the event of closure or bankruptcy.
Immutable backups are created per schedule, encrypted, and stored securely with restricted access.
Accredible maintains a documented cryptographic key management process covering generation, rotation, exchange, secure storage, and replacement using AWS KMS and FIPS-compliant standards.

Version 4.1.0

uired Questions."
'Additional Information".

u are an issuer of digital credentials and access a Dashboard web property via a
dministrate certificates and badges

Guidance	Analyst Notes
DO complete the Product and Infrastructure worksheets	

Guidance	Analyst Notes
Describe how strong authentication is enforced (e.g., complex passwords, multifactor tokens, certificates, biometrics, aging requirements, re-use policy).	
Provide a detailed description of your local authentication mode practices.	

Describe how password/passphrase complexity requirements are implemented in the product.	
Describe these limitations and/or restrictions and state what lengths and complexities are supported.	
Describe your documented password/passphrase reset procedures that are currently implemented in the system and/or customer support.	
List the entity IDs registered in the Additional Information column.	
List which systems and versions supported (such as Active Directory, Kerberos, or other LDAP compatible directory) in Additional Info.	

Describe all authentication services supported by the system.	
State the web SSO standards supported by your solution and provide additional details about your support, including framework(s) in use, how information is exchanged securely, etc.	
List all supported multifactor authentication methods, technologies, and/or solutions and provide a brief summary of each.	
Describe the default behavior of this capability.	

Guidance	Analyst Notes
Summarize your transport encryption strategy.	
Summarize your data encryption strategy and state what encryption options are available.	
Provide reference to FIPS 140-3 validation certificates.	

State the length of time that the institution's data will be available in the system at the completion of the contract.	
Provide references, as needed.	
Provide a general summary of your archival environment.	
State the length of time that the institution's data will be available in the system at the completion of the contract.	
Provide a general summary of how full and partial backups of data can be extracted.	
Decribe your overall strategy to accomplish these elements.	
Summarize your off-site backup strategy.	
State any plans to implement off-site physical backups in your environment.	
Summarize the encryption algorithm/strategy you are using to secure backups.	
Provide documented details of this process (link or attached).	

Provide a detailed summary outlining the security controls implemented to protect the institution's data.	
Provide reference to your data ownership documention.	
State how the institution will be notified of imminent termination.	
If your strategy uses different processes for services and data, ensure that all strategies are clearly stated and supported.	

HECVAT Solution Provider Response - *Infrastructure*

Date Completed	*12/9/2025*

Instructions for Solution Providers

1. Complete the "Start Here" tab and review the "Required Questions" guidance to find the other

2. Complete the "Organization" tab and the applicable questions in each of the next 5 tabs (Produ

3. Guidance in column E may change based on your answers to prompt details in "Additional Info

4. DO NOT complete any fields in the "Evaluation" sheets or the "Analyst Notes" column.

5. Return the completed file to institutions.

** Denotes critical questions. Critical questions are those deemed most important to institutions by higher edu*

For full instructions, please visit educause.edu/HECVAT

General Information		**Answer**
GNRL-01	Solution Provider Name	*EdInvent Inc. d.b.a. Accre*
GNRL-02	Solution Name	*Accredible*
GNRL-03	Solution Description	*Accredible is a clo*
GNRL-08	Country of Company Headquarters	*United States*

Required Questions		**Answer**
REQU-01	Are you offering either a product or platform, as opposed to only offering a service	Yes

Application/Service Security		**Answer**
APPL-01	Are access controls for institutional accounts based on structured rules, such as role-based access control (RBAC), attribute-based access control (ABAC), or policy-based access control (PBAC)?*	Yes
APPL-02	Are you using a web application firewall (WAF)?*	Yes

APPL-03	Are only currently supported operating system(s), software, and libraries leveraged by the system(s)/application(s) that will have access to institution's data?*	Yes
APPL-04	Does your application require access to location or GPS data?	No
APPL-05	Does your application provide separation of duties between security administration, system administration, and standard user functions?*	Yes
APPL-06	Do you subject your code to static code analysis and/or static application security testing prior to release?*	Yes
APPL-07	Do you have software testing processes (dynamic or static) that are established and followed?*	Yes
APPL-08	Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or PBAC?	Yes
APPL-09	Does the system provide data input validation and error messages?	Yes
APPL-10	Do you have a process and implemented procedures for managing your software supply chain (e.g., libraries, repositories, frameworks, etc.)	Yes
APPL-11	Have your developers been trained in secure coding techniques?	Yes
APPL-12	Was your application developed using secure coding techniques?	Yes
APPL-13	If mobile, is the application available from a trusted source (e.g., App Store, Google Play Store)?	Yes

APPL-14	Do you have a fully implemented policy or procedure that details how your employees obtain administrator access to institutional instance of the application?	Yes
Datacenter		**Answer**
DCTR-01	Select your hosting option.	AWS
DCTR-02	Is a SOC 2 Type 2 report available for the hosting environment?	Yes
DCTR-03	Are you generally able to accommodate storing each institution's data within its geographic region?	Yes
DCTR-04	Are the data centers staffed 24 hours a day, seven days a week (i.e., 24 x 7 x 365)?	Yes
DCTR-05	Are your servers separated from other companies via a physical barrier, such as a cage or hard walls?	Yes
DCTR-06	Does a physical barrier fully enclose the physical space, preventing unauthorized physical contact with any of your devices?*	Yes
DCTR-07	Are your primary and secondary data centers geographically diverse?	Yes
DCTR-08	Is the service hosted in a high-availability environment?	Yes
DCTR-09	Is redundant power available for all data centers where institutional data will reside?	Yes

DCTR-10	Are redundant power strategies tested?*	Yes
DCTR-11	Does the center where the data will reside have cooling and fire-suppression systems that are active and regularly tested?	Yes
DCTR-12	Do you have Internet Service Provider (ISP) redundancy?	Yes
DCTR-13	Does every data center where the institution's data will reside have multiple telephone company or network provider entrances to the facility?	Yes
DCTR-14	Do you require multifactor authentication for all administrative accounts in your environment?	Yes
DCTR-15	Are you using your cloud provider's available hardening tools or pre-hardened images?	Yes
DCTR-16	Does your cloud solution provider have access to your encryption keys?	No
Firewalls, IDS, IPS, and Networking		**Answer**
FIDP-01	Are you utilizing a stateful packet inspection (SPI) firewall?*	Yes
FIDP-02	Do you have a documented policy for firewall change requests?*	Yes
FIDP-03	Have you implemented an intrusion detection system (network-based)?*	Yes
FIDP-04	Do you employ host-based intrusion detection?*	Yes
FIDP-05	Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?*	Yes
FIDP-06	Is authority for firewall change approval documented? Please list approver names or titles in Additional Info.	Yes
FIDP-07	Have you implemented an intrusion prevention system (network-based)?	Yes

FIDP-08	Do you employ host-based intrusion prevention?	Yes
FIDP-09	Are you employing any next-generation persistent threat (NGPT) monitoring?	Yes
FIDP-10	Is intrusion monitoring performed internally or by a third-party service?	Both
FIDP-11	Do you monitor for intrusions on a 24 x 7 x 365 basis?	Yes
Incident Handling		**Answer**
HFIH-01	Do you have a formal incident response plan?	Yes
HFIH-02	Do you either have an internal incident response team or retain an external team?	Yes
HFIH-03	Do you have the capability to respond to incidents on a 24 x 7 x 365 basis?	Yes
HFIH-04	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?	Yes
Vulnerability Management		**Answer**
VULN-01	Are your systems and applications scanned with an authenticated user account for vulnerabilities (that are remediated) prior to new releases?*	Yes
VULN-02	Will you provide results of application and system vulnerability scans to the institution?*	Yes
VULN-03	Will you allow the institution to perform its own vulnerability testing and/or scanning of your systems and/or application, provided that testing is performed at a mutually agreed upon time and date?*	Yes
VULN-04	Have your systems and applications had a third-party security assessment completed in the last year?	Yes

VULN-05	Do you regularly scan for common web application security vulnerabilities (e.g., SQL injection, XSS, XSRF, etc.)?	Yes
VULN-06	Are your systems and applications regularly scanned externally for vulnerabilities?	Yes

sections are required for your product or service.
ct through Privacy) that apply, based on your answers to the "Req
rmation." If leaving an answer blank, you must also state why in "

cation volunteers.

edible.

ud-hosted, shared-tenant Software as a Service solution. As the customer, you
modern web browser to design, create, deliver and a

Accredible provides a SaaS-based digital credentialing platform that enables organizations to issue, manage, and verify digital certificates and badges. Implementation and support services are provided to ensure success but are not the primary offering.
Additional Information
Accredible enforces role-based access control (RBAC) with least-privilege principles.
Accredible employs WAF protection through AWS services to mitigate web-based threats.

Accredible uses supported OS, libraries, and frameworks, with dependency scanning to detect unsupported components.
Accredible does not require or collect location/GPS data.
Administrative, security, and user functions are segregated by role and access policies.
Accredible applies static application security testing (SAST) as part of its CI/CD pipeline.
Automated and manual testing, including DAST and penetration testing, are applied pre-release.
Internal staff access is role-based with periodic reviews.
Accredible enforces input validation, sanitization, and safe error messages.
Dependency management, SBOM tracking, and vulnerability scanning are applied to third-party libraries.
All developers undergo secure coding training during onboarding and annually.
OWASP and secure coding practices are applied throughout the SDLC.
Accredible’s mobile-accessible features are distributed via trusted app stores.

Administrative access to customer instances follows documented approval, least-privilege, and logging procedures.
Additional Information
Accredible is hosted in AWS with enterprise-grade security.
Accredible offers EU and US hosting options via AWS
Redundant hosting across AWS availability zones and regions.
Redundancy and failover ensure high availability.

MFA is enforced for all privileged accounts.
Accredible uses pre-hardened AWS AMIs and CIS benchmarks.
Accredible manages encryption keys via AWS KMS; providers do not access customer keys.
Additional Information
Stateful firewalls are deployed for all network layers.
Firewall change requests require documented approval.
Network-based IDS is deployed.
Host-based IDS agents monitor servers.
All changes are logged and monitored.
Security/operations managers approve firewall changes.
Network-based IPS is active.

Host-level protections are deployed.
Advanced monitoring tools are deployed for APT detection.
Internal monitoring is supplemented with third-party services.
Continuous monitoring is in place through SIEM and SOC coverage.
Additional Information
Accredible maintains a documented IRP with defined roles, processes, and escalation paths.
Accredible uses an internal incident response team and external experts as needed.
Incident response coverage is continuous, leveraging monitoring and on-call teams.
Accredible maintains cyber liability insurance for coverage against outages, breaches, and incidents.
Additional Information
Vulnerability scans with authenticated accounts are performed in staging prior to release.
Accredible provides scan results upon request under NDA.
Customers may perform scans subject to scheduling agreements.
Accredible undergoes annual third-party penetration testing and SOC 2 audits.

OWASP Top 10 vulnerabilities are scanned and remediated regularly.
External vulnerability scans are conducted regularly by independent tools and third parties.

Version 4.1.0

uired Questions."
'Additional Information".

ı are an issuer of digital credentials and access a Dashboard web property via a ıdministrate certificates and badges

Guidance	Analyst Notes
DO complete the Product and Infrastructure worksheets	
Guidance	**Analyst Notes**
Describe available roles.	
Describe the currently implemented WAF.	

Please provide a list of all required dependencies.	
Please indicate any future plans that would require access to this data	
Describe or provide a reference to the facilities available in the system to provide separation of duties between security administration and system administration functions.	
Provide a list of all tools utilized during static code analysis or static application security testing.	
Describe testing processes, including but not limited to, development of test plans, personnel involved in the testing process, and authorized individual accountable for approval and certification of test results.	
Describe how your system(s) provide data input validation and error messages.	
Provide supporting documentation of your processes.	
Summarize your secure coding training.	
Summarize your secure coding practices.	
State the application title as listed within the trusted source.	

Describe or provide a reference that details how administrator access is handled (e.g., provisioning, principle of least privilege, deprovisioning, etc.).	

Guidance	Analyst Notes
Based on the response to DCTR-01, this question does not apply to this product or service.	
Based on the response to DCTR-01, this question does not apply to this product or service.	
Based on the response to DCTR-01, this question does not apply to this product or service.	
Based on the response to DCTR-01, this question does not apply to this product or service.	
State your primary and secondary data center locations. For cloud infrastructures, state the primary and secondary zones.	
Provide a summary to support your response selection.	
Based on the response to DCTR-01, this question does not apply to this product or service.	

Based on the response to DCTR-01, this question does not apply to this product or service.	
Based on the response to DCTR-01, this question does not apply to this product or service.	
Based on the response to DCTR-01, this question does not apply to this product or service.	
Based on the response to DCTR-01, this question does not apply to this product or service.	
State which model of MFA you are using.	

Guidance	Analyst Notes
Describe the currently implemented SPI firewall.	
Describe your documented firewall change request policy.	
Describe the currently implemented IDS.	
Describe the currently implemented host-based IDS solution(s).	
Describe your current network systems logging strategy.	
List approver names or titles.	
Describe the currently implemented IPS.	

Describe the currently implemented host-based IPS solution(s).	
Describe your NGPT monitoring strategy.	
In addition to stating your intrusion monitoring strategy, provide a brief summary of its implementation.	
Provide a brief summary of this activity.	
Guidance	**Analyst Notes**
Summarize or provide a link to your formal incident response plan.	
Summarize your incident response and reporting processes.	
Summarize your internal approach or reference your third-party contractor.	
Describe the coverage in place for this solution.	
Guidance	**Analyst Notes**
Provide a brief description.	
Provide a reference to security scan documentation.	
Provide reference to the process or procedure to set up security testing times and scopes.	
Provide the results with this document (link or attached), if possible. State the date of the last completed third-party security assessment.	

Decribe your external application vulnerability scanning strategy.	

HECVAT Solution Provider Response - *IT Accessibility*

Date Completed	*12/9/2025*

Instructions for Solution Providers

1. Complete the "Start Here" tab and review the "Required Questions" guidance to find the other

2. Complete the "Organization" tab and the applicable questions in each of the next 5 tabs (Produ

3. Guidance in column E may change based on your answers to prompt details in "Additional Info

4. DO NOT complete any fields in the "Evaluation" sheets or the "Analyst Notes" column.

5. Return the completed file to institutions.

** Denotes critical questions. Critical questions are those deemed most important to institutions by higher edu*

For full instructions, please visit educause.edu/HECVAT

General Information		**Answer**
GNRL-01	Solution Provider Name	*EdInvent Inc. d.b.a. Accre*
GNRL-02	Solution Name	*Accredible*
GNRL-03	Solution Description	*Accredible is a clo*
GNRL-08	Country of Company Headquarters	*United States*

Required Questions		**Answer**
REQU-02	Does your product or service have an interface?	Yes

IT Accessibility		**Answer**
ITAC-01	Solution Provider Accessibility Contact Name	Accredible Accessibility Team
ITAC-02	Solution Provider Accessibility Contact Title	Accessibility & Compliance Lead
ITAC-03	Solution Provider Accessibility Contact Email	accessibility@accredible.com
ITAC-04	Solution Provider Accessibility Contact Phone Number	

ITAC-05	Web Link to Accessibility Statement or VPAT	
ITAC-06	Has a VPAT or ACR been created or updated for the solution and version under consideration within the past 12 months?*	Yes
ITAC-07	Will your company agree to meet your stated accessibility standard or WCAG 2.1 AA as part of your contractual agreement for the solution?*	Yes
ITAC-08	Does the solution substantially conform to WCAG 2.1 AA?*	Yes
ITAC-09	Do you have a documented and implemented process for reporting and tracking accessibility issues?*	Yes
ITAC-10	Do you have documentation to support the accessibility features of your solution?	Yes
ITAC-11	Has a third-party expert conducted an audit of the most recent version of your solution?	Yes
ITAC-12	Do you have a documented and implemented process for verifying accessibility conformance?	Yes
ITAC-13	Have you adopted a technical or legal standard of conformance for the solution?	Yes
ITAC-14	Can you provide a current, detailed accessibility roadmap with delivery timelines?	Yes

ITAC-15	Do you expect your staff to maintain a current skill set in IT accessibility?	Yes
ITAC-16	Do you have documented processes and procedures for implementing accessibility into your development lifecycle?	Yes
ITAC-17	Can all functions of the application or service be performed using only the keyboard?	Yes
ITAC-18	Does your product rely on activating a special "accessibility mode," a "lite version," or using an alternate interface (including “overlay” or AI-based alternates) for accessibility purposes?	No

sections are required for your product or service.
ct through Privacy) that apply, based on your answers to the "Req
rmation." If leaving an answer blank, you must also state why in "

cation volunteers.

edible.

ud-hosted, shared-tenant Software as a Service solution. As the customer, you
modern web browser to design, create, deliver and a

Accredible includes both an administrative interface for issuing and managing credentials, and a recipient-facing interface that allows learners to view, share, and verify credentials easily.
Additional Information
Accredible maintains a dedicated accessibility contact available via our support and compliance channels.
This role oversees accessibility initiatives across the product lifecycle.
A monitored mailbox ensures timely responses to accessibility-related queries.

Accredible publishes its accessibility statement and VPAT on its Trust Center website. https://www.accredible.com/trust-center
Accredible maintains an updated VPAT/ACR, reviewed annually to ensure compliance with WCAG 2.1 AA.
Accredible contractually commits to WCAG 2.1 AA standards upon request.
The Accredible platform is designed and tested to substantially conform with WCAG 2.1 AA accessibility requirements.
Accredible maintains a formal accessibility issue reporting and tracking workflow, integrated into its support and product management systems.
Documentation describing accessibility features is available to customers and evaluators.
Accredible engages third-party experts for periodic audits of accessibility compliance.
Accredible validates accessibility as part of QA cycles and with external reviews, documented in the SDLC.
Accredible aligns with WCAG 2.1 AA as the technical accessibility conformance standard.
Accredible maintains an accessibility roadmap, including upcoming improvements, available under NDA.

Staff undergo training and continuing education in accessibility standards and practices.
Accessibility testing and review are integrated into design, development, and release processes.
Accredible ensures full keyboard navigation support, including issuing, managing, and consuming credentials.
The Accredible platform is designed to be fully accessible by default without requiring overlays, alternate modes, or separate interfaces.

Version 4.1.0

uired Questions."
'Additional Information".

u are an issuer of digital credentials and access a Dashboard web property via a
dministrate certificates and badges

Guidance	Analyst Notes
DO complete the IT Accessibility worksheet.	

Guidance	Analyst Notes

VPAT can also be added as an attachment	
State the date the VPAT was completed. Include this VPAT in your submission and/or link to its web location.	
Describe the process and any recent examples of fixes as a result of the process.	
Provide examples with links where possible.	
State when the audit was conducted and by whom. Include the results in your submission and/or link to its web location.	
Describe your processes and methodologies for validating accessibility conformance.	
Indicate which primary standards and all additional standards the solution meets.	
Comment on how far into the future the roadmap extends. Provide evidence (including links) of having delivered upon the accessibility roadmap in the past.	

Provide any further relevant information about how expertise is maintained; include any accessibility certifications staff may hold (e.g., IAAP WAS <https://www.accessibilityassociation.org/certifications> or DHS Trusted Tester <https://section508.gov/test/trusted-tester>).	
Provide further details in Additional Information.	
State when and on which platform this was verified.	

HECVAT Solution Provider Response - *Case-Specific Quest*

Date Completed	*12/9/2025*

Instructions for Solution Providers

1. Complete the "Start Here" tab and review the "Required Questions" guidance to find the other

2. Complete the "Organization" tab and the applicable questions in each of the next 5 tabs (Produ

3. Guidance in column E may change based on your answers to prompt details in "Additional Info

4. DO NOT complete any fields in the "Evaluation" sheets or the "Analyst Notes" column.

5. Return the completed file to institutions.

* *Denotes critical questions. Critical questions are those deemed most important to institutions by higher edu*

For full instructions, please visit educause.edu/HECVAT

General Information		**Answer**
GNRL-01	Solution Provider Name	*EdInvent Inc. d.b.a. Accre*
GNRL-02	Solution Name	*Accredible*
GNRL-03	Solution Description	*Accredible is a cl*
GNRL-08	Country of Company Headquarters	*United States*

Required Questions		**Answer**
REQU-03	Are you providing consulting services?	Yes

REQU-05	Does your solution process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act (HIPAA)?	No
REQU-06	Is the solution designed to process, store, or transmit credit card information?	No
REQU-07	Does operating your solution require the institution to operate a physical or virtual appliance in their own environment or to provide inbound firewall exceptions to allow your employees to remotely administer systems in the institution's environment?	No
Consulting Services		**Answer**
CONS-01	Will the consultant require access to the institution's network resources?*	No
CONS-02	Has the consultant received training on (sensitive, HIPAA, PCI, etc.) data handling?*	Yes (where applicable)
CONS-03	Is the data encrypted (at rest) while in the consultant's possession?*	Yes
CONS-04	Can access be restricted based on source IP address?*	Yes
CONS-05	Will the consulting take place on-premises?	No
CONS-06	Will the consultant require access to hardware in the institution's data centers?	No
CONS-07	Will the consultant require an account within the institution's domain (@*.edu)?	No
CONS-08	Will any data be transferred to the consultant's possession?	No
CONS-09	Will the consultant need remote access to the institution's network or systems?	No
HIPAA Compliance		**Answer**
HIPA-01	Do your workforce members receive regular training related to the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules and the HITECH Act?*	

HIPA-02	Have you identified areas of risk?*	
HIPA-03	Have the relevant policies/plans been tested?*	
HIPA-04	Have you entered into a Business Associate Agreements with all subcontractors who may have access to protected health information (PHI)?*	
HIPA-05	Do you monitor or receive information regarding changes in HIPAA regulations?	
HIPA-06	Has your organization designated HIPAA Privacy and Security officers as required by the rules?	
HIPA-07	Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)?	
HIPA-08	Have you conducted a risk analysis as required under the HIPAA Security Rule?	
HIPA-09	Have you taken actions to mitigate the identified risks?	
HIPA-10	Does your application require user and system administrator password changes at a frequency no greater than 90 days?	

HIPA-11	Does your application require users to set their own password after an administrator reset or on first use of the account?	
HIPA-12	Does your application lock out an account after a number of failed login attempts?	
HIPA-13	Does your application automatically lock or log-out an account after a period of inactivity?	
HIPA-14	Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e., database accounts, etc.)?	
HIPA-15	If the application is institution-hosted, can all service level and administrative account passwords be changed by the institution?	
HIPA-16	Does your application provide the ability to define user access levels?	
HIPA-17	Does your application support varying levels of access to administrative tasks defined individually per user?	
HIPA-18	Does your application support varying levels of access to records based on user ID?	
HIPA-19	Is there a limit to the number of groups to which a user can be assigned?	

HIPA-20	Do accounts used for solution provider-supplied remote support abide by the same authentication policies and access logging as the rest of the system?	
HIPA-21	Does the application log record access including specific user, date/time of access, and originating IP or device?	
HIPA-22	Does the application log administrative activity, such as user account access changes and password changes, including specific user, date/time of changes, and originating IP or device?	
HIPA-23	Do you retain logs for at least as long as required by HIPAA regulations?	
HIPA-24	Can the application logs be archived?	
HIPA-25	Can the application logs be saved externally?	
HIPA-26	Do you have a disaster recovery plan and emergency mode operation plan?	
HIPA-27	Can you provide a HIPAA compliance attestation document?	
HIPA-28	Are you willing to enter into a Business Associate Agreement (BAA)?	

HIPA-29	Do your data backup and retention policies and practices meet HIPAA requirements?	
Payment Card Industry Data Security Standard (PCI DSS)		**Answer**
PCID-01	Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?*	
PCID-02	Is the application listed as an approved Payment Application Data Security Standard (PA-DSS) application?*	
PCID-03	Does the system or solutions use a third party to collect, store, process, or transmit cardholder (payment/credit/debt card) data?*	
PCID-04	Do your systems or solutions store, process, or transmit cardholder (payment/credit/debt card) data?	
PCID-05	Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?	
PCID-06	Are you classified as a service provider?	
PCID-07	Are you on the list of Visa approved service providers?	
PCID-08	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?	
PCID-09	Describe the architecture employed by the system to verify and authorize credit card transactions.	

PCID-10	What payment processors/gateways does the system support?	
PCID-11	Can the application be installed in a PCI DSS–compliant manner?	
PCID-12	Include documentation describing the system's abilities to comply with the PCI DSS and any features or capabilities of the system that must be added or changed in order to operate in compliance with the standards.	

On-Premises Data Solutions		Answer
OPEM-01	Do you support role-based access control (RBAC) for system administrators?	
OPEM-02	Can your employees access customer systems remotely?	
OPEM-03	Can you provide overall system and/or application architecture diagrams including a full description of the data communications architecture for all components of the system?	
OPEM-04	Do you require remote management of the system?	
OPEM-05	If you answered "yes" to OPEM-04, are your remote actions and changes logged or otherwise visible to the campus?	

OPEM-06	If you maintain remote access to the system, will you handle data in a FERPA-compliant manner?	
OPEM-07	Do you support campus status monitoring through SNMPv3 or other means?	
OPEM-08	Describe or provide a reference to any other safeguards used to monitor for malicious activity.	
OPEM-09	Describe how long your organization has conducted business in this area.	
OPEM-10	Do you have existing higher education customers?	

tions

sections are required for your product or service.

ct through Privacy) that apply, based on your answers to the "Req

rmation." If leaving an answer blank, you must also state why in "

cation volunteers.

edible.

oud-hosted, shared-tenant Software as a Service solution. As the customer, yo
modern web browser to design, create, deliver and

Additional Information

Accredible does not operate as a consulting company. Professional services are provided only to support integration, onboarding, and credential program rollout, always in conjunction with the platform.

Accredible is not designed to handle PHI and does not process HIPAA-covered data. The platform is focused on credential and achievement data for education, training, and certification.

Accredible does not store, process, or transmit credit card information. Where billing is required, trusted PCI DSS–compliant third-party payment processors are used.

Accredible is a fully managed SaaS solution. It does not require the institution to operate appliances in their environment or to configure inbound firewall exceptions for Accredible staff.

Additional Information

Accredible’s SaaS platform is delivered fully managed in the cloud. Consulting support does not

Accredible staff providing professional services are trained in data security, privacy, and

All data handled by Accredible remains encrypted in transit and at rest within the platform. Consultants do not store institutional data locally.

If consulting requires system access, access restrictions (e.g., IP allowlisting, VPN) can be

Consulting engagements are typically delivered remotely. On-premises services are not required

Accredible is a cloud-native solution and does not require access to institutional hardware.

Accredible does not require domain accounts within the institution. Access is managed within

Data remains within the Accredible platform. Consultants do not extract or store institutional

Remote access to institutional networks or systems is not required. All services are delivered

Additional Information

Additional Information

Additional Information

Version 4.1.0

uired Questions."

'Additional Information".

ɔu are an issuer of digital credentials and access a Dashboard web property via a administrate certificates and badges

Guidance	Analyst Notes
DO complete the Consulting section in the Case-Specific worksheet	

DO NOT complete the HIPAA section in the Case-Specific worksheet	
DO NOT complete the PCI-DSS section in the Case-Specific worksheet	
DO NOT complete the On-Prem section in the Case-Specific worksheet	

Guidance	Analyst Notes
No need to answer CONS-07	
No need to answer CONS-09	

Guidance	Analyst Notes
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	

Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	

Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	

Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	

Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.	

Guidance	Analyst Notes
Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.	

Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.	

Guidance	Analyst Notes
Based on the response to REQU-07 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-07 on the "START HERE" tab, this question does not	
Based on the response to REQU-07 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-07 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-07 on the "START HERE" tab, this question does not apply to this product or service.	

Based on the response to REQU-07 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-07 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-07 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-07 on the "START HERE" tab, this question does not apply to this product or service.	
Based on the response to REQU-07 on the "START HERE" tab, this question does not apply to this product or service.	

HECVAT Solution Provider Response - *AI*

Date Completed	*12/9/2025*

Instructions for Solution Providers

1. Complete the "Start Here" tab and review the "Required Questions" guidance to find the other

2. Complete the "Organization" tab and the applicable questions in each of the next 5 tabs (Produ

3. Guidance in column E may change based on your answers to prompt details in "Additional Info

4. DO NOT complete any fields in the "Evaluation" sheets or the "Analyst Notes" column.

5. Return the completed file to institutions.

** Denotes critical questions. Critical questions are those deemed most important to institutions by higher edu*

For full instructions, please visit educause.edu/HECVAT

General Information		**Answer**
GNRL-01	Solution Provider Name	*EdInvent Inc. d.b.a. Accre*
GNRL-02	Solution Name	*Accredible*
GNRL-03	Solution Description	*Accredible is a clo*
GNRL-08	Country of Company Headquarters	*United States*

Required Questions		**Answer**
REQU-04	Does your solution have AI features, or are there plans to implement AI features in the next 12 months?	Yes

AI Qualifying Questions		**Answer**
AIQU-01	Does your solution leverage machine learning (ML) or do you plan to do so in the next 12 months?	Yes
AIQU-02	Does your solution leverage a large language model (LLM) or do you plan to do so in the next 12 months?	Yes

General AI Questions		**Answer**

AIGN-01	Does your solution have an AI risk model when developing or implementing your solution's AI model?*	Yes
AIGN-02	Can your solution's AI features be disabled by tenant and/or user?*	Yes
AIGN-03	Have your staff completed responsible AI training?*	Yes
AIGN-04	Please describe the capabilities of your solution's AI features.	Skills tagging and analytics
AIGN-05	Does your solution support business rules to protect sensitive data from being ingested by the AI model?	Yes
AI Policy		**Answer**
AIPL-01	Are your AI developer's policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks conspicuously posted, unambiguous, and implemented effectively?*	Yes
AIPL-02	Have you identified and measured AI risks?*	Yes
AIPL-03	In the event of an incident, can your solution's AI features be disabled in a timely manner?*	Yes
AIPL-04	If disabled because of an incident, can your solution's AI features be re-enabled in a timely manner?*	Yes
AIPL-05	Do you have documented technical and procedural processes to address potential negative impacts of AI as described by the AI Risk Management Framework (RMF)?	Yes
AI Data Security		**Answer**
AISC-01	If sensitive data is introduced to your solution's AI model, can the data be removed from the AI model by request?*	Yes

AISC-02	Is user input data used to influence your solution's AI model?*	No
AISC-03	Do you provide logging for your solution's AI feature(s) that includes user, date, and action taken?*	Yes
AISC-04	Please describe how you validate user inputs.	Validation and sanitization
AISC-05	Do you plan for and mitigate supply-chain risk related to your AI features?	Yes
AI Machine Learning		**Answer**
AIML-01	Do you separate ML training data from your ML solution data?*	Yes
AIML-02	Do you authenticate and verify your ML model's feedback?*	Yes
AIML-03	Is your ML training data vetted, validated, and verified before training the solution's AI model?	Yes
AIML-04	Is your ML training data monitored and audited?	Yes
AIML-05	Have you limited access to your ML training data to only staff with an explicit business need?	Yes
AIML-06	Have you implemented adversarial training or other model defense mechanisms to protect your ML-related features?	Yes
AIML-07	Do you make your ML model transparent through documentation and log inputs and outputs?	Yes
AIML-08	Do you watermark your ML training data?	No (not applicable)
AI Large Language Model (LLM)		**Answer**
AILM-01	Do you limit your solution's LLM privileges by default?*	Yes
AILM-02	Is your LLM training data vetted, validated, and verified before training the solution's AI model?*	Yes

AILM-03	Do any actions taken by your solution's LLM features or plugins require human intervention?*	Yes
AILM-04	Do you limit multiple LLM model plugins being called as part of a single input?*	Yes
AILM-05	Do you limit your solution's LLM resource use per request, per step, and per action?	Yes
AILM-06	Do you leverage LLM model tuning or other model validation mechanisms?	Yes

sections are required for your product or service.
ct through Privacy) that apply, based on your answers to the "Req
rmation." If leaving an answer blank, you must also state why in "

cation volunteers.

edible.

ud-hosted, shared-tenant Software as a Service solution. As the customer, you
modern web browser to design, create, deliver and a

Additional Information

Accredible uses AI and machine learning for credential fraud detection, analytics, and usage insights. Future roadmap items also include expanded AI capabilities, all aligned with ethical AI principles such as transparency, fairness, and human oversight.

Additional Information

Accredible uses Generative AI for a skills tagging feature. In this feature, a user can elect to generate skill tags for a given achievement, which takes the course description as an input, and suggests skills as an output.

Additional Information

Accredible identifies AI risks through vulnerability assessments, ethical AI review, and adherence to security/privacy frameworks. Risks are mitigated via secure development practices, bias testing, and oversight.
Accredible's AI features (e.g., skills tagging, analytics) are optional and can be enabled or disabled by customers as needed.
Relevant staff receive training on responsible AI practices, covering bias mitigation, data minimization, and compliance with AI governance principles.
Accredible uses generative AI and ML to analyze credential/course descriptions and provide skills tagging, fraud detection, and usage insights. Customer data is not used for training AI models.
Accredible ensures sensitive data (e.g., personal or institutional) is excluded from AI training. Only course description metadata is processed, and no customer-owned data is persisted within AI services.
Additional Information
Accredible maintains AI development policies that align with the NIST AI Risk Management Framework. These are communicated internally, implemented consistently, and reinforced through training and review.
Accredible identifies and measures risks such as bias, misuse, data leakage, and model drift. Risks are tracked and mitigated within the product risk management framework.
Accredible AI features can be immediately disabled by system administrators or customers if needed.
AI features can be safely re-enabled after remediation and validation of security or ethical issues.
Accredible maintains documented processes to identify, monitor, and mitigate potential negative AI impacts. This includes bias testing, ethical reviews, and continuous monitoring consistent with AI RMF guidance.
Additional Information
Accredible ensures no customer-owned sensitive data is used for AI model training. If sensitive data were inadvertently introduced, processes exist to remove it and retrain or roll back models.

Accredible AI features operate on course and credential metadata. User input data is not persisted or used for model training.
Accredible AI features generate logs that capture user activity, timestamp, and actions, which can be exported for compliance and monitoring.
Accredible applies input validation, sanitization, and schema enforcement to ensure only appropriate and safe data is processed by AI features.
Accredible manages supply-chain risks by vetting AI vendors, monitoring dependencies, and applying SBOM tracking and vulnerability scanning to all AI components.
Additional Information
Accredible separates ML training data from production solution data. Training is performed using non-customer data, and customer credential data is never used to train models.
ML outputs are validated against expected patterns, and feedback is subject to review and verification before influencing downstream actions.
Accredible vets and validates training data to ensure accuracy, quality, and absence of sensitive or inappropriate content.
Training datasets are monitored for drift and bias and are periodically reviewed and audited to ensure compliance with standards.
Access to ML training data is restricted on a least-privilege basis to approved engineering and data science staff.
Accredible applies defenses such as adversarial testing, anomaly detection, and fallback controls to protect ML models against manipulation.
Accredible maintains documentation of ML features, including inputs/outputs, and logs model activity for monitoring and audit purposes.
Accredible does not watermark training data, as only non-customer metadata is used. Instead, provenance controls and dataset validation processes ensure integrity.
Additional Information
Accredible applies least-privilege principles to LLM features, ensuring they only perform defined tasks within restricted contexts.
Accredible validates and vets all training datasets used for LLM features to ensure accuracy, compliance, and exclusion of sensitive data. Customer-owned data is never used for training.

Human-in-the-loop oversight is enforced for high-impact actions. LLM outputs support administrators and users but do not trigger irreversible actions without human confirmation.
Accredible restricts plugin chaining and enforces input/output controls to avoid unintended escalation or excessive API calls.
Resource usage limits, including token, step, and action thresholds, are applied to protect performance and reduce risk of abuse.
Accredible uses fine-tuning, validation datasets, and monitoring mechanisms to ensure safe, accurate, and reliable LLM feature performance.

Version 4.1.0

uired Questions."
'Additional Information".

ı are an issuer of digital credentials and access a Dashboard web property via a ıdministrate certificates and badges

Guidance	Analyst Notes
DO complete the Artificial Intelligence (AI) worksheet	
Guidance	**Analyst Notes**
Guidance	**Analyst Notes**

Looking for the capabilities, use-case, goals, and benefits of the AI model or feature(s).	

Guidance	Analyst Notes

Guidance	Analyst Notes

Looking for how the solution is checked for input anomalies, patterns, and malicious input rejection.	
Guidance	**Analyst Notes**
Looking for watermarking of training data to aid in your incident response.	
Guidance	**Analyst Notes**

HECVAT Solution Provider Response - *Privacy*

Date Completed	*12/9/2025*

Instructions for Solution Providers

1. Complete the "Start Here" tab and review the "Required Questions" guidance to find the other

2. Complete the "Organization" tab and the applicable questions in each of the next 5 tabs (Produ

3. Guidance in column E may change based on your answers to prompt details in "Additional Info

4. DO NOT complete any fields in the "Evaluation" sheets or the "Analyst Notes" column.

5. Return the completed file to institutions.

** Denotes critical questions. Critical questions are those deemed most important to institutions by higher edu*

For full instructions, please visit educause.edu/HECVAT

General Information		**Answer**
GNRL-01	Solution Provider Name	*EdInvent Inc. d.b.a. Accre*
GNRL-02	Solution Name	*Accredible*
GNRL-03	Solution Description	*Accredible is a clo*
GNRL-08	Country of Company Headquarters	*United States*
GNRL-09	Employee Work Locations (all)	*Accredibl* *All em*

Required Questions		**Answer**
REQU-04	Does your solution have AI features, or are there plans to implement AI features in the next 12 months?	Yes
REQU-05	Does your solution process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act (HIPAA)?	No
REQU-06	Is the solution designed to process, store, or transmit credit card information?	No

REQU-08	Does your solution have access to personal or institutional data?	Yes
General Privacy		**Answer**
PRGN-01	Does your solution process FERPA-related data?	Yes
PRGN-02	Does your solution process GDPR-related or PIPL-related data?	Yes
PRGN-03	Does your solution process personal data regulated by state law(s) (e.g., CCPA)?	Yes
PRGN-04	Does your solution process user-provided data that may contain regulated information?	Yes (limited)
PRGN-05	Web Link to Product/Service Privacy Notice	
Privacy-Specific Company Details		**Answer**
PCOM-01	Have you had a personal data breach in the past three years that involved reporting to a governmental agency, notice to individuals (including voluntary notice), or notice to another organization or institution?*	No
PCOM-02	Use this area to share information about your privacy practices that will assist those who are assessing your company data privacy program.*	Yes
PCOM-03	Have you had any data privacy policy or law violations in the past 36 months?	No

PCOM-04	Do you have a dedicated data privacy staff or office?	No (dedicated role, not separate office)
Privacy-Specific Documentation		**Answer**
PDOC-01	If you have completed a SOC 2 audit, does it include the Privacy Trust Service Principle?	No
PDOC-02	Do you conform with a specific industry-standard privacy framework (e.g., NIST Privacy Framework, GDPR, ISO 27701)?	Yes
PDOC-03	Does your employee onboarding and offboarding policy include training of employees on information security and data privacy?	Yes
Privacy of Third Parties		**Answer**
PTHP-01	Do you have contractual agreements with third parties that require them to maintain standards and to comply with all regulatory requirements?*	Yes
PTHP-02	Do you perform privacy impact assesments of third parties that collect, process, or have access to personal data to ensure they meet industry and regulatory standards and to mitigate harmful, unethical, or discriminatory impacts on data subjects?	Yes
Privacy Change Management		**Answer**
PCHG-01	Does your change management process include privacy review and approval?	Yes
PCHG-02	Do you have policy and procedure, currently implemented, guiding how privacy risks are mitigated until they can be resolved?	Yes
Privacy of Sensitive Data		**Answer**

PDAT-01	Do you collect, process, or store demographic information?*	Limited
PDAT-02	Do you capture or create genetic, biometric, or behaviometric information (e.g., facial recognition or fingerprints)?*	No
PDAT-03	Do you combine institutional data (including "de-identified," "anonymized," or otherwise masked data) with personal data from any other sources?*	No
PDAT-04	Is institutional data coming into or going out of the United States at any point during collection, processing, storage, or archiving?	Yes (if applicable)
PDAT-05	Do you capture device information (e.g., IP address, MAC address)?	Yes (minimal)
PDAT-06	Does any part of this service/project involve a web/app tracking component (e.g., use of web-tracking pixels, cookies)?	Yes
PDAT-07	Does your staff (or a third party) have access to institutional data (e.g., financial, PHI, or other sensitive information) through any means?	Limited and controlled
PDAT-08	Will you handle personal data in a manner compliant with all relevant laws, regulations, and applicable institution policies?	Yes
Privacy Policies and Procedures		**Answer**
PRPO-01	Do you have a documented privacy management process?	Yes
PRPO-02	Are privacy principles designed into the product lifecycle (i.e., privacy-by-design)?	Yes
PRPO-03	Will you comply with applicable breach notification laws?	Yes
PRPO-04	Will you comply with the institution's policies regarding user privacy and data protection?	Yes
PRPO-05	Is your company subject to the laws and regulations of the institution's geographic region?	Yes

PRPO-06	Do you have a privacy awareness/training program?*	Yes
PRPO-07	Is privacy awareness training mandatory for all employees?	Yes
PRPO-08	Is AI privacy and ethics awareness/training required for all employees who work with AI?	Yes
PRPO-09	Do you have any decision-making processes that are completely automated (i.e., there is no human involvement)?	No
PRPO-10	Do you have a documented process for managing automated processing, including validations, monitoring, and data subject requests?	Yes
PRPO-11	Do you have a documented policy for sharing information with law enforcement?	Yes
PRPO-12	Do you share any institutional data with law enforcement without a valid warrant?*	No
PRPO-13	Does your incident response team include a privacy analyst/officer?	Yes
International Privacy		**Answer**
INTL-01	Will data be collected from or processed in or stored in the European Economic Area (EEA)?	Yes
INTL-02	Do you have a data protection officer (DPO)?	Yes
INTL-03	Will you sign appropriate GDPR Standard Contractual Clauses (SCCs) with the institution?	Yes
INTL-04	Will data be collected from or processed in or stored in China?	Yes (if applicable)
INTL-05	Do you comply with PIPL security, privacy, and data localization requirements?	Yes
Data Privacy		**Answer**

DRPV-01	Have you performed a Data Privacy Impact Assesssment for the solution/project?	Yes
DRPV-02	Do you provide an end-user privacy notice about privacy policies and procedures that identify the purpose(s) for which personal information is collected, used, retained, and disclosed?	Yes
DRPV-03	Do you describe the choices available to the individual and obtain implicit or explicit consent with respect to the collection, use, and disclosure of personal information?	Yes
DRPV-04	Do you collect personal information only for the purpose(s) identified in the agreement with an institution or, if there is none, the purpose(s) identified in the privacy notice?	Yes
DRPV-05	Do you have a documented list of personal data your service maintains?	Yes
DRPV-06	Do you retain personal information for only as long as necessary to fulfill the stated purpose(s) or as required by law or regulation and thereafter appropriately dispose of such information?	Yes
DRPV-07	Do you provide individuals with access to their personal information for review and update (i.e., data subject rights)?	Yes
DRPV-08	Do you disclose personal information to third parties only for the purpose(s) identified in the privacy notice or with the implicit or explicit consent of the individual?	Yes
DRPV-09	Do you protect personal information against unauthorized access (both physical and logical)?	Yes
DRPV-10	Do you maintain accurate, complete, and relevant personal information for the purposes identified in the privacy notice?	Yes
DRPV-11	Do you have procedures to address privacy-related noncompliance complaints and disputes?	Yes
DRPV-12	Do you "anonymize," "de-identify," or otherwise mask personal data?	Yes

DRPV-13	Do you or your subprocessors use or disclose "anonymized," "de-identified," or otherwise masked data for any purpose other than those identified in the agreement with an institution (e.g., sharing with ad networks or data brokers, marketing, creation of profiles, analytics unrelated to services provided to institution)?	No
DRPV-14	Do you certify stop-processing requests, including any data that is processed by a third party on your behalf?	Yes
DRPV-15	Do you have a process to review code for ethical considerations?	Yes

Privacy and AI		Answer
DPAI-01	Does your service use AI for the processing of institutional data?	Yes (limited)
DPAI-02	Is any institutional data retained in AI processing?*	No
DPAI-03	Do you have agreements in place with third parties or subprocessors regarding the protection of customer data and use of AI?*	Yes
DPAI-04	Will institutional data be processed through a third party or subprocessor that also uses AI?	No
DPAI-05	Is AI processing limited to fully licensed commercial enterprise AI services?	Yes
DPAI-06	Will institutional data be used or processed by any shared AI services?	No
DPAI-07	Do you have safeguards in place to protect institutional data and data privacy from unintended AI queries or processing?	Yes
DPAI-08	Do you provide choice to the user to opt out of AI use?	No

sections are required for your product or service.
ct through Privacy) that apply, based on your answers to the "Req
rmation." If leaving an answer blank, you must also state why in "

cation volunteers.

edible.

ud-hosted, shared-tenant Software as a Service solution. As the customer, you
modern web browser to design, create, deliver and a

e is a globally distributed organization, so employees and contractors outside t
ployees and contractors are formally vetted in the same way, with uniform bac

Additional Information
Accredible uses AI and machine learning for credential fraud detection, analytics, and usage insights. Future roadmap items also include expanded AI capabilities, all aligned with ethical AI principles such as transparency, fairness, and human oversight.
Accredible is not designed to handle PHI and does not process HIPAA-covered data. The platform is focused on credential and achievement data for education, training, and certification.
Accredible does not store, process, or transmit credit card information. Where billing is required, trusted PCI DSS–compliant third-party payment processors are used.

Accredible processes personal data such as name, email, and credential metadata necessary to issue and manage credentials. Access is controlled, minimized, and governed by GDPR/CCPA-compliant policies. Institutional data is protected through encryption, access controls, and logical segregation.
Additional Information
Accredible may process limited student directory information (e.g., names, emails, achievement details) when issuing academic credentials. Accredible supports compliance with FERPA by ensuring access controls, encryption, and institutional control over shared data.
Accredible processes personal data from EU and China-based data subjects under GDPR and PIPL, respectively. Compliance includes data minimization, legal basis for processing, data subject rights, and Standard Contractual Clauses for cross-border transfers.
Accredible complies with CCPA and other state privacy laws by honoring access, deletion, and opt-out rights for data subjects.
Accredible processes user-provided credential data, which may include regulated personal information depending on institutional use cases. Customers remain controllers of the data, and Accredible enforces technical and contractual safeguards.
https://www.accredible.com/legal/privacy-policy
Additional Information
Accredible has not experienced any reportable personal data breaches in the past three years. Proactive monitoring, encryption, and access controls reduce breach likelihood, and an incident response plan is in place should an event occur.
Accredible maintains a GDPR- and CCPA-compliant privacy program that incorporates Privacy by Design, data minimization, and user rights management. Privacy policies are reviewed annually, and customers have transparency into subprocessor lists and data flows via the Trust Center.
Accredible has had no violations of privacy laws or policies. External audits and customer reviews confirm adherence to data privacy standards.

Accredible has a designated data privacy lead embedded in the compliance and engineering teams. This individual coordinates privacy policy enforcement, risk assessment, and response activities, ensuring compliance without maintaining a separate office.
Additional Information
Accredible aligns its privacy program with GDPR, CCPA, NIST Privacy Framework, and ISO 27701 standards. This includes privacy governance, risk management, and support for data subject rights.
Accredible requires all employees to complete training on data security and privacy as part of onboarding and refresher training annually. Policies also cover secure account provisioning and deprovisioning during onboarding and offboarding.
Additional Information
Accredible requires all third-party vendors and subprocessors to enter into contracts that mandate compliance with applicable laws and regulatory requirements, including GDPR, CCPA, and other privacy and security standards. Contracts also enforce confidentiality, incident reporting, and security safeguards.
Accredible conducts vendor due diligence and periodic reviews, including privacy and security assessments of third parties with access to personal data. This process ensures vendors adhere to regulatory standards and ethical data handling practices, and that risks to data subjects are mitigated.
Additional Information
Accredible’s change management process includes privacy impact review for new features and system changes. Product and engineering teams consult with privacy and compliance leads to ensure that changes do not introduce unnecessary data collection or risk.
Accredible maintains policies and procedures for risk treatment. If a privacy risk is identified, compensating controls (e.g., configuration restrictions, access limitations, enhanced monitoring) are applied until a permanent resolution is deployed.
Additional Information

Accredible may process limited demographic information only if provided by the institution as part of credential metadata. Accredible does not independently collect demographic data.
Accredible does not capture, process, or store biometric, genetic, or behaviometric information.
Accredible does not enrich or combine institutional data with third-party personal data sources. Data remains within the platform under institutional control.
Accredible may transfer data across borders for hosting redundancy. Safeguards such as SCCs, encryption, and regional hosting options ensure compliance with GDPR and other frameworks.
Accredible captures IP address and related metadata for security logging and fraud detection. MAC addresses are not collected.
Accredible uses essential cookies and limited analytics for service performance. No third-party advertising trackers are used.
Access to institutional data is restricted to authorized personnel under least-privilege, logged, and monitored. No PHI or PCI data is processed.
Accredible complies with GDPR, CCPA, FERPA, and other applicable privacy regulations. Institutional data is handled under strict policies and data processing agreements.
Additional Information
Accredible maintains a documented privacy management process aligned with GDPR, CCPA, and NIST Privacy Framework. This process covers governance, risk management, data subject rights, and vendor oversight.
Privacy-by-Design principles are embedded into Accredible’s SDLC, with privacy reviews performed during feature design, development, and deployment.
Accredible’s incident response plan includes compliance with GDPR, CCPA, and other breach notification requirements. Customers are notified promptly in accordance with laws.
Accredible accommodates institutional privacy policies by contract and through product configuration options.
Accredible operates globally and complies with applicable local, regional, and international laws where customers operate.

Accredible provides a privacy awareness program for all employees, including onboarding and annual refresher training.
Privacy awareness training is required for all employees and tracked for compliance.
Employees working with AI features complete additional training focused on ethical AI practices, bias prevention, and data minimization.
Accredible does not use fully automated decision-making for high-risk processes. AI features support human users but do not make binding determinations without oversight.
Accredible documents processes for monitoring automated functions, validating accuracy, and supporting subject rights such as opt-out of automated processing.
Accredible maintains a law enforcement request policy requiring review, legal validation, and leadership approval before disclosing any data.
Accredible requires a valid legal order or warrant before releasing institutional data to law enforcement.
Accredible's incident response team includes a designated privacy lead responsible for assessing privacy impacts during incidents.
Additional Information
Accredible provides hosting options in the EU/EEA and processes data in compliance with GDPR. Customers may select EU-based data residency.
Accredible has appointed a Data Protection Officer responsible for overseeing GDPR compliance, data protection governance, and data subject rights.
Accredible will execute SCCs with institutions to enable lawful cross-border data transfers outside the EEA.
Accredible may process limited personal data from China-based learners and applies PIPL-compliant practices, including data localization where required.
Accredible complies with China's Personal Information Protection Law (PIPL), ensuring data minimization, purpose limitation, user consent, and regional storage controls.
Additional Information

Accredible conducts Data Privacy Impact Assessments (DPIAs) for new features and services where personal data processing is material.
Accredible provides a Privacy Notice published on its Trust Center describing purposes of data use, retention, and disclosure.
Accredible provides individuals with rights to consent, opt-out, or control use of personal information as required under GDPR, CCPA, and other laws.
Accredible processes only the personal information needed to issue, verify, and manage credentials, consistent with institutional agreements or privacy notices.
Accredible maintains a data inventory and records of processing activities (ROPA) documenting personal data categories.
Accredible enforces a retention schedule aligned with contractual obligations and legal requirements. Data is securely deleted using NIST 800-88 standards when no longer required.
Accredible provides mechanisms for data subjects to access, correct, delete, or export their personal information.
Accredible shares data only with subprocessors as necessary to deliver services, with contractual safeguards in place. No data is sold or used for advertising.
Personal information is encrypted in transit and at rest, access is restricted by least-privilege, and data centers are protected by physical security controls.
Accredible relies on institutions and credential issuers to supply accurate data, and enforces checks to maintain relevance and integrity.
Complaints and disputes are logged, investigated, and resolved via established procedures with escalation to the privacy lead and, if necessary, regulators.
Accredible applies pseudonymization and anonymization where possible to reduce data exposure risks.

Accredible and its subprocessors do not use anonymized or de-identified data for advertising, profiling, or unrelated analytics.
Accredible certifies compliance with stop-processing requests and flows such obligations down to subprocessors.
Accredible incorporates ethical review into its SDLC, including privacy, fairness, and responsible AI reviews for relevant features.
Additional Information
Accredible uses AI for credential fraud detection, skills tagging, and analytics. Institutional data processed through AI features is limited to credential/course metadata.
Accredible AI features process data transiently. No institutional data is stored or retained within AI models.
Accredible contracts with subprocessors require compliance with privacy/security standards and prohibit use of institutional data for AI training.
Institutional data is not passed to third-party AI services for training or enrichment. Any AI services leveraged by subprocessors operate under contractual data protection obligations.
Accredible limits any external AI processing to enterprise-grade, licensed services that meet security and compliance requirements.
Accredible ensures institutional data is not exposed to shared or public AI services. AI processing occurs only in isolated, secure environments.
Accredible enforces strict access controls, input validation, and monitoring to prevent unintended or unauthorized AI queries.
Accredible uses Generative AI for a skills tagging feature. In this feature, a user can elect to generate skill tags for a given achievement, which takes the course description as an input, and suggests skills as an output.

Version 4.1.0

uired Questions."
'Additional Information".

ı are an issuer of digital credentials and access a Dashboard web property via a
ıdminister certificates and badges

the US have access to organization networks, product code or systems.
ckground checking, training, equipment and access control policies.

Guidance	Analyst Notes
DO complete the Artificial Intelligence (AI) worksheet	
DO NOT complete the HIPAA section in the Case-Specific worksheet	
DO NOT complete the PCI-DSS section in the Case-Specific worksheet	

DO complete the Privacy tab	
Guidance	**Analyst Notes**
Guidance	**Analyst Notes**

Describe your Data Privacy Office or plans, including size, talents, resources, etc.	
Guidance	**Analyst Notes**
Provide documentation on how your organization conforms to your chosen framework and indicate current certification levels, where appropriate.	
Guidance	**Analyst Notes**
Provide a summary of your practices that assures that the third party will be subject to the appropriate standards regarding data privacy.	
Guidance	**Analyst Notes**
Please describe your process for privacy review.	
Guidance	**Analyst Notes**

Describe the tracking component and what is done with the information.	

Guidance	Analyst Notes
Describe privacy management process or provide links or attach documentation.	
Summarize the privacy principles designed into the product lifecycle.	
State how quickly the institution will be notified.	

Summarize your privacy awareness training content and state how frequently employees are required to undergo privacy awareness training	
Provide documentation describing management processes.	
Guidance	**Analyst Notes**
Describe where and what activities will take place in the EEA.	
Provide the name and contact information for the DPO.	
Guidance	**Analyst Notes**

Guidance	**Analyst Notes**

There are cells within this worksheet are auto populated from the previous worksheets and drop down lists.

HECVAT™ Ins

Instructions for An

1. Upon initial review, yo
2. When evaluating an a
3. For questions that are
4. Each worksheet shows
5. If you are evaluating a

For full instructions, plea

Solution Provider Name

Solution Provider Conta

Solution Provider Conta

Solution Provider Conta

Solution Name

Solution Description

Date Prepared

HECVAT Anal

Institution Assessr

Instructions for An

1. Upon initial review, yo

2. When evaluating an a

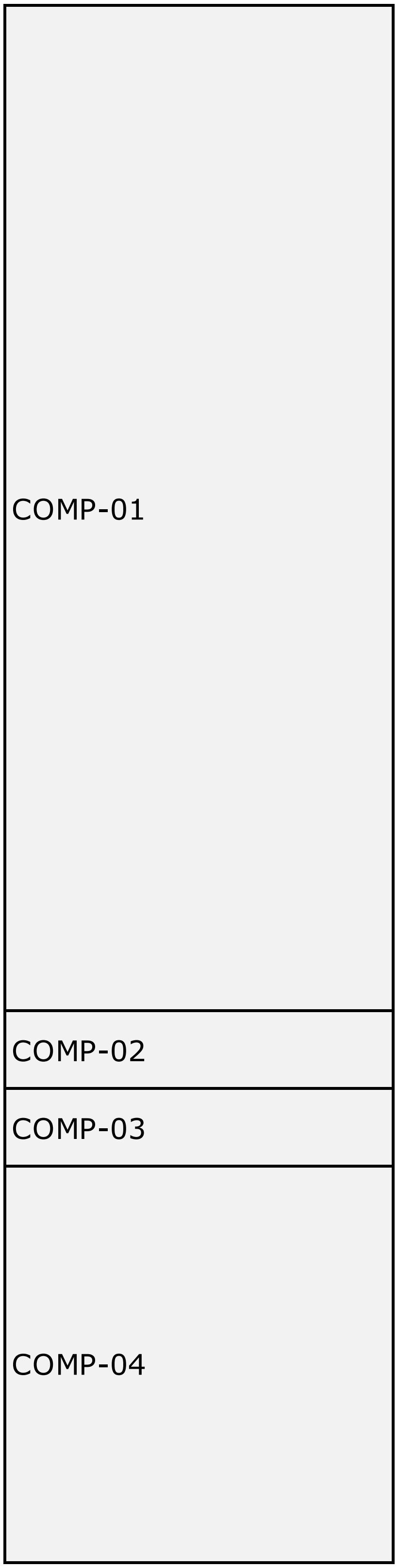
3. For questions that are

4. Each worksheet shows

5. If you are evaluating a

For full instructions, plea

ID
General Informati
GNRL-01
GNRL-02
GNRL-03
GNRL-04
GNRL-05
GNRL-06
GNRL-07
GNRL-08
GNRL-09
Company Informa


COMP-01
COMP-02
COMP-03
COMP-04

COMP-05

Required Question

REQU-01

REQU-02
REQU-03
REQU-04
REQU-05

REQU-06
REQU-07
REQU-08
Documentation
DOCU-01
DOCU-02

DOCU-03
DOCU-04
DOCU-05

DOCU-06
DOCU-07
Assessment of Thi
THRD-01

THRD-02
THRD-03
THRD-04
THRD-05
Change Manageme

CHNG-01
CHNG-02
CHNG-03

CHNG-04
CHNG-05
CHNG-06

CHNG-07
CHNG-08
CHNG-09

CHNG-10
CHNG-11
CHNG-12
CHNG-13
CHNG-14

CHNG-15
CHNG-16
Policies, Processes
PPPR-01
PPPR-02
PPPR-03
PPPR-04

PPPR-05
PPPR-06
PPPR-07
PPPR-08

PPPR-09
PPPR-10
PPPR-11

PPPR-12
PPPR-13
PPPR-14

PPPR-15
Authentication, Au
AAAI-01
AAAI-02
AAAI-03
AAAI-04

AAAI-05
AAAI-06
AAAI-07
AAAI-08
AAAI-09
AAAI-10
AAAI-11
AAAI-12
AAAI-13
AAAI-14

AAAI-15
AAAI-16
AAAI-17
AAAI-18
Data
DATA-01
DATA-02
DATA-03
DATA-04

DATA-05
DATA-06
DATA-07
DATA-08
DATA-09
DATA-10
DATA-11
DATA-12

DATA-13
DATA-14
DATA-15
DATA-16
DATA-17
DATA-18
DATA-19
DATA-20

DATA-21
DATA-22
DATA-23
Application/Servic
APPL-01
APPL-02
APPL-03
APPL-04

APPL-05
APPL-06
APPL-07
APPL-08
APPL-09
APPL-10
APPL-11

APPL-12
APPL-13
APPL-14
Datacenter
DCTR-01
DCTR-02
DCTR-03
DCTR-04
DCTR-05
DCTR-06

DCTR-07
DCTR-08
DCTR-09
DCTR-10
DCTR-11
DCTR-12
DCTR-13
DCTR-14
DCTR-15
DCTR-16
Firewalls, IDS, IPS

FIDP-01
FIDP-02
FIDP-03
FIDP-04
FIDP-05
FIDP-06
FIDP-07
FIDP-08
FIDP-09
FIDP-10
FIDP-11
Incident Handling
HFIH-01

HFIH-02
HFIH-03
HFIH-04
Vulnerability Mana
VULN-01
VULN-02
VULN-03
VULN-04
VULN-05
VULN-06
IT Accessibility

ITAC-01
ITAC-02
ITAC-03
ITAC-04
ITAC-05
ITAC-06
ITAC-07
ITAC-08
ITAC-09
ITAC-10
ITAC-11

ITAC-12
ITAC-13
ITAC-14
ITAC-15
ITAC-16

ITAC-17
ITAC-18
Consulting Service
CONS-01
CONS-02
CONS-03
CONS-03
CONS-04
CONS-05
CONS-06
CONS-07
CONS-08
CONS-09
HIPAA Compliance
HIPA-01

HIPA-02
HIPA-03
HIPA-04
HIPA-05
HIPA-06
HIPA-07

HIPA-08
HIPA-09
HIPA-10
HIPA-11
HIPA-12
HIPA-13

HIPA-14
HIPA-15
HIPA-16
HIPA-17
HIPA-18
HIPA-19

HIPA-20
HIPA-21
HIPA-22
HIPA-23
HIPA-24
HIPA-25

HIPA-26
HIPA-27
HIPA-28
HIPA-29
Payment Card Ind
PCID-01
PCID-02

PCID-03
PCID-04
PCID-05
PCID-06
PCID-07
PCID-08

PCID-09
PCID-10
PCID-11
PCID-12
On-Premises Data
OPEM-01
OPEM-02

OPEM-03
OPEM-04
OPEM-05
OPEM-06
OPEM-07
OPEM-08

OPEM-09
OPEM-10
AI Qualifying Que
AIQU-01
AIQU-02
General AI Questi
AIGN-01
AIGN-02
AIGN-03
AIGN-04
AIGN-05
AI Policy
AIPL-01
AIPL-02
AIPL-03

AIPL-04
AIPL-05
AI Data Security
AISC-01
AISC-02
AISC-03
AISC-04
AISC-05
AI Machine Learni
AIML-01
AIML-02
AIML-03
AIML-04
AIML-05
AIML-06
AIML-07
AIML-08
AI Large Languag
AILM-01

AILM-02
AILM-03
AILM-04
AILM-05
AILM-06

stitution Evaluation

alysts

u can check the "Non-Negotiable" box by any question to compile a report of
nswer, a default importance level has been set. You can use the "Importance
qualitative or for which you disagree with the preferred response, make a sel
s a report for that section. See the "Analyst Report" sheet for a full report of a
a question that appears in an earlier section, the Importance and Compliant O
se visit EDUCAUSE.edu/HECVAT

ct Name
ct Title
ct Email

Report Sections
Company Information
Documentation
Assessment of Third Parties

Change Management
Policies, Processes, and Procedures
Authentication, Authorization, and Account Management
Data
Application/Service Security
Datacenter
Firewalls, IDS, IPS, and Networking
Incident Handling
Vulnerability Management
Consulting Services

HIPAA Compliance
Payment Card Industry Data Security Standard (PCI DSS)
On-Premises Data Solutions
IT Accessibility
AI *(aggregated)*
Privacy *(aggregated)*
Overall Score

yst Report

nent

alysts

u can check the "Non-Negotiable" box by any question to compile a report of
nswer, a default importance level has been set. You can use the "Importance
qualitative or for which you disagree with the preferred response, make a sel
s a report for that section. See the "Analyst Report" sheet for a full report of a
a question that appears in an earlier section, the Importance and Compliant O
se visit EDUCAUSE.edu/HECVAT

Question
on
Solution Provider Name
Solution Name
Solution Description
Solution Provider Contact Name
Solution Provider Contact Title
Solution Provider Contact Email
Solution Provider Contact Phone Number
Country of Company Headquarters
Employee Work Locations (all)
tion

Do you have a dedicated software and system development team(s) (e.g., customer support, implementation, product management, etc.)?*
Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships.
Have you operated without unplanned disruptions to this solution in the past 12 months?
Do you have a dedicated information security staff or office?

Use this area to share information about your environment that will assist those who are assessing your company's data security program.

ns

Are you offering either a product or platform, as opposed to only offering a service

Does your product or service have an interface?
Are you providing consulting services?
Does your solution have AI features, or are there plans to implement AI features in the next 12 months?
Does your solution process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act (HIPAA)?

Is the solution designed to process, store, or transmit credit card information?
Does operating your solution require the institution to operate a physical or virtual appliance in their own environment or to provide inbound firewall exceptions to allow your employees to remotely administer systems in the institution's environment?
Does your solution have access to personal or institutional data?
Do you have a well-documented business continuity plan (BCP), with a clear owner, that is tested annually?*
Do you have a well-documented disaster recovery plan (DRP), with a clear owner, that is tested annually?*

Have you undergone a SSAE 18/SOC 2 audit?
Do you conform with a specific industry standard security framework (e.g., NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)?
Can you provide overall system and/or application architecture diagrams, including a full description of the data flow for all components of the system?

Does your organization have a data privacy policy?

Do you have a documented, and currently implemented, employee onboarding and offboarding policy?

rd Parties

Do you perform security assessments of third-party companies with which you share data (e.g., hosting providers, cloud services, PaaS, IaaS, SaaS)?*

Do you have contractual language in place with third parties governing access to institutional data?*
Do the contracts in place with these third parties address liability in the event of a data breach?*
Do you have an implemented third-party management strategy?*
Do you have a process and implemented procedures for managing your hardware supply chain (e.g., telecommunications equipment, export licensing, computing devices)?

ent

Will the institution be notified of major changes to your environment that could impact the institution's security posture?*
Does the system support client customizations from one release to another?*
Do you have an implemented system configuration management process (e.g.,secure "gold" images, etc.)?*

Do you have a documented change management process?
Does your change management process minimally include authorization, impact analysis, testing, and validation before moving changes to production?
Does your change management process verify that all required third-party libraries and dependencies are still supported with each major change?

Do you have policy and procedure, currently implemented, managing how critical patches are applied to all systems and applications?
Have you implemented policies and procedures that guide how security risks are mitigated until patches can be applied?
Do clients have the option to not participate in or postpone an upgrade to a new release?

Do you have a fully implemented solution support strategy that defines how many concurrent versions you support?
Do you have a release schedule for product updates?
Do you have a technology roadmap, for at least the next two years, for enhancements and bug fixes for the solution being assessed?
Can solution updates be completed without institutional involvement (i.e., technically or organizationally)?
Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?

Do procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval)?
Do you have a systems management and configuration strategy that encompasses servers, appliances, cloud services, applications, and mobile devices (company and employee owned)?
s, and Procedures
Do you have a documented patch management process?*
Can your organization comply with institutional policies on privacy and data protection with regard to users of institutional systems, if required?*
Is your company subject to the institution's geographic region's laws and regulations?*
Can you accommodate encryption requirements using open standards?

Do you have a documented systems development life cycle (SDLC)?
Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?
Do you require new employees to fill out agreements and review policies?
Do you have a documented information security policy?

Are information security principles designed into the product lifecycle?
Will you comply with applicable breach notification laws?
Do you have an information security awareness program?

Is security awareness training mandatory for all employees?
Do you have process and procedure(s) documented, and currently followed, that require a review and update of the access list(s) for privileged accounts?
Do you have documented, and currently implemented, internal audit processes and procedures?

Does your organization have physical security controls and policies in place?
uthorization, and Account Management
Does your solution support single sign-on (SSO) protocols for user and administrator authentication?*
For customers not using SSO, does your solution support local authentication protocols for user and administrator authentication?*
For customers not using SSO, can you enforce password/passphrase complexity requirements (provided by the institution)?*
For customers not using SSO, does the system have password complexity or length limitations and/or restrictions?*

For customers not using SSO, do you have documented password/passphrase reset procedures that are currently implemented in the system and/or customer support?*
Does your organization participate in InCommon or another eduGAIN-affiliated trust federation?*
Are there any passwords/passphrases hard-coded into your systems or solutions?*
Are you storing any passwords in plaintext?*
Are audit logs available that include AT LEAST all of the following: login, logout, actions performed, and source IP address?*
Describe or provide a reference to the (a) system capability to log security/authorization changes, as well as user and administrator security events (i.e., physical or electronic), such as login failures, access denied, changes accepted; and (b) all requirements necessary to implement logging and monitoring on the system. Include (c) information about SIEM/log collector usage.*
Can you provide the institution documentation regarding the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how)?*
For customers not using SSO, does your application support integration with other authentication and authorization systems?
Do you allow the customer to specify attribute mappings for any needed information beyond a user identifier? (e.g., Reference eduPerson, ePPA/ePPN/ePE)
For customers not using SSO, does your application support directory integration for user accounts?

Does your solution support any of the following web SSO standards: SAML2 (with redirect flow), OIDC, CAS, or other?
Do you support differentiation between email address and user identifier?
For customers not using SSO, does your application and/or user frontend/portal support multifactor authentication (e.g., Duo, Google Authenticator, OTP, etc.)?
Does your application automatically lock the session or log out an account after a period of inactivity?
Will the institution's data be stored on any devices (database servers, file servers, SAN, NAS, etc.) configured with non-RFC 1918/4193 (i.e., publicly routable) IP addresses?*
Is the transport of sensitive data encrypted using security protocols/algorithms (e.g., system-to-client)?*
Is the storage of sensitive data encrypted using security protocols/algorithms (e.g., disk encryption, at-rest, files, and within a running database)?*
Do all cryptographic modules in use in your solution conform to the Federal Information Processing Standards (FIPS PUB 140-2 or 140-3)?*

Will the institution's data be available within the system for a period of time at the completion of this contract?*
Are these rights retained even through a provider acquisition or bankruptcy event?*
Do backups containing the institution's data ever leave the institution's data zone either physically or via network routing?*
Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?*
At the completion of this contract, will data be returned to the institution and/or deleted from all your systems and archives?
Can the institution extract a full or partial backup of data?
Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?
Are you performing off-site backups (i.e., digitally moved off site)?

Are physical backups taken off-site (i.e., physically moved off site)?
Are data backups encrypted?
Do you have a media handling process that is documented and currently implemented that meets established business needs and regulatory requirements, including end-of-life, repurposing, and data-sanitization procedures?
Does the process described in DATA-15 adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?
Does your staff (or third party) have access to institutional data (e.g., financial, PHI, or other sensitive information) through any means?
Do you have a documented and currently implemented strategy for securing employee workstations when they work remotely (i.e., not in a trusted computing environment)?
Does the environment provide for dedicated single-tenant capabilities? If not, describe how your solution or environment separates data from different customers (e.g., logically, physically, single tenancy, multi-tenancy).
Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?

In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide 90 days for customers to get their data out of the system and migrate applications?
Are involatile backup copies made according to predefined schedules and securely stored and protected?
Do you have a cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement) that is documented and currently implemented, for all system components (e.g., database, system, web, etc.)?
ce Security
Are access controls for institutional accounts based on structured rules, such as role-based access control (RBAC), attribute-based access control (ABAC), or policy-based access control (PBAC)?*
Are you using a web application firewall (WAF)?*
Are only currently supported operating system(s), software, and libraries leveraged by the system(s)/application(s) that will have access to institution's data?*
Does your application require access to location or GPS data?

Does your application provide separation of duties between security administration, system administration, and standard user functions?*
Do you subject your code to static code analysis and/or static application security testing prior to release?*
Do you have software testing processes (dynamic or static) that are established and followed?*
Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or PBAC?
Does the system provide data input validation and error messages?
Do you have a process and implemented procedures for managing your software supply chain (e.g., libraries, repositories, frameworks, etc.)
Have your developers been trained in secure coding techniques?

Was your application developed using secure coding techniques?
If mobile, is the application available from a trusted source (e.g., App Store, Google Play Store)?
Do you have a fully implemented policy or procedure that details how your employees obtain administrator access to institutional instance of the application?
Select your hosting option.
Is a SOC 2 Type 2 report available for the hosting environment?
Are you generally able to accommodate storing each institution's data within its geographic region?
Are the data centers staffed 24 hours a day, seven days a week (i.e., 24 x 7 x 365)?
Are your servers separated from other companies via a physical barrier, such as a cage or hard walls?
Does a physical barrier fully enclose the physical space, preventing unauthorized physical contact with any of your devices?*

Are your primary and secondary data centers geographically diverse?
Is the service hosted in a high-availability environment?
Is redundant power available for all data centers where institutional data will reside?
Are redundant power strategies tested?*
Does the center where the data will reside have cooling and fire-suppression systems that are active and regularly tested?
Do you have Internet Service Provider (ISP) redundancy?
Does every data center where the institution's data will reside have multiple telephone company or network provider entrances to the facility?
Do you require multifactor authentication for all administrative accounts in your environment?
Are you using your cloud provider's available hardening tools or pre-hardened images?
Does your cloud solution provider have access to your encryption keys?
S, and Networking

Are you utilizing a stateful packet inspection (SPI) firewall?*
Do you have a documented policy for firewall change requests?*
Have you implemented an intrusion detection system (network-based)?*
Do you employ host-based intrusion detection?*
Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?*
Is authority for firewall change approval documented? Please list approver names or titles in Additional Info.
Have you implemented an intrusion prevention system (network-based)?
Do you employ host-based intrusion prevention?
Are you employing any next-generation persistent threat (NGPT) monitoring?
Is intrusion monitoring performed internally or by a third-party service?
Do you monitor for intrusions on a 24 x 7 x 365 basis?
Do you have a formal incident response plan?

Do you either have an internal incident response team or retain an external team?
Do you have the capability to respond to incidents on a 24 x 7 x 365 basis?
Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?
agement
Are your systems and applications scanned with an authenticated user account for vulnerabilities (that are remediated) prior to new releases?*
Will you provide results of application and system vulnerability scans to the institution?*
Will you allow the institution to perform its own vulnerability testing and/or scanning of your systems and/or application, provided that testing is performed at a mutually agreed upon time and date?*
Have your systems and applications had a third-party security assessment completed in the last year?
Do you regularly scan for common web application security vulnerabilities (e.g., SQL injection, XSS, XSRF, etc.)?
Are your systems and applications regularly scanned externally for vulnerabilities?

Solution Provider Accessibility Contact Name
Solution Provider Accessibility Contact Title
Solution Provider Accessibility Contact Email
Solution Provider Accessibility Contact Phone Number
Web Link to Accessibility Statement or VPAT
Has a VPAT or ACR been created or updated for the solution and version under consideration within the past 12 months?*
Will your company agree to meet your stated accessibility standard or WCAG 2.1 AA as part of your contractual agreement for the solution?*
Does the solution substantially conform to WCAG 2.1 AA?*
Do you have a documented and implemented process for reporting and tracking accessibility issues?*
Do you have documentation to support the accessibility features of your solution?
Has a third-party expert conducted an audit of the most recent version of your solution?

Do you have a documented and implemented process for verifying accessibility conformance?
Have you adopted a technical or legal standard of conformance for the solution?
Can you provide a current, detailed accessibility roadmap with delivery timelines?
Do you expect your staff to maintain a current skill set in IT accessibility?
Do you have documented processes and procedures for implementing accessibility into your development lifecycle?

Can all functions of the application or service be performed using only the keyboard?
Does your product rely on activating a special "accessibility mode," a "lite version," or using an alternate interface (including “overlay” or AI-based alternates) for accessibility purposes?
es
Will the consultant require access to the institution's network resources?*
Has the consultant received training on (sensitive, HIPAA, PCI, etc.) data handling?*
Is the data encrypted (at rest) while in the consultant's possession?*
Is the data encrypted (at rest) while in the consultant's possession?*
Can access be restricted based on source IP address?*
Will the consulting take place on-premises?
Will the consultant require access to hardware in the institution's data centers?
Will the consultant require an account within the institution's domain (@*.edu)?
Will any data be transferred to the consultant's possession?
Will the consultant need remote access to the institution's network or systems?
e
Do your workforce members receive regular training related to the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules and the HITECH Act?*

Have you identified areas of risk?*
Have the relevant policies/plans been tested?*
Have you entered into a Business Associate Agreements with all subcontractors who may have access to protected health information (PHI)?*
Do you monitor or receive information regarding changes in HIPAA regulations?
Has your organization designated HIPAA Privacy and Security officers as required by the rules?
Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)?

Have you conducted a risk analysis as required under the HIPAA Security Rule?
Have you taken actions to mitigate the identified risks?
Does your application require user and system administrator password changes at a frequency no greater than 90 days?
Does your application require users to set their own password after an administrator reset or on first use of the account?
Does your application lock out an account after a number of failed login attempts?
Does your application automatically lock or log-out an account after a period of inactivity?

Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e., database accounts, etc.)?
If the application is institution-hosted, can all service level and administrative account passwords be changed by the institution?
Does your application provide the ability to define user access levels?
Does your application support varying levels of access to administrative tasks defined individually per user?
Does your application support varying levels of access to records based on user ID?
Is there a limit to the number of groups to which a user can be assigned?

Do accounts used for solution provider-supplied remote support abide by the same authentication policies and access logging as the rest of the system?
Does the application log record access including specific user, date/time of access, and originating IP or device?
Does the application log administrative activity, such as user account access changes and password changes, including specific user, date/time of changes, and originating IP or device?
Do you retain logs for at least as long as required by HIPAA regulations?
Can the application logs be archived?
Can the application logs be saved externally?

Do you have a disaster recovery plan and emergency mode operation plan?
Can you provide a HIPAA compliance attestation document?
Are you willing to enter into a Business Associate Agreement (BAA)?
Do your data backup and retention policies and practices meet HIPAA requirements?

ustry Data Security Standard (PCI DSS)

Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?*
Is the application listed as an approved Payment Application Data Security Standard (PA-DSS) application?*

Does the system or solutions use a third party to collect, store, process, or transmit cardholder (payment/credit/debt card) data?*
Do your systems or solutions store, process, or transmit cardholder (payment/credit/debt card) data?
Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?
Are you classified as a service provider?
Are you on the list of Visa approved service providers?
Are you classified as a merchant? If so, what level (1, 2, 3, 4)?

Describe the architecture employed by the system to verify and authorize credit card transactions.

What payment processors/gateways does the system support?

Can the application be installed in a PCI DSS–compliant manner?

Include documentation describing the system's abilities to comply with the PCI DSS and any features or capabilities of the system that must be added or changed in order to operate in compliance with the standards.

Solutions

Do you support role-based access control (RBAC) for system administrators?

Can your employees access customer systems remotely?

Can you provide overall system and/or application architecture diagrams including a full description of the data communications architecture for all components of the system?
Do you require remote management of the system?
If you answered "yes" to OPEM-04, are your remote actions and changes logged or otherwise visible to the campus?
If you maintain remote access to the system, will you handle data in a FERPA-compliant manner?
Do you support campus status monitoring through SNMPv3 or other means?
Describe or provide a reference to any other safeguards used to monitor for malicious activity.

Describe how long your organization has conducted business in this area.
Do you have existing higher education customers?
stions
Does your solution leverage machine learning (ML) or do you plan to do so in the next 12 months?
Does your solution leverage a large language model (LLM) or do you plan to do so in the next 12 months?
ons
Does your solution have an AI risk model when developing or implementing your solution's AI model?*
Can your solution's AI features be disabled by tenant and/or user?*
Have your staff completed responsible AI training?*
Please describe the capabilities of your solution's AI features.
Does your solution support business rules to protect sensitive data from being ingested by the AI model?
Are your AI developer's policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks conspicuously posted, unambiguous, and implemented effectively?*
Have you identified and measured AI risks?*
In the event of an incident, can your solution's AI features be disabled in a timely manner?*

If disabled because of an incident, can your solution's AI features be re-enabled in a timely manner?*
Do you have documented technical and procedural processes to address potential negative impacts of AI as described by the AI Risk Management Framework (RMF)?
If sensitive data is introduced to your solution's AI model, can the data be removed from the AI model by request?*
Is user input data used to influence your solution's AI model?*
Do you provide logging for your solution's AI feature(s) that includes user, date, and action taken?*
Please describe how you validate user inputs.
Do you plan for and mitigate supply-chain risk related to your AI features?
ng
Do you separate ML training data from your ML solution data?*
Do you authenticate and verify your ML model's feedback?*
Is your ML training data vetted, validated, and verified before training the solution's AI model?
Is your ML training data monitored and audited?
Have you limited access to your ML training data to only staff with an explicit business need?
Have you implemented adversarial training or other model defense mechanisms to protect your ML-related features?
Do you make your ML model transparent through documentation and log inputs and outputs?
Do you watermark your ML training data?
e Model (LLM)
Do you limit your solution's LLM privileges by default?*

Is your LLM training data vetted, validated, and verified before training the solution's AI model?*
Do any actions taken by your solution's LLM features or plugins require human intervention?*
Do you limit multiple LLM model plugins being called as part of a single input?*
Do you limit your solution's LLM resource use per request, per step, and per action?
Do you leverage LLM model tuning or other model validation mechanisms?

JSE

questions that may prohibit a full review.
Override" dropdown to override the default and adjust the value of the questio
ection in the "Compliant Override" dropdown to adjust the question's impact or
ll sections.
verride cannot be changed but additional notes can be added.

EdInvent Inc. d.b.a. Accredible.
Alan Heppenstall
CTO
alan@accredible.com
Accredible
Accredible is a cloud-hosted, shared-tenant Software as a Service solution. As the
12/9/2025

Include in Score?	Max Score	Score
TRUE	30	25
TRUE	90	90
TRUE	90	90

TRUE	150	145
TRUE	145	145
TRUE	250	230
TRUE	280	255
TRUE	200	200
TRUE	170	170
TRUE	145	145
TRUE	25	25
TRUE	85	85
TRUE	130	110

TRUE	0	0
TRUE	0	0
TRUE	0	0
TRUE	170	170
TRUE	405	400
TRUE	565	495
	2,930	**2,780**

questions that may prohibit a full review.
Override" dropdown to override the default and adjust the value of the questio
ection in the "Compliant Override" dropdown to adjust the question's impact or
ıll sections.
›verride cannot be changed but additional notes can be added.

Answer	Additional Information	Guidance
EdInvent Inc. d.b.a. Accre		
Accredible		
Accredible is a cloud-host		
Alan Heppenstall		
CTO		
alan@accredible.com		
+1 (628) 214-2701		
United States		
Accredible is a globally dis		

Yes	Accredible maintains dedicated teams across engineering, product management, implementation, and customer support. Engineering focuses on platform reliability, integrations, and security. Product management ensures alignment with customer needs and industry trends. Implementation specialists oversee onboarding and rollout, while customer support provides responsive assistance. This structure ensures scalability and high-quality service delivery.	Describe the structure and size of your software and system development teams. (e.g., customer support, implementation, product management, etc.).
Yes		
Yes		
No	Accredible does not maintain a dedicated, standalone information security office. Instead, security responsibilities are integrated into its broader engineering, infrastructure, and compliance practices	Describe any plans to create an information security office for your organization.

	Security is integrated into the software development lifecycle, access management, and infrastructure operations. Controls align with ISO 27001, NIST CSF, and CIS Controls. Annual SOC 2 Type II audits validate effectiveness. Data is encrypted in transit and at rest, with least-privilege access enforced. Incident response and business continuity procedures are documented, tested, and reviewed regularly. Accredible maintains GDPR/CCPA-compliant privacy practices, and vendor risk management processes hold subprocessors to equivalent standards.	Share any details that would help information security analysts assess your solution.
Yes	Accredible provides a SaaS-based digital credentialing platform that enables organizations to issue, manage, and verify digital certificates and badges. Implementation and support services are provided to ensure success but are not the primary offering.	DO complete the Product and Infrastructure worksheets

Yes	Accredible includes both an administrative interface for issuing and managing credentials, and a recipient-facing interface that allows learners to view, share, and verify credentials easily.	DO complete the IT Accessibility worksheet.
Yes	Accredible does not operate as a consulting company. Professional services are provided only to support integration, onboarding, and credential program rollout, always in conjunction with the platform.	DO complete the Consulting section in the Case-Specific worksheet
Yes	Accredible uses AI and machine learning for credential fraud detection, analytics, and usage insights. Future roadmap items also include expanded AI capabilities, all aligned with ethical AI principles such as transparency, fairness, and human oversight.	DO complete the Artificial Intelligence (AI) worksheet
No	Accredible is not designed to handle PHI and does not process HIPAA-covered data. The platform is focused on credential and achievement data for education, training, and certification.	DO NOT complete the HIPAA section in the Case-Specific worksheet

No	Accredible does not store, process, or transmit credit card information. Where billing is required, trusted PCI DSS–compliant third-party payment processors are used.	DO NOT complete the PCI-DSS section in the Case-Specific worksheet
No	Accredible is a fully managed SaaS solution. It does not require the institution to operate appliances in their environment or to configure inbound firewall exceptions for Accredible staff.	DO NOT complete the On-Prem section in the Case-Specific worksheet
Yes	Accredible processes personal data such as name, email, and credential metadata necessary to issue and manage credentials. Access is controlled, minimized, and governed by GDPR/CCPA-compliant policies. Institutional data is protected through encryption, access controls, and logical segregation.	DO complete the Privacy tab
Yes		
Yes		

Yes	Accredible is SOC2 Type 2 certified tested annually with a copy available under NDA; SOC3 is available here https://www.accredible.com/trust-center	Provide the date of assessment and include a SOC 2 Type 2 (preferred) or SOC 3 report. If you have a SOC 3 report, state how to obtain a copy. Indicate if your hosting provider was the subject of the audit.
Yes	Accredible aligns its security practices with established industry standards and frameworks. While Accredible does not currently maintain a formal ISO 27001 certification, the platform's policies and controls are designed to be consistent with widely recognized security frameworks such as ISO 27001, the NIST Cybersecurity Framework, and the CIS Controls. These frameworks inform Accredible's approach to access management, encryption, incident response, vendor risk, and infrastructure security. Security is	Provide documentation on how your organization conforms to your chosen framework and indicate current certification levels, where appropriate.
Yes	Diagrams are available here https://www.accredible.com/trust-center	Provide your diagrams (or a valid link to it) upon submission.

Yes	https://www.accredible.com/legal/privacy-policy	Provide your data privacy document (or a valid link to it) upon submission.
Yes	Accredible maintains formal employee onboarding and offboarding policies as part of its internal security and compliance program. These policies govern account provisioning, role-based access control, device management, and the timely removal of access upon employee departure. Supporting documentation includes procedural checklists for onboarding (such as background checks, confidentiality agreements, and assignment of appropriate access) and for offboarding (such as immediate deactivation	Provide a reference to your employee onboarding and offboarding policy and supporting documentation or submit it along with this fully populated HECVAT.
[redacted]		
Yes	Accredible conducts risk assessments before engaging with any third-party service provider, focusing on security, privacy, and recoverability. Reviews are refreshed periodically based on vendor criticality.	Provide a summary of your practices that assures that the third party will be subject to the appropriate standards regarding security, service recoverability, and confidentiality.

Yes	Accredible requires contractual obligations for confidentiality, security practices, incident reporting, and business continuity. These are standard terms in all third-party agreements.	List each third party and why institutional data is shared with them. Format example: [Third Party Name] - Reason
Yes		
Yes	Accredible enforces the principle of least privilege. Third parties are granted access only to the data and systems required to deliver their contracted services. Access is time-bound, monitored, and revoked promptly when no longer required.	Provide additional information that may help analysts better understand your environment and how it relates to third-party solutions.
Yes	Accredible contracts mandate that third parties uphold security and confidentiality programs aligned with recognized industry standards (such as SOC 2, ISO 27001, or equivalent). Vendors must provide evidence of compliance during onboarding and renewal.	State what countries and/or regions this process is compliant with.

Yes	Accredible maintains a change communication process for material updates that could impact security posture or customer integrations. Notices are sent in advance through the customer communication channels and release notes, with timelines, impact descriptions, and required customer actions when applicable.	State how and when the institution will be notified of major changes to your environment.
Yes	Accredible preserves customer configurations and white-label settings across releases. Backward compatibility is maintained for documented APIs and webhooks, and feature toggles minimize disruption. Deprecations follow an advance-notice process with guidance for transition.	Describe or provide reference to your solution support strategy in regard to maintaining client customizations from one release to another.
Yes	Accredible uses infrastructure-as-code and hardened base images with baseline configurations, patching standards, and least-privilege access. Changes to system configurations follow peer review and approval prior to deployment.	Summarize your implemented system configuration management precess.

Yes	Accredible’s SDLC and change control procedures cover planning, risk assessment, approval, testing, deployment, and post-deployment verification, with records retained for audit	Summarize your current change management process.
Yes	All non-emergency changes require documented approval, impact and rollback analysis, test evidence in staging, and validation/monitoring in production. Production access is limited and logged.	Indicate all procedures that are implemented in your change management process. (a) An impact analysis of the upgrade is performed. (b) The change is appropriately authorized. (c) Changes are made first in a test environment. (d) The ability to implement the upgrades/changes in the production environment is limited to appropriate IT personnel.
Yes	Dependency management, automated scanning for vulnerabilities and end-of-support risks, and upgrade gates during CI/CD to prevent deployment of unsafe or unsupported components.	Please describe your program to track these dependancies.

Yes	Accredible applies security patches according to severity-based SLAs. Critical patches are prioritized and may be deployed outside normal windows following expedited review and verification.	Summarize the policy and procedure(s) managing how critical patches are applied to systems and applications.
Yes	When immediate patching is not possible, compensating controls are implemented, such as configuration changes, WAF rules, network segmentation, and enhanced monitoring until remediation is complete.	Summarize the policy and procedure(s) guiding risk mitigation practices before critical patches can be applied.
No	As a managed SaaS platform, Accredible applies platform updates to maintain security and reliability. Where feasible, changes are backward compatible and communicated in advance. Customers may use feature flags, sandbox testing, and documented deprecation timelines to manage transitions; critical security patches are not deferrable.	Summarize why clients do not have alternative release options.

Yes	Accredible operates a single current production version with API/version compatibility policies and documented deprecation timelines. Older interfaces are supported for a defined period with advance-notice and migration guidance.	Describe or provide a reference to your solution support strategy in regard to maintaining software currency (i.e., how many concurrent versions are you willing to run and support?).
Yes	Accredible follows a regular release cadence for enhancements and fixes, publishes release notes, and maintains a change calendar. Out-of-band releases are used for urgent security or stability updates.	Provide a reference to this solution's release schedule.
Yes	Accredible maintains a forward-looking roadmap and quarterly plans.	Provide a reference to your technology roadmap.
Yes		
Yes	Planned changes are executed during maintenance windows or using zero-/low-downtime deployment techniques. Customer-facing impact is minimized and communicated in advance where applicable.	Define current off-peak hours, including time zones as necessary.

Yes	An expedited emergency change procedure permits rapid remediation with immediate documentation, post-implementation review, and formal after-the-fact approval.	Summarize implemented procedures ensuring that emergency changes are documented and authorized.
Yes	Accredible’s strategy covers cloud infrastructure, applications, and corporate devices. Cloud resources are defined via infrastructure-as-code with baseline controls; endpoints are managed with MDM for company-owned devices and policy-based controls, aligned to least-privilege and secure configuration standards.	ppp
[redacted]		
Yes		
Yes	All employees and contractors are required to sign confidentiality agreements as part of the onboarding process, committing them to safeguarding company and customer data during and after employment.	State that you have reviewed the institution's IT policies with regards to user privacy and data protection.
Yes		
Yes		

Yes	Accredible enforces remote work security policies, including requirements for VPN usage, MFA, device encryption, and endpoint protection. Personal devices are restricted unless approved by IT/security.	Briefly summarize your SDLC or provide a link or attachment.
Yes	Accredible has a documented onboarding and offboarding process, including provisioning/deprovisioning accounts, role-based access assignment, return or wiping of devices, and termination of system access on the last day of employment.	Summarize your background check practices.
Yes	Access is provisioned on a least-privilege basis, tied to role requirements. Access rights are reviewed periodically and adjusted based on job changes or terminations.	Summarize the required agreements and reviewed policies.
Yes	Accredible conducts scheduled access reviews for all critical systems to ensure access remains appropriate. Unused or unnecessary accounts are disabled promptly.	Provide a reference to your information security policy or submit documentation with this fully populated HECVAT.

Yes	Accredible maintains a comprehensive set of security and privacy policies, including information security, data classification, incident response, access control, acceptable use, and vendor management. Policies are reviewed and updated annually.	Summarize the information security principles designed into the product lifecycle.
Yes	Employees must acknowledge policies annually to ensure understanding and compliance. A record of acceptance is maintained as part of HR compliance tracking.	State how quickly the institution will be notified of a data breach or security incident.
Yes	Accredible maintains a documented incident response plan covering detection, escalation, containment, investigation, remediation, and customer notification. The plan is reviewed annually and tested through tabletop exercises.	Summarize your information security awareness program.

Yes	Accredible operates a disaster recovery program designed to restore critical systems and services within defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Plans are tested periodically to validate effectiveness.	Summarize your security awareness training content and state how frequently employees are required to undergo security awareness training.
Yes	Accredible maintains a business continuity plan that identifies critical business functions, responsible owners, recovery strategies, and communication protocols. The plan ensures services can continue during unexpected disruptions.	Provide a brief summary and the implement review interval.
Yes	Accredible’s information security program is formally approved and sponsored by senior management. Executive oversight ensures alignment with business objectives and resource allocation for ongoing improvements.	Summarize your internal audit processes and procedures.

Yes	Accredible has a designated security lead responsible for coordinating security policies, risk management, compliance, and incident response. This role ensures security is integrated across engineering, product, and operations.	Provide a copy of your physical security controls and policies along with this document (link or attached).
Yes	Accredible supports SAML 2.0 and OAuth/OIDC for SSO, enabling secure and seamless authentication for both administrators and end users.	Describe how strong authentication is enforced (e.g., complex passwords, multifactor tokens, certificates, biometrics, aging requirements, re-use policy).
Yes	Local authentication is supported with username/password login for customers not implementing SSO.	Provide a detailed description of your local authentication mode practices.
Yes	Password policies can be configured to align with institutional requirements, including minimum length, character mix, and expiration.	Describe how password/passphrase complexity requirements are implemented in the product.
Yes	Passwords must meet minimum complexity requirements. Accredible enforces strong password standards by default.	Describe these limitations and/or restrictions and state what lengths and complexities are supported.

Yes	Accredible provides automated password reset capabilities and documented support processes to ensure secure recovery.	Describe your documented password/passphrase reset procedures that are currently implemented in the system and/or customer support.
Yes	Accredible supports integration with InCommon and other eduGAIN federations for academic institutions.	List the entity IDs registered in the Additional Information column.
No		
No		
Yes		
Yes		
Yes		
Yes	Accredible supports directory and identity system integrations via SAML, OIDC, and SCIM.	List which systems and versions supported (such as Active Directory, Kerberos, or other LDAP compatible directory) in Additional Info.
Yes		
Yes	Directory integration with LDAP/AD and similar services is supported through SAML/OIDC.	Describe all authentication services supported by the system.

Yes	Accredible supports SAML 2.0, OAuth/OIDC, and other federation protocols for secure SSO.	State the web SSO standards supported by your solution and provide additional details about your support, including framework(s) in use, how information is exchanged securely, etc.
Yes		
Yes	MFA is supported using TOTP-based authenticators and institutional SSO integrations with MFA enforcement.	List all supported multifactor authentication methods, technologies, and/or solutions and provide a brief summary of each.
Yes	Session timeouts and inactivity auto-logout are enforced according to best practices.	Describe the default behavior of this capability.
No		
Yes	All transport of sensitive data uses TLS 1.2+ encryption between clients and systems, and system-to-system integrations.	Summarize your transport encryption strategy.
Yes	All data at rest is encrypted with AES-256 encryption, including files, disks, and databases.	Summarize your data encryption strategy and state what encryption options are available.
Yes	Accredible uses FIPS 140-2/3 validated modules through AWS KMS and TLS libraries.	Provide reference to FIPS 140-3 validation certificates.

Yes	Accredible provides customers with a defined period of access to export their data at the end of a contract.	State the length of time that the institution's data will be available in the system at the completion of the contract.
Yes	Accredible contracts guarantee customer ownership rights in the event of acquisition or bankruptcy.	Provide references, as needed.
No		
Yes	Data is stored in redundant, environmentally controlled AWS facilities with strong physical security.	Provide a general summary of your archival environment.
Yes	Accredible securely returns data to customers and deletes all data from systems and backups in compliance with NIST 800-88.	State the length of time that the institution's data will be available in the system at the completion of the contract.
Yes	Customers can export full or partial datasets through APIs and administrative tools.	Provide a general summary of how full and partial backups of data can be extracted.
Yes	Backups include the application and data layers needed to restore service.	Decribe your overall strategy to accomplish these elements.
Yes	Accredible replicates backups across AWS availability zones and regions.	Summarize your off-site backup strategy.

No	Accredible does not transport physical media. Backups are cloud-native only.	State any plans to implement off-site physical backups in your environment.
Yes	All backups are encrypted in transit and at rest using AES-256.	Summarize the encryption algorithm/strategy you are using to secure backups.
Yes	Accredible maintains a documented process for data lifecycle management, including secure wiping, repurposing, and destruction of data media.	Provide documented details of this process (link or attached).
Yes		
Limited and controlled		
Yes	Accredible enforces security for remote employees through VPN, MFA, device encryption, endpoint protection, and MDM.	Provide a detailed summary outlining the security controls implemented to protect the institution's data.
Logical separation		
Yes	Customers retain full ownership of their data at all times. Accredible does not claim rights over inputs, outputs, or metadata.	Provide reference to your data ownership documention.

Yes	Accredible provides customers at least 90 days to retrieve and migrate data in the event of closure or bankruptcy.	State how the institution will be notified of imminent termination.
Yes	Immutable backups are created per schedule, encrypted, and stored securely with restricted access.	If your strategy uses different processes for services and data, ensure that all strategies are clearly stated and supported.
Yes		
Yes	Accredible enforces role-based access control (RBAC) with least-privilege principles.	Describe available roles.
Yes	Accredible employs WAF protection through AWS services to mitigate web-based threats.	Describe the currently implemented WAF.
Yes	Accredible uses supported OS, libraries, and frameworks, with dependency scanning to detect unsupported components.	Please provide a list of all required dependencies.
No	Accredible does not require or collect location/GPS data.	Please indicate any future plans that would require access to this data

Yes	Administrative, security, and user functions are segregated by role and access policies.	Describe or provide a reference to the facilities available in the system to provide separation of duties between security administration and system administration functions.
Yes	Accredible applies static application security testing (SAST) as part of its CI/CD pipeline.	Provide a list of all tools utilized during static code analysis or static application security testing.
Yes	Automated and manual testing, including DAST and penetration testing, are applied pre-release.	Describe testing processes, including but not limited to, development of test plans, personnel involved in the testing process, and authorized individual accountable for approval and certification of test results.
Yes		
Yes	Accredible enforces input validation, sanitization, and safe error messages.	Describe how your system(s) provide data input validation and error messages.
Yes	Dependency management, SBOM tracking, and vulnerability scanning are applied to third-party libraries.	Provide supporting documentation of your processes.
Yes	All developers undergo secure coding training during onboarding and annually.	Summarize your secure coding training.

Yes	OWASP and secure coding practices are applied throughout the SDLC.	Summarize your secure coding practices.
Yes	Accredible’s mobile-accessible features are distributed via trusted app stores.	State the application title as listed within the trusted source.
Yes	Administrative access to customer instances follows documented approval, least-privilege, and logging procedures.	Describe or provide a reference that details how administrator access is handled (e.g., provisioning, principle of least privilege, deprovisioning, etc.).
AWS		
Yes		Based on the response to DCTR-01, this question does not apply to this product or service.
Yes		
Yes		Based on the response to DCTR-01, this question does not apply to this product or service.
Yes		Based on the response to DCTR-01, this question does not apply to this product or service.
Yes		Based on the response to DCTR-01, this question does not apply to this product or service.

Yes	Redundant hosting across AWS availability zones and regions.	State your primary and secondary data center locations. For cloud infrastructures, state the primary and secondary zones.
Yes	Redundancy and failover ensure high availability.	Provide a summary to support your response selection.
Yes		Based on the response to DCTR-01, this question does not apply to this product or service.
Yes		Based on the response to DCTR-01, this question does not apply to this product or service.
Yes		Based on the response to DCTR-01, this question does not apply to this product or service.
Yes		Based on the response to DCTR-01, this question does not apply to this product or service.
Yes		Based on the response to DCTR-01, this question does not apply to this product or service.
Yes	MFA is enforced for all privileged accounts.	State which model of MFA you are using.
Yes		
No		

Yes	Stateful firewalls are deployed for all network layers.	Describe the currently implemented SPI firewall.
Yes	Firewall change requests require documented approval.	Describe your documented firewall change request policy.
Yes	Network-based IDS is deployed.	Describe the currently implemented IDS.
Yes	Host-based IDS agents monitor servers.	Describe the currently implemented host-based IDS solution(s).
Yes	All changes are logged and monitored.	Describe your current network systems logging strategy.
Yes	Security/operations managers approve firewall changes.	List approver names or titles.
Yes	Network-based IPS is active.	Describe the currently implemented IPS.
Yes	Host-level protections are deployed.	Describe the currently implemented host-based IPS solution(s).
Yes	Advanced monitoring tools are deployed for APT detection.	Describe your NGPT monitoring strategy.
Both	Internal monitoring is supplemented with third-party services.	In addition to stating your intrusion monitoring strategy, provide a brief summary of its implementation.
Yes	Continuous monitoring is in place through SIEM and SOC coverage.	Provide a brief summary of this activity.
Yes	Accredible maintains a documented IRP with defined roles, processes, and escalation paths.	Summarize or provide a link to your formal incident response plan.

Yes	Accredible uses an internal incident response team and external experts as needed.	Summarize your incident response and reporting processes.
Yes	Incident response coverage is continuous, leveraging monitoring and on-call teams.	Summarize your internal approach or reference your third-party contractor.
Yes	Accredible maintains cyber liability insurance for coverage against outages, breaches, and incidents.	Describe the coverage in place for this solution.
Yes	Vulnerability scans with authenticated accounts are performed in staging prior to release.	Provide a brief description.
Yes	Accredible provides scan results upon request under NDA.	Provide a reference to security scan documentation.
Yes	Customers may perform scans subject to scheduling agreements.	Provide reference to the process or procedure to set up security testing times and scopes.
Yes	Accredible undergoes annual third-party penetration testing and SOC 2 audits.	Provide the results with this document (link or attached), if possible. State the date of the last completed third-party security assessment.
Yes		
Yes	External vulnerability scans are conducted regularly by independent tools and third parties.	Decribe your external application vulnerability scanning strategy.

Accredible Accessibility Team		
Accessibility & Compliance Lead		
accessibility@accredible.com		
	Accredible publishes its accessibility statement and VPAT on its Trust Center website. https://www.accredible.com/trust-center	VPAT can also be added as an attachment
Yes	Accredible maintains an updated VPAT/ACR, reviewed annually to ensure compliance with WCAG 2.1 AA.	State the date the VPAT was completed. Include this VPAT in your submission and/or link to its web location.
Yes		
Yes		
Yes	Accredible maintains a formal accessibility issue reporting and tracking workflow, integrated into its support and product management systems.	Describe the process and any recent examples of fixes as a result of the process.
Yes	Documentation describing accessibility features is available to customers and evaluators.	Provide examples with links where possible.
Yes	Accredible engages third-party experts for periodic audits of accessibility compliance.	State when the audit was conducted and by whom. Include the results in your submission and/or link to its web location.

Yes	Accredible validates accessibility as part of QA cycles and with external reviews, documented in the SDLC.	Describe your processes and methodologies for validating accessibility conformance.
Yes	Accredible aligns with WCAG 2.1 AA as the technical accessibility conformance standard.	Indicate which primary standards and all additional standards the solution meets.
Yes	Accredible maintains an accessibility roadmap, including upcoming improvements, available under NDA.	Comment on how far into the future the roadmap extends. Provide evidence (including links) of having delivered upon the accessibility roadmap in the past.
Yes	Staff undergo training and continuing education in accessibility standards and practices.	Provide any further relevant information about how expertise is maintained; include any accessibility certifications staff may hold (e.g., IAAP WAS <https://www.accessibilityassociation.org/certifications> or DHS Trusted Tester <https://section508.gov/test/trusted-tester>).
Yes	Accessibility testing and review are integrated into design, development, and release processes.	Provide further details in Additional Information.

Yes	Accredible ensures full keyboard navigation support, including issuing, managing, and consuming credentials.	State when and on which platform this was verified.
No		
No		
Yes (where applicable)		
Yes		
Yes		
Yes		
No		
No		
No		
No	Data remains within the Accredible platform. Consultants do not extract or store institutional data outside of the environment.	No need to answer CONS-07
No	Remote access to institutional networks or systems is not required. All services are delivered through Accredible's secure, hosted SaaS environment.	No need to answer CONS-09
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.

		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.

		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.

		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.

		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.

		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-05 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.

		Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.

		Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-06 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-07 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-07 on the "START HERE" tab, this question does not apply to this product or service.

		Based on the response to REQU-07 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-07 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-07 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-07 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-07 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-07 on the "START HERE" tab, this question does not apply to this product or service.

		Based on the response to REQU-07 on the "START HERE" tab, this question does not apply to this product or service.
		Based on the response to REQU-07 on the "START HERE" tab, this question does not apply to this product or service.
Yes		
Yes		
Yes		
Yes		
Yes		
Skills tagging and analytics	Accredible uses generative AI and ML to analyze credential/course descriptions and provide skills tagging, fraud detection, and usage insights. Customer data is not used for training AI models.	Looking for the capabilities, use-case, goals, and benefits of the AI model or feature(s).
Yes		
Yes		
Yes		
Yes		

Yes		
Yes		
Yes		
No		
Yes		
Validation and sanitization	Accredible applies input validation, sanitization, and schema enforcement to ensure only appropriate and safe data is processed by AI features.	Looking for how the solution is checked for input anomalies, patterns, and malicious input rejection.
Yes		
Yes		
Yes		
Yes		
Yes		
Yes		
Yes		
Yes		
No (not applicable)	Accredible does not watermark training data, as only non-customer metadata is used. Instead, provenance controls and dataset validation processes ensure integrity.	Looking for watermarking of training data to aid in your incident response.
Yes		

Yes		
Yes		
Yes		
Yes		
Yes		

n.
 the score.

e customer, you are an issuer of digital credentials and access a Dashboard web p

Score %	Jump To
83%	Jump to Company Information
100%	Jump to Documentation
100%	Jump to Assessment of Third Parties

97%	Jump to Change Management
100%	Jump to Policies, Processes, and Procedures
92%	Jump to Authentication, Authorization, and Account
91%	Jump to Data
100%	Jump to Application/Service Security
100%	Jump to Datacenter
100%	Jump to Firewalls, IDS, IPS, and Networking
100%	Jump to Incident Handling
100%	Jump to Vulnerability Management
85%	Jump to Consulting Services

N/A	Jump to HIPAA Compliance
N/A	Jump to Payment Card Industry Data Security Stan
N/A	Jump to On-Premises Data Solutions
100%	Jump to IT Accessibility
99%	Jump to AI Questions
88%	Jump to Privacy Scorecard
95%	

n.
 the score.

Analyst Notes	**Analysts: Use columns G and I to override the**

(Will reflect across applicable tabs)	**Compliant Response**	**Compliant Override**
Back to Scorecard		
	Not scored	
	Not scored	
	Not scored	
	Not scored	
	Not scored	
	Not scored	
	Not scored	
	Not scored	
	Not scored	
Back to Scorecard	**Compliant Response**	**Compliant Override**

	Yes	
	Not scored	
	Yes	
	Yes	

	Not scored	
Back to Scorecard	**Compliant Response**	**Compliant Override**
	Not scored	

	Not scored	
	Not scored	
	Not scored	
	Not scored	

	Not scored	
	Not scored	
	Not scored	

Back to Scorecard	Compliant Response	Compliant Override
	Yes	
	Yes	

	Yes	
	Yes	
	Yes	

	Yes	
	Yes	

Back to Scorecard	Compliant Response	Compliant Override
	Yes	

	Yes	
	Yes	
	Yes	
	Yes	
Back to Scorecard	**Compliant Response**	**Compliant Override**

	Yes	
	Yes	
	Yes	

	Yes	
	Yes	
	Yes	

	Yes	
	Yes	
	Yes	

	Yes	
	Yes	
	Yes	
	Yes	
	Yes	

	Yes	
	Yes	

Back to Scorecard	**Compliant Response**	**Compliant Override**
	Yes	
	Yes	
	Yes	
	Yes	

	Yes	
	Yes	
	Yes	
	Yes	

	Yes	
	Yes	
	Yes	

	Yes	
	Yes	
	Yes	

	Yes	

Back to Scorecard	Compliant Response	Compliant Override
	Yes	
	Yes	
	Yes	
	No	

	Yes	
	Yes	
	No	
	No	
	Yes	
	Not scored	
	Yes	
	Yes	
	Yes	
	Yes	

	Yes	
	Yes	
	Yes	
	Yes	

Back to Scorecard	Compliant Response	Compliant Override
	No	
	Yes	
	Yes	
	Yes	

	Yes	
	Yes	
	No	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	

	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	

	Yes	
	Yes	
	Yes	

Back to Scorecard	**Compliant Response**	**Compliant Override**
	Yes	
	Yes	
	Yes	
	No	

	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	

	Yes	
	Yes	
	Yes	

Back to Scorecard	**Compliant Response**	**Compliant Override**
	Not scored	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	

	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	No	
Back to Scorecard	**Compliant Response**	**Compliant Override**

	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Not scored	
	Yes	

Back to Scorecard	**Compliant Response**	**Compliant Override**
	Yes	

	Yes	
	Yes	
	Yes	
Back to Scorecard	**Compliant Response**	**Compliant Override**
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
Back to Scorecard	**Compliant Response**	**Compliant Override**

	Not scored	
	Not scored	
	Not scored	
	Not scored	
	Not scored	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	

	Yes	
	Yes	
	Yes	
	Yes	
	Yes	

	Yes	
	No	

Back to Scorecard	Compliant Response	Compliant Override
	No	
	Yes	
	Yes	
	Yes	
	Yes	
	No	
	No	
	No	
	No	
	No	

Back to Scorecard	Compliant Response	Compliant Override
	Yes	

	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	

	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	

	No	
	Yes	
	Yes	
	Yes	
	No	
	Yes	

	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	

	Yes	
	Yes	
	Yes	
	Yes	
Back to Scorecard	**Compliant Response**	**Compliant Override**
	Yes	
	No	

	No	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	

	Not scored	
	Yes	
	Yes	
	Not scored	

Back to Scorecard	Compliant Response	Compliant Override
	Yes	
	No	

	Yes	
	No	
	Yes	
	Yes	
	Yes	
	Not scored	

	Not scored	
	Yes	

Back to Scorecard	Compliant Response	Compliant Override
	Not scored	
	Not scored	

Back to Scorecard	Compliant Response	Compliant Override
	Yes	
	Yes	
	Yes	
	Not scored	
	Yes	

Back to Scorecard	Compliant Response	Compliant Override
	Yes	
	Yes	
	Yes	

	Yes	
	Yes	

Back to Scorecard	Compliant Response	Compliant Override
	Yes	
	No	
	Yes	
	Not scored	
	Yes	

Back to Scorecard	Compliant Response	Compliant Override
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	

Back to Scorecard	Compliant Response	Compliant Override
	Yes	

	Yes	
	Yes	
	Yes	
	Yes	
	Yes	

Version 4.1.0

roperty via amodern web browser to design, create, deliver and administrate cer

: Management

dard (PCI DSS)

response compliance and importance level.

Default Importance	Importance Override
Default Importance	Importance Override

Critical Importance	
Minor Importance	
Minor Importance	
Minor Importance	

Minor Importance	

Default Importance	Importance Override

Default Importance	**Importance Override**
Critical Importance	
Critical Importance	

Standard Importance	
Standard Importance	
Standard Importance	

Standard Importance	
Standard Importance	
Default Importance	**Importance Override**
Critical Importance	

Critical Importance	
Critical Importance	
Critical Importance	
Standard Importance	
Default Importance	**Importance Override**

Critical Importance	
Critical Importance	
Critical Importance	

Standard Importance	
Standard Importance	
Standard Importance	

Standard Importance	
Standard Importance	
Minor Importance	

Minor Importance	
Minor Importance	
Minor Importance	
Minor Importance	
Minor Importance	

Minor Importance	
Minor Importance	

Default Importance	Importance Override
Critical Importance	
Critical Importance	
Critical Importance	
Standard Importance	

Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	

Minor Importance	
Minor Importance	
Minor Importance	

Minor Importance	
Minor Importance	
Minor Importance	

Minor Importance	
Default Importance	**Importance Override**
Critical Importance	
Critical Importance	
Critical Importance	
Critical Importance	

Critical Importance	
Critical Importance	
Critical Importance	
Critical Importance	
Critical Importance	
Critical Importance	
Critical Importance	
Standard Importance	
Standard Importance	
Standard Importance	

Minor Importance	
Minor Importance	
Minor Importance	
Minor Importance	

Default Importance	Importance Override
Critical Importance	
Critical Importance	
Critical Importance	
Critical Importance	

Critical Importance	
Critical Importance	
Critical Importance	
Critical Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	

Standard Importance	
Minor Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Minor Importance	
Minor Importance	

Minor Importance	
Minor Importance	
Minor Importance	

Default Importance	Importance Override
Critical Importance	
Critical Importance	
Critical Importance	
Critical Importance	

Critical Importance	
Critical Importance	
Critical Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	

Standard Importance	
Minor Importance	
Minor Importance	
Default Importance	**Importance Override**
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Critical Importance	

Standard Importance	
Standard Importance	
Standard Importance	
Critical Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Default Importance	**Importance Override**

Critical Importance	
Critical Importance	
Critical Importance	
Critical Importance	
Critical Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Minor Importance	
Default Importance	**Importance Override**
Standard Importance	

Minor Importance	
Minor Importance	
Minor Importance	
Default Importance	**Importance Override**
Critical Importance	
Critical Importance	
Critical Importance	
Standard Importance	
Standard Importance	
Minor Importance	
Default Importance	**Importance Override**

Standard Importance	
Critical Importance	
Critical Importance	
Critical Importance	
Critical Importance	
Standard Importance	
Standard Importance	

Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	

Standard Importance	
Standard Importance	
Default Importance	**Importance Override**
Critical Importance	
Critical Importance	
Critical Importance	
Critical Importance	
Critical Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Default Importance	**Importance Override**
Critical Importance	

Critical Importance	
Critical Importance	
Critical Importance	
Standard Importance	
Standard Importance	
Standard Importance	

Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	

Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	

Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	

Standard Importance	
Standard Importance	
Standard Importance	
Minor Importance	
Default Importance	**Importance Override**
Critical Importance	
Critical Importance	

Critical Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	

Minor Importance	
Minor Importance	
Minor Importance	
Minor Importance	

Default Importance	Importance Override
Standard Importance	
Standard Importance	

Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	

Minor Importance	
Minor Importance	
Default Importance	**Importance Override**
Default Importance	**Importance Override**
Critical Importance	
Critical Importance	
Critical Importance	
Standard Importance	
Standard Importance	
Default Importance	**Importance Override**
Critical Importance	
Critical Importance	
Critical Importance	

Critical Importance	
Minor Importance	
Default Importance	**Importance Override**
Critical Importance	
Critical Importance	
Critical Importance	
Standard Importance	
Standard Importance	
Default Importance	**Importance Override**
Critical Importance	
Critical Importance	
Standard Importance	
Standard Importance	
Minor Importance	
Minor Importance	
Minor Importance	
Minor Importance	
Default Importance	**Importance Override**
Critical Importance	

Critical Importance	
Critical Importance	
Critical Importance	
Standard Importance	
Standard Importance	

tificates and badges

HECVAT Institution Evaluation - High Ris

Instructions for High-Risk Scorecard

1. The scorecard below reflects those questions marked as "Critical I

2. Use these condensed, aggregated views to review those questions

3. Changes cannot be made in this sheet. Please make changes in th

4. For instructions on how to do a "HECVAT Lite" evaluation, please visit educ

Solution Provider Name	EdInvent Inc. d.b.a. Accredible.
Solution Provider Contact Name	Alan Heppenstall
Solution Provider Contact Title	CTO
Solution Provider Contact Email	alan@accredible.com
Solution Name	Accredible
Solution Description	Accredible is a cloud-hosted, shared-t
Date Prepared	*12/9/2025*

Report Sections	Question Count
Non-Negotiable	**0**
Critical Importance/Lite Score	**90**

Critical Importance Questions (Lite Review Questions)

Code	Question

1	#NAME?	
2	#NAME?	
3	#NAME?	
4	#NAME?	
5	#NAME?	
6	#NAME?	
7	#NAME?	
8	#NAME?	
9	#NAME?	
10	#NAME?	
11	#NAME?	
12	#NAME?	
13	#NAME?	
14	#NAME?	
15	#NAME?	
16	#NAME?	
17	#NAME?	
18	#NAME?	
19	#NAME?	
20	#NAME?	
21	#NAME?	
22	#NAME?	
23	#NAME?	
24	#NAME?	
25	#NAME?	
26	#NAME?	
27	#NAME?	
28	#NAME?	
29	#NAME?	
30	#NAME?	

31	#NAME?	
32	#NAME?	
33	#NAME?	
34	#NAME?	
35	#NAME?	
36	#NAME?	
37	#NAME?	
38	#NAME?	
39	#NAME?	
40	#NAME?	
41	#NAME?	
42	#NAME?	
43	#NAME?	
44	#NAME?	
45	#NAME?	
46	#NAME?	
47	#NAME?	
48	#NAME?	
49	#NAME?	
50	#NAME?	
51	#NAME?	
52	#NAME?	
53	#NAME?	
54	#NAME?	
55	#NAME?	
56	#NAME?	
57	#NAME?	
58	#NAME?	
59	#NAME?	
60	#NAME?	
61	#NAME?	
62	#NAME?	
63	#NAME?	
64	#NAME?	
65	#NAME?	
66	#NAME?	
67	#NAME?	
68	#NAME?	
69	#NAME?	
70	#NAME?	
71	#NAME?	
72	#NAME?	
73	#NAME?	
74	#NAME?	
75	#NAME?	

76	#NAME?	
77	#NAME?	
78	#NAME?	
79	#NAME?	
80	#NAME?	
81	#NAME?	
82	#NAME?	
83	#NAME?	
84	#NAME?	
85	#NAME?	
86	#NAME?	
87	#NAME?	
88	#NAME?	
89	#NAME?	
90	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	

	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	

	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	

	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	

	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	

	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	

sk

Importance" or those where the "Non-Negotiable" box was checked.
s that pose the highest risk.
ne appropriate "Evaluation" tab.
cause.edu/HECVAT.

enant Software as a Service solution. As the customer, you are an issuer of digital cred

Max Score	Score	Score %
0	0	N/A
1,620	1,580	98%

Answer	Additional Information	Analyst Notes

			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]

			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]
			[redacted]

[redacted]

[redacted]

[redacted]

Version 4.1.0

dentials and access a Dashboard web property via amodern web

Non-Negotiable Questions

Code	Question

1	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	

	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	

	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	

	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	

	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	

	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	

	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	

	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	
	#NAME?	

browser to design, create, deliver and administrate certificates

Answer	Additional Information

and badges

Analyst Notes

HECVAT Institution Evaluation - Privacy

Instructions for Analysts

1. Upon initial review, you can check the "Non-Negotiable" box by any question

2. When evaluating an answer, a default importance level has been set. You can

3. For questions that are qualitative or for which you disagree with the preferred

4. Each worksheet shows a report for that section. See the "Analyst Report" she

5. If you are evaluating a question that appears in an earlier section, the Import

For full instructions, please visit EDUCAUSE.edu/HECVAT

Solution Provider Name
Solution Provider Contact Name
Solution Provider Contact Title
Solution Provider Contact Email
Solution Name
Solution Description
Date Prepared

Report Sections
General Privacy
Privacy-Specific Company Details
Privacy-Specific Documentation
Privacy of Third Parties

Privacy Change Management
Privacy of Sensitive Data
Privacy Policies and Procedures
International Privacy
Data Privacy
Privacy and AI
Privacy Score

HECVAT Analyst Report - Privacy

Institution Assessment

Instructions for Analysts

1. Upon initial review, you can check the "Non-Negotiable" box by any question

2. When evaluating an answer, a default importance level has been set. You can

3. For questions that are qualitative or for which you disagree with the preferred

4. Each worksheet shows a report for that section. See the "Analyst Report" she

5. If you are evaluating a question that appears in an earlier section, the Import

For full instructions, please visit EDUCAUSE.edu/HECVAT

ID	Question
General Privacy	

PRGN-01	Does your solution process FERPA-related data?
PRGN-02	Does your solution process GDPR-related or PIPL-related data?
PRGN-03	Does your solution process personal data regulated by state law(s) (e.g., CCPA)?
PRGN-04	Does your solution process user-provided data that may contain regulated information?
PRGN-05	Web Link to Product/Service Privacy Notice

Privacy-Specific Company Details

PCOM-01	Have you had a personal data breach in the past three years that involved reporting to a governmental agency, notice to individuals (including voluntary notice), or notice to another organization or institution?*
PCOM-02	Use this area to share information about your privacy practices that will assist those who are assessing your company data privacy program.*
PCOM-03	Have you had any data privacy policy or law violations in the past 36 months?
PCOM-04	Do you have a dedicated data privacy staff or office?

Privacy-Specific Documentation

PDOC-01	If you have completed a SOC 2 audit, does it include the Privacy Trust Service Principle?
PDOC-02	Do you conform with a specific industry-standard privacy framework (e.g., NIST Privacy Framework, GDPR, ISO 27701)?
PDOC-03	Does your employee onboarding and offboarding policy include training of employees on information security and data privacy?

Privacy of Third Parties

PTHP-01	Do you have contractual agreements with third parties that require them to maintain standards and to comply with all regulatory requirements?*
PTHP-02	Do you perform privacy impact assesments of third parties that collect, process, or have access to personal data to ensure they meet industry and regulatory standards and to mitigate harmful, unethical, or discriminatory impacts on data subjects?

Privacy Change Management

PCHG-01	Does your change management process include privacy review and approval?
PCHG-02	Do you have policy and procedure, currently implemented, guiding how privacy risks are mitigated until they can be resolved?

Privacy of Sensitive Data

PDAT-01	Do you collect, process, or store demographic information?*
PDAT-02	Do you capture or create genetic, biometric, or behaviometric information (e.g., facial recognition or fingerprints)?*
PDAT-03	Do you combine institutional data (including "de-identified," "anonymized," or otherwise masked data) with personal data from any other sources?*
PDAT-04	Is institutional data coming into or going out of the United States at any point during collection, processing, storage, or archiving?
PDAT-05	Do you capture device information (e.g., IP address, MAC address)?
PDAT-06	Does any part of this service/project involve a web/app tracking component (e.g., use of web-tracking pixels, cookies)?
PDAT-07	Does your staff (or a third party) have access to institutional data (e.g., financial, PHI, or other sensitive information) through any means?

PDAT-08	Will you handle personal data in a manner compliant with all relevant laws, regulations, and applicable institution policies?

Privacy Policies and Procedures

PRPO-01	Do you have a documented privacy management process?
PRPO-02	Are privacy principles designed into the product lifecycle (i.e., privacy-by-design)?
PRPO-03	Will you comply with applicable breach notification laws?
PRPO-04	Will you comply with the institution's policies regarding user privacy and data protection?
PRPO-05	Is your company subject to the laws and regulations of the institution's geographic region?
PRPO-06	Do you have a privacy awareness/training program?*
PRPO-07	Is privacy awareness training mandatory for all employees?
PRPO-08	Is AI privacy and ethics awareness/training required for all employees who work with AI?
PRPO-09	Do you have any decision-making processes that are completely automated (i.e., there is no human involvement)?
PRPO-10	Do you have a documented process for managing automated processing, including validations, monitoring, and data subject requests?
PRPO-11	Do you have a documented policy for sharing information with law enforcement?
PRPO-12	Do you share any institutional data with law enforcement without a valid warrant?*

PRPO-13	Does your incident response team include a privacy analyst/officer?

International Privacy

INTL-01	Will data be collected from or processed in or stored in the European Economic Area (EEA)?
INTL-02	Do you have a data protection officer (DPO)?
INTL-03	Will you sign appropriate GDPR Standard Contractual Clauses (SCCs) with the institution?
INTL-04	Will data be collected from or processed in or stored in China?
INTL-05	Do you comply with PIPL security, privacy, and data localization requirements?

Data Privacy

DRPV-01	Have you performed a Data Privacy Impact Assesssment for the solution/project?
DRPV-02	Do you provide an end-user privacy notice about privacy policies and procedures that identify the purpose(s) for which personal information is collected, used, retained, and disclosed?
DRPV-03	Do you describe the choices available to the individual and obtain implicit or explicit consent with respect to the collection, use, and disclosure of personal information?
DRPV-04	Do you collect personal information only for the purpose(s) identified in the agreement with an institution or, if there is none, the purpose(s) identified in the privacy notice?
DRPV-05	Do you have a documented list of personal data your service maintains?

DRPV-06	Do you retain personal information for only as long as necessary to fulfill the stated purpose(s) or as required by law or regulation and thereafter appropriately dispose of such information?
DRPV-07	Do you provide individuals with access to their personal information for review and update (i.e., data subject rights)?
DRPV-08	Do you disclose personal information to third parties only for the purpose(s) identified in the privacy notice or with the implicit or explicit consent of the individual?
DRPV-09	Do you protect personal information against unauthorized access (both physical and logical)?
DRPV-10	Do you maintain accurate, complete, and relevant personal information for the purposes identified in the privacy notice?
DRPV-11	Do you have procedures to address privacy-related noncompliance complaints and disputes?
DRPV-12	Do you "anonymize," "de-identify," or otherwise mask personal data?
DRPV-13	Do you or your subprocessors use or disclose "anonymized," "de-identified," or otherwise masked data for any purpose other than those identified in the agreement with an institution (e.g., sharing with ad networks or data brokers, marketing, creation of profiles, analytics unrelated to services provided to institution)?
DRPV-14	Do you certify stop-processing requests, including any data that is processed by a third party on your behalf?
DRPV-15	Do you have a process to review code for ethical considerations?

Privacy and AI

DPAI-01	Does your service use AI for the processing of institutional data?
DPAI-02	Is any institutional data retained in AI processing?*
DPAI-03	Do you have agreements in place with third parties or subprocessors regarding the protection of customer data and use of AI?*
DPAI-04	Will institutional data be processed through a third party or subprocessor that also uses AI?
DPAI-05	Is AI processing limited to fully licensed commercial enterprise AI services?
DPAI-06	Will institutional data be used or processed by any shared AI services?
DPAI-07	Do you have safeguards in place to protect institutional data and data privacy from unintended AI queries or processing?
DPAI-08	Do you provide choice to the user to opt out of AI use?

PRIVACY REFERENCE QUESTIONS *-these fields cannot be ed*

ID	Question
Company Information	
COMP-01	Do you have a dedicated software and system development team(s) (e.g., customer support
COMP-02	Describe your organization's business background and ownership structure, including all parent and subsidiary
COMP-03	Have you operated without unplanned disruptions to this solution in the past 12 months?
COMP-04	Do you have a dedicated information security staff or office?
Required Questions	
REQU-04	Does your solution have AI features, or are there plans to implement AI features in the next 12 months?
REQU-05	Does your solution process protected health information (PHI) or any data covered by the Health Insurance
REQU-06	Is the solution designed to process, store, or transmit credit card information?
REQU-08	Does your solution have access to personal or institutional data?
Documentation	
DOCU-01	Do you have a well-documented business continuity plan (BCP), with a clear owner, that is tested annually?*

DOCU-03	Have you undergone a SSAE 18/SOC 2 audit?
DOCU-04	Do you conform with a specific industry standard security framework (e.g., NIST Cybersecurity
DOCU-05	Can you provide overall system and/or application architecture diagrams, including a full description of the
DOCU-06	Does your organization have a data privacy policy?
DOCU-07	Do you have a documented, and currently implemented, employee onboarding and offboarding policy?

IT Accessibility

ITAC-05	Web Link to Accessibility Statement or VPAT
ITAC-07	Will your company agree to meet your stated accessibility standard or WCAG 2.1 AA as part of your

Assessment of Third Parties

THRD-01	Do you perform security assessments of third-party companies with which you share data (e.g., hosting
THRD-02	Do you have contractual language in place with third parties governing access to institutional data?*
THRD-03	Do the contracts in place with these third parties address liability in the event of a data breach?*
THRD-04	Do you have an implemented third-party management strategy?*

Consulting Services

CONS-01	Will the consultant require access to the institution's network resources?*
CONS-02	Has the consultant received training on (sensitive, HIPAA, PCI, etc.) data handling?*
CONS-03	Is the data encrypted (at rest) while in the consultant's possession?*
CONS-04	Can access be restricted based on source IP address?*
CONS-05	Will the consulting take place on-premises?
CONS-06	Will the consultant require access to hardware in the institution's data centers?
CONS-07	Will the consultant require an account within the institution's domain (@*.edu)?
CONS-08	Will any data be transferred to the consultant's possession?
CONS-09	Will the consultant need remote access to the institution's network or systems?

Application/Service Security

APPL-01	Are access controls for institutional accounts based on structured rules, such as role-based access control
APPL-02	Are you using a web application firewall (WAF)?*
APPL-08	Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or

Authentication, Authorization, and Account Management

AAAI-01	Does your solution support single sign-on (SSO) protocols for user and administrator authentication?*
AAAI-02	For customers not using SSO, does your solution support local authentication protocols for user and administrator
AAAI-12	For customers not using SSO, does your application support integration with other authentication and
AAAI-13	Do you allow the customer to specify attribute mappings for any needed information beyond a user identifier?
AAAI-17	For customers not using SSO, does your application and/or user frontend/portal support multifactor

Change Management

CHNG-01	Will the institution be notified of major changes to your environment that could impact the institution's security
CHNG-02	Does the system support client customizations from one release to another?*

Data

DATA-03	Is the storage of sensitive data encrypted using security protocols/algorithms (e.g., disk encryption, at-rest, files
DATA-04	Do all cryptographic modules in use in your solution conform to the Federal Information Processing
DATA-06	Are these rights retained even through a provider acquisition or bankruptcy event?*
DATA-07	Do backups containing the institution's data ever leave the institution's data zone either physically or via
DATA-08	Is media used for long-term retention of business data and archival purposes stored in a secure
DATA-09	At the completion of this contract, will data be returned to the institution and/or deleted from all your systems
DATA-10	Can the institution extract a full or partial backup of data?
DATA-11	Do current backups include all operating system software, utilities, security software, application

DATA-12	Are you performing off-site backups (i.e., digitally moved off site)?
DATA-13	Are physical backups taken off-site (i.e., physically moved off site)?
DATA-14	Are data backups encrypted?
DATA-15	Do you have a media handling process that is documented and currently implemented that meets
DATA-17	Does your staff (or third party) have access to institutional data (e.g., financial, PHI, or other sensitive
DATA-22	Are involatile backup copies made according to predefined schedules and securely stored and
DATA-23	Do you have a cryptographic key management process (generation, exchange, storage, safeguards, use,
Datacenter	
DCTR-01	Select your hosting option.
DCTR-03	Are you generally able to accommodate storing each institution's data within its geographic region?
Firewalls, IDS, IPS, and Networking	
FIDP-01	Are you utilizing a stateful packet inspection (SPI) firewall?*
FIDP-02	Do you have a documented policy for firewall change requests?*
FIDP-03	Have you implemented an intrusion detection system (network-based)?*
FIDP-04	Do you employ host-based intrusion detection?*
FIDP-05	Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?*
FIDP-09	Are you employing any next-generation persistent threat (NGPT) monitoring?
Policies, Processes, and Procedures	
PPPR-03	Is your company subject to the institution's geographic region's laws and regulations?*
PPPR-04	Can you accommodate encryption requirements using open standards?
PPPR-10	Will you comply with applicable breach notification laws?
PPPR-11	Do you have an information security awareness program?
PPPR-12	Is security awareness training mandatory for all employees?
PPPR-14	Do you have documented, and currently implemented, internal audit processes and procedures?
PPPR-15	Does your organization have physical security controls and policies in place?
Incident Handling	
HFIH-01	Do you have a formal incident response plan?
HFIH-02	Do you either have an internal incident response team or retain an external team?
HFIH-03	Do you have the capability to respond to incidents on a 24 x 7 x 365 basis?
HFIH-04	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen,
Vulnerability Management	
VULN-01	Are your systems and applications scanned with an authenticated user account for vulnerabilities (that are
VULN-02	Will you provide results of application and system vulnerability scans to the institution?*
VULN-04	Have your systems and applications had a third-party security assessment completed in the last year?
VULN-06	Are your systems and applications regularly scanned externally for vulnerabilities?
HIPAA Compliance	
HIPA-01	Do your workforce members receive regular training related to the Health Insurance Portability and
HIPA-02	Have you identified areas of risk?*
HIPA-03	Have the relevant policies/plans been tested?*
HIPA-04	Have you entered into a Business Associate Agreements with all subcontractors who may have access to
HIPA-05	Do you monitor or receive information regarding changes in HIPAA regulations?
HIPA-06	Has your organization designated HIPAA Privacy and Security officers as required by the rules?
HIPA-07	Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health
HIPA-08	Have you conducted a risk analysis as required under the HIPAA Security Rule?
HIPA-09	Have you taken actions to mitigate the identified risks?

HIPA-10	Does your application require user and system administrator password changes at a frequency no
HIPA-11	Does your application require users to set their own password after an administrator reset or on first use of
HIPA-12	Does your application lock out an account after a number of failed login attempts?
HIPA-13	Does your application automatically lock or log-out an account after a period of inactivity?
HIPA-14	Are passwords visible in plain text, whether when stored or entered, including service-level accounts (i.e.
HIPA-15	If the application is institution-hosted, can all service-level and administrative account passwords be changed
HIPA-16	Does your application provide the ability to define user access levels?
HIPA-17	Does your application support varying levels of access to administrative tasks defined individually per user?
HIPA-18	Does your application support varying levels of access to records based on user ID?
HIPA-19	Is there a limit to the number of groups to which a user can be assigned?
HIPA-20	Do accounts used for solution provider-supplied remote support abide by the same authentication policies and
HIPA-21	Does the application log record access including specific user, date/time of access, and originating IP or device?
HIPA-22	Does the application log administrative activity, such as user account access changes and password changes
HIPA-23	Do you retain logs for at least as long as required by HIPAA regulations?
HIPA-24	Can the application logs be archived?
HIPA-25	Can the application logs be saved externally?
HIPA-26	Do you have a disaster recovery plan and emergency mode operation plan?
HIPA-27	Can you provide a HIPAA compliance attestation document?
HIPA-28	Are you willing to enter into a Business Associate Agreement (BAA)?
HIPA-29	Do your data backup and retention policies and practices meet HIPAA requirements?
Payment Card Industry Data Security Standard (PCI DSS)	
PCID-01	Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on
PCID-02	Is the application listed as an approved Payment Application Data Security Standard (PA-DSS)
PCID-03	Does the system or solutions use a third party to collect, store, process, or transmit cardholder
PCID-04	Do your systems or solutions store, process, or transmit cardholder (payment/credit/debt card) data?
PCID-05	Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?
PCID-06	Are you classified as a service provider?
PCID-07	Are you on the list of Visa approved service providers?
PCID-08	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?
PCID-09	Describe the architecture employed by the system to verify and authorize credit card transactions.
PCID-10	What payment processors/gateways does the system support?
PCID-11	Can the application be installed in a PCI DSS–compliant manner?
PCID-12	Include documentation describing the system's abilities to comply with the PCI DSS and any features or

to compile a report of questions that may prohibit a full review.
use the "Importance Override" dropdown to override the default and adjust th
l response, make a selection in the "Compliant Override" dropdown to adjust th
et for a full report of all sections.
ance and Compliant Override cannot be changed but additional notes can be ad

EdInvent Inc. d.b.a. Accredible.
Alan Heppenstall
CTO
alan@accredible.com
Accredible
Accredible is a cloud-hosted, shared-tenant Software as a Service solution modern web browser to desigr
12/9/2025

Include in Score?	Max Score	Score
TRUE	0	0
TRUE	30	25
TRUE	30	20
TRUE	25	25

TRUE	15	15
TRUE	85	65
TRUE	100	100
TRUE	50	30
TRUE	150	150
TRUE	80	65
	565	**495**

to compile a report of questions that may prohibit a full review.
use the "Importance Override" dropdown to override the default and adjust th
l response, make a selection in the "Compliant Override" dropdown to adjust th
:et for a full report of all sections.
ance and Compliant Override cannot be changed but additional notes can be ad

Vendor Answer	**Additional Information**	**Guidance**

Yes		
Yes		
Yes		
Yes (limited)		
No		
Yes		
No		
No (dedicated role, not separate office)	Accredible has a designated data privacy lead embedded in the	Describe your Data Privacy Office or plans, including size, talents,
No		
Yes	Accredible aligns its privacy program with GDPR, CCPA, NIST	Provide documentation on how your organization conforms to your chosen
Yes		

Yes		
Yes	Accredible conducts vendor due diligence and periodic reviews, including privacy and security assessments of third parties with access	Provide a summary of your practices that assures that the third party will be subject to the appropriate standards regarding data
Yes	Accredible's change management process includes privacy impact	Please describe your process for privacy review.
Yes		
No		
No		
No		
Yes (if applicable)		
Yes (minimal)		
Yes	Accredible uses essential cookies and limited analytics for service	Describe the tracking component and what is done with the
Limited and controlled		

Yes		
Yes	Accredible maintains a documented privacy management process	Describe privacy management process or provide links or attach
Yes	Privacy-by-Design principles are embedded into Accredible’s SDLC,	Summarize the privacy principles designed into the product lifecycle.
Yes	Accredible’s incident response plan includes compliance with GDPR,	State how quickly the institution will be notified.
Yes		
Yes		
Yes		
Yes	Privacy awareness training is required for all employees and tracked	Summarize your privacy awareness training content and state how
Yes		
No		
Yes	Accredible documents processes for monitoring automated functions,	Provide documentation describing management processes.
Yes		
No		

Yes		
Yes	Accredible provides hosting options in the EU/EEA and processes	Describe where and what activities will take place in the EEA.
Yes	Accredible has appointed a Data Protection Officer responsible for	Provide the name and contact information for the DPO.
Yes		
Yes (if applicable)		
Yes		
Yes		
Yes		
Yes		
Yes		
Yes		

Yes		
Yes		
Yes		
Yes		
Yes		
Yes		
Yes		
No		
Yes		
Yes		
[redacted]	[redacted]	[redacted]

Yes (limited)		
No		
Yes		
No		
Yes		
No		
Yes		
No		

ited and must be changed on the "Institution Evaluation" ta

Vendor Answer	Additional Information	Guidance
Yes	Accredible maintains	Describe the structure
Yes		
Yes		
No	Accredible does not	Describe any plans to
Yes	Accredible uses AI and	DO complete the Artificial
No	Accredible is not designed	DO NOT complete the
No	Accredible does not store,	DO NOT complete the
Yes	Accredible processes	DO complete the Privacy
Yes		

Yes	Accredible is SOC2 Type	Provide the date of
Yes	Accredible aligns its	Provide documentation
Yes	Diagrams are available	Provide your diagrams
Yes	https://www.accredible.c	Provide your data privacy
Yes	Accredible maintains	Provide a reference to
	Accredible publishes its	VPAT can also be added
Yes		
Yes	Accredible conducts risk	Provide a summary of
Yes	Accredible requires	List each third party and
Yes		
Yes	Accredible enforces the	Provide additional
No		
Yes (where applicable)		
Yes		
Yes		
No		
No		
No		
No	Data remains within the	No need to answer CONS-
No	Remote access to	No need to answer CONS-
Yes	Accredible enforces role-	Describe available roles.
Yes	Accredible employs WAF	Describe the currently
Yes		
Yes	Accredible supports SAML	Describe how strong
Yes	Local authentication is	Provide a detailed
Yes	Accredible supports	List which systems and
Yes		
Yes	MFA is supported using	List all supported
Yes	Accredible maintains a	State how and when the
Yes	Accredible preserves	Describe or provide
Yes	All data at rest is	Summarize your data
Yes	Accredible uses FIPS 140-	Provide reference to FIPS
Yes	Accredible contracts	Provide references, as
No		
Yes	Data is stored in	Provide a general
Yes	Accredible securely	State the length of time
Yes	Customers can export	Provide a general
Yes	Backups include the	Decribe your overall

Yes	Accredible replicates	Summarize your off-site
No	Accredible does not	State any plans to
Yes	All backups are encrypted	Summarize the
Yes	Accredible maintains a	Provide documented
Limited and controlled		
Yes	Immutable backups are	If your strategy uses
Yes		
AWS		
Yes		
Yes	Stateful firewalls are	Describe the currently
Yes	Firewall change requests	Describe your
Yes	Network-based IDS is	Describe the currently
Yes	Host-based IDS agents	Describe the currently
Yes	All changes are logged	Describe your current
Yes	Advanced monitoring	Describe your NGPT
Yes		
Yes		
Yes	Employees must	State how quickly the
Yes	Accredible maintains a	Summarize your
Yes	Accredible operates a	Summarize your security
Yes	Accredible's information	Summarize your internal
Yes	Accredible has a	Provide a copy of your
Yes	Accredible maintains a	Summarize or provide a
Yes	Accredible uses an	Summarize your incident
Yes	Incident response	Summarize your internal
Yes	Accredible maintains	Describe the coverage in
Yes	Vulnerability scans with	Provide a brief
Yes	Accredible provides scan	Provide a reference to
Yes	Accredible undergoes	Provide the results with
Yes	External vulnerability	Decribe your external
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to

		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to
		Based on the response to

e value of the question.

e question's impact on the score.

lded.

. As the customer, you are an issuer of digital credentials and access a Dashboard
, create, deliver and administrate certificates and badges

Score %	Jump To
N/A	Jump to General Privacy
83%	Jump to Privacy-Specific Company Details
67%	Jump to Privacy-Specific Documentation
100%	Jump to Privacy of Third Parties

100%	Jump to Privacy Change Management
76%	Jump to Privacy of Sensitive Data
100%	Jump to Privacy Policies and Procedures
60%	Jump to International Privacy
100%	Jump to Data Privacy
81%	Jump to Privacy and AI
88%	

e value of the question.
e question's impact on the score.

lded.

Analyst Notes	**Analysts: Use columns G and I to override the**	
(Will reflect across applicable tabs)	**Compliant Response**	**Compliant Override**
Back to Scorecard	**Compliant Response**	**Compliant Override**

	Not scored	
	Not scored	
	Not scored	
	Not scored	
	Not scored	
Back to Scorecard	**Compliant Response**	**Compliant Override**
	No	
	Not scored	
	No	
	Yes	
Back to Scorecard	**Compliant Response**	**Compliant Override**
	Yes	
	Yes	
	Yes	

Back to Scorecard	Compliant Response	Compliant Override
	Yes	
	Yes	

Back to Scorecard	Compliant Response	Compliant Override
	Yes	
	Yes	

Back to Scorecard	Compliant Response	Compliant Override
	No	
	No	
	No	
	No	
	No	
	No	
	No	

	Yes	

Back to Scorecard	Compliant Response	Compliant Override
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	No	
	Yes	
	Yes	
	No	

	Yes	

Back to Scorecard	Compliant Response	Compliant Override
	No	
	Yes	
	Yes	
	No	
	Yes	

Back to Scorecard	Compliant Response	Compliant Override
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	

	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	No	
	Yes	
	Yes	
Back to Scorecard	**Compliant Response**	**Compliant Override**

	No	
	No	
	Yes	
	No	
	Yes	
	No	
	Yes	
	Yes	

b.		
Analyst Notes	**Compliant Response**	**Compliant Override**
Back to Scorecard		
	Yes	
	Not scored	
	Yes	
	Yes	
Back to Scorecard	**Compliant Response**	**Compliant Override**
	Not scored	
	Not scored	
	Not scored	
	Not scored	
Back to Scorecard	**Compliant Response**	**Compliant Override**
	Yes	

	Yes	
	Yes	
	Yes	
	Yes	
	Yes	

Back to Scorecard	Compliant Response	Compliant Override
	Not scored	
	Yes	

Back to Scorecard	Compliant Response	Compliant Override
	Yes	
	Yes	
	Yes	
	Yes	

Back to Scorecard	Compliant Response	Compliant Override
	No	
	Yes	
	Yes	
	Yes	
	No	
	No	
	No	
	No	
	No	

Back to Scorecard	Compliant Response	Compliant Override
	Yes	
	Yes	
	Yes	

Back to Scorecard	Compliant Response	Compliant Override
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	

Back to Scorecard	Compliant Response	Compliant Override
	Yes	
	Yes	

Back to Scorecard	Compliant Response	Compliant Override
	Yes	
	Yes	
	Yes	
	No	
	Yes	
	Yes	
	Yes	
	Yes	

	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
Back to Scorecard	**Compliant Response**	**Compliant Override**
	Not scored	
	Yes	
Back to Scorecard	**Compliant Response**	**Compliant Override**
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
Back to Scorecard	**Compliant Response**	**Compliant Override**
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
Back to Scorecard	**Compliant Response**	**Compliant Override**
	Yes	
	Yes	
	Yes	
	Yes	
Back to Scorecard	**Compliant Response**	**Compliant Override**
	Yes	
	Yes	
	Yes	
	Yes	
Back to Scorecard	**Compliant Response**	**Compliant Override**
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	

	Yes	
	Yes	
	Yes	
	Yes	
	No	
	Yes	
	Yes	
	Yes	
	No	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	

Back to Scorecard	**Compliant Response**	**Compliant Override**
	Yes	
	No	
	No	
	Yes	
	Yes	
	Yes	
	Yes	
	Yes	
	Not scored	
	Yes	
	Yes	
	Not scored	

Version 4.1.0

web property via a

response compliance and importance level.

Default Importance	Importance Override
Default Importance	Importance Override

Standard Importance	
Default Importance	**Importance Override**
Critical Importance	
Critical Importance	
Minor Importance	
Minor Importance	
Default Importance	**Importance Override**
Standard Importance	
Standard Importance	
Standard Importance	

Default Importance	Importance Override
Critical Importance	
Minor Importance	
Default Importance	**Importance Override**
Standard Importance	
Minor Importance	
Default Importance	**Importance Override**
Critical Importance	
Critical Importance	
Critical Importance	
Minor Importance	
Minor Importance	
Minor Importance	
Minor Importance	

Minor Importance	
Default Importance	**Importance Override**
Minor Importance	
Minor Importance	
Standard Importance	
Minor Importance	
Minor Importance	
Critical Importance	
Minor Importance	
Minor Importance	
Minor Importance	
Minor Importance	
Minor Importance	
Critical Importance	

Minor Importance	

Default Importance	Importance Override
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	

Default Importance	Importance Override
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	

Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Default Importance	**Importance Override**

Standard Importance	
Critical Importance	
Critical Importance	
Standard Importance	
Minor Importance	
Minor Importance	
Minor Importance	
Minor Importance	

Default Importance	**Importance Override**
Critical Importance	
Minor Importance	
Minor Importance	
Minor Importance	
Default Importance	**Importance Override**
Default Importance	**Importance Override**
Critical Importance	

Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Default Importance	**Importance Override**
Standard Importance	
Critical Importance	
Default Importance	**Importance Override**
Critical Importance	
Critical Importance	
Critical Importance	
Critical Importance	
Default Importance	**Importance Override**
Critical Importance	
Critical Importance	
Critical Importance	
Critical Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Default Importance	**Importance Override**
Critical Importance	
Critical Importance	
Standard Importance	
Default Importance	**Importance Override**
Critical Importance	
Critical Importance	
Standard Importance	
Standard Importance	
Minor Importance	
Default Importance	**Importance Override**
Critical Importance	
Critical Importance	
Default Importance	**Importance Override**
Critical Importance	
Critical Importance	
Critical Importance	
Critical Importance	
Critical Importance	
Standard Importance	
Standard Importance	
Standard Importance	

Standard Importance	
Standard Importance	
Minor Importance	
Standard Importance	
Standard Importance	
Minor Importance	
Minor Importance	
Default Importance	**Importance Override**
Standard Importance	
Default Importance	**Importance Override**
Critical Importance	
Critical Importance	
Critical Importance	
Critical Importance	
Critical Importance	
Standard Importance	
Default Importance	**Importance Override**
Critical Importance	
Standard Importance	
Minor Importance	
Minor Importance	
Minor Importance	
Minor Importance	
Minor Importance	
Default Importance	**Importance Override**
Standard Importance	
Minor Importance	
Minor Importance	
Minor Importance	
Default Importance	**Importance Override**
Critical Importance	
Critical Importance	
Standard Importance	
Minor Importance	
Default Importance	**Importance Override**
Critical Importance	
Critical Importance	
Critical Importance	
Critical Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	

Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Minor Importance	

Default Importance	Importance Override
Critical Importance	
Critical Importance	
Critical Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Standard Importance	
Minor Importance	
Minor Importance	
Minor Importance	
Minor Importance	

HECVAT Analyst Reference

Connect with your higher education peers by joining the EDUCAUSE HECVAT Users Commu

You can find full tutorials on the HECVAT at educause.edu/HECVAT

This sheet provides additional context on each questions for analysts at institution

Use the "find" feature (CTRL+F on a PC or Command+F on a Mac) to search for a

General Information

GNRL-01	Solution Provider Name
GNRL-02	Solution Name
GNRL-03	Solution Description
GNRL-04	Solution Provider Contact Name
GNRL-05	Solution Provider Contact Title
GNRL-06	Solution Provider Contact Email
GNRL-07	Solution Provider Contact Phone Number
GNRL-08	Country of Company Headquarters
GNRL-09	Employee Work Locations (all)

Company Information

COMP-01	Do you have a dedicated software and system development team(s) (e.g., customer support, implementation, product management, etc.)?*
COMP-02	Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships.
COMP-03	Have you operated without unplanned disruptions to this solution in the past 12 months?
COMP-04	Do you have a dedicated information security staff or office?
COMP-05	Use this area to share information about your environment that will assist those who are assessing your company's data security program.

Required Questions

Required Questions indicate to the solution provider which questions apply to their pro

REQU-01	Are you offering either a product or platform, as opposed to only offering a service
REQU-02	Does your product or service have an interface?
REQU-03	Are you providing consulting services?
REQU-04	Does your solution have AI features, or are there plans to implement AI features in the next 12 months?
REQU-05	Does your solution process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act (HIPAA)?
REQU-06	Is the solution designed to process, store, or transmit credit card information?
REQU-07	Does operating your solution require the institution to operate a physical or virtual appliance in their own environment or to provide inbound firewall exceptions to allow your employees to remotely administer systems in the institution's environment?

Documentation

DOCU-01	Do you have a well-documented business continuity plan (BCP), with a clear owner, that is tested annually?*
DOCU-02	Do you have a well-documented disaster recovery plan (DRP), with a clear owner, that is tested annually?*
DOCU-03	Have you undergone a SSAE 18/SOC 2 audit?
DOCU-04	Do you conform with a specific industry standard security framework (e.g., NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)?
DOCU-05	Can you provide overall system and/or application architecture diagrams, including a full description of the data flow for all components of the system?

DOCU-06	Does your organization have a data privacy policy?
DOCU-07	Do you have a documented, and currently implemented, employee onboarding and offboarding policy?

IT Accessibility

ITAC-01	Solution Provider Accessibility Contact Name
ITAC-02	Solution Provider Accessibility Contact Title
ITAC-03	Solution Provider Accessibility Contact Email
ITAC-04	Solution Provider Accessibility Contact Phone Number
ITAC-05	Web Link to Accessibility Statement or VPAT
ITAC-06	Has a VPAT or ACR been created or updated for the solution and version under consideration within the past 12 months?*
ITAC-07	Will your company agree to meet your stated accessibility standard or WCAG 2.1 AA as part of your contractual agreement for the solution?*
ITAC-08	Does the solution substantially conform to WCAG 2.1 AA?*
ITAC-09	Do you have a documented and implemented process for reporting and tracking accessibility issues?*
ITAC-10	Do you have documentation to support the accessibility features of your solution?

ITAC-11	Has a third-party expert conducted an audit of the most recent version of your solution?
ITAC-12	Do you have a documented and implemented process for verifying accessibility conformance?
ITAC-13	Have you adopted a technical or legal standard of conformance for the solution?
ITAC-14	Can you provide a current, detailed accessibility roadmap with delivery timelines?
ITAC-15	Do you expect your staff to maintain a current skill set in IT accessibility?
ITAC-16	Do you have documented processes and procedures for implementing accessibility into your development lifecycle?
ITAC-17	Can all functions of the application or service be performed using only the keyboard?
ITAC-18	Does your product rely on activating a special "accessibility mode," a "lite version," or using an alternate interface (including “overlay” or AI-based

Assessment of Third Parties

THRD-01	Do you perform security assessments of third-party companies with which you share data (e.g., hosting providers, cloud services, PaaS, IaaS, SaaS)?*
THRD-02	Do you have contractual language in place with third parties governing access to institutional data?*
THRD-03	Do the contracts in place with these third parties address liability in the event of a data breach?*
THRD-04	Do you have an implemented third-party management strategy?*
THRD-05	Do you have a process and implemented procedures for managing your hardware supply chain (e.g., telecommunications equipment, export licensing, computing devices)?

Consulting Services

CONS-01	Will the consultant require access to the institution's network resources?*

CONS-02	Has the consultant received training on (sensitive, HIPAA, PCI, etc.) data handling?*
CONS-03	Is the data encrypted (at rest) while in the consultant's possession?*
CONS-04	Can access be restricted based on source IP address?*
CONS-05	Will the consulting take place on-premises?
CONS-06	Will the consultant require access to hardware in the institution's data centers?
CONS-07	Will the consultant require an account within the institution's domain (@*.edu)?
CONS-08	Will any data be transferred to the consultant's possession?

CONS-09	Will the consultant need remote access to the institution's network or systems?
Application/Service Security	
APPL-01	Are access controls for institutional accounts based on structured rules, such as role-based access control (RBAC), attribute-based access control (ABAC), or policy-based access control (PBAC)?*
APPL-02	Are you using a web application firewall (WAF)?*
APPL-03	Are only currently supported operating system(s), software, and libraries leveraged by the system(s)/application(s) that will have access to institution's data?*
APPL-04	Does your application require access to location or GPS data?
APPL-05	Does your application provide separation of duties between security administration, system administration, and standard user functions?*

APPL-06	Do you subject your code to static code analysis and/or static application security testing prior to release?*
APPL-07	Do you have software testing processes (dynamic or static) that are established and followed?*
APPL-08	Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or PBAC?
APPL-09	Does the system provide data input validation and error messages?
APPL-10	Do you have a process and implemented procedures for managing your software supply chain (e.g., libraries, repositories, frameworks, etc.)
APPL-11	Have your developers been trained in secure coding techniques?

APPL-12	Was your application developed using secure coding techniques?
APPL-13	If mobile, is the application available from a trusted source (e.g., App Store, Google Play Store)?
APPL-14	Do you have a fully implemented policy or procedure that details how your employees obtain administrator access to institutional instance of the application?
Authentication, Authorization, and Account Management	
AAAI-01	Does your solution support single sign-on (SSO) protocols for user and administrator authentication?*
AAAI-02	For customers not using SSO, does your solution support local authentication protocols for user and administrator authentication?*
AAAI-03	For customers not using SSO, can you enforce password/passphrase complexity requirements (provided by the institution)?*
AAAI-04	For customers not using SSO, does the system have password complexity or length limitations and/or restrictions?*
AAAI-05	For customers not using SSO, do you have documented password/passphrase reset procedures that are currently implemented in the system and/or customer support?*
AAAI-06	Does your organization participate in InCommon or another eduGAIN-affiliated trust federation?*

AAAI-07	Are there any passwords/passphrases hard-coded into your systems or solutions?*
AAAI-08	Are you storing any passwords in plaintext?*
AAAI-09	Are audit logs available that include AT LEAST all of the following: login, logout, actions performed, and source IP address?*
AAAI-10	Describe or provide a reference to the (a) system capability to log security/authorization changes, as well as user and administrator security events (i.e., physical or electronic), such as login failures, access denied, changes accepted; and (b) all requirements necessary to implement logging and monitoring on the system. Include (c) information about SIEM/log collector usage.*
AAAI-11	Can you provide the institution documentation regarding the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how)?*
AAAI-12	For customers not using SSO, does your application support integration with other authentication and authorization systems?
AAAI-13	Do you allow the customer to specify attribute mappings for any needed information beyond a user identifier? (e.g., Reference eduPerson, ePPA/ePPN/ePE)

AAAI-14	For customers not using SSO, does your application support directory integration for user accounts?
AAAI-15	Does your solution support any of the following web SSO standards: SAML2 (with redirect flow), OIDC, CAS, or other?
AAAI-16	Do you support differentiation between email address and user identifier?
AAAI-17	For customers not using SSO, does your application and/or user frontend/portal support multifactor authentication (e.g., Duo, Google Authenticator, OTP, etc.)?
AAAI-18	Does your application automatically lock the session or log out an account after a period of inactivity?
Change Management	
CHNG-01	Will the institution be notified of major changes to your environment that could impact the institution's security posture?*
CHNG-02	Does the system support client customizations from one release to another?*
CHNG-03	Do you have an implemented system configuration management process (e.g.,secure "gold" images, etc.)?*

CHNG-04	Do you have a documented change management process?
CHNG-05	Does your change management process minimally include authorization, impact analysis, testing, and validation before moving changes to production?
CHNG-06	Does your change management process verify that all required third-party libraries and dependencies are still supported with each major change?
CHNG-07	Do you have policy and procedure, currently implemented, managing how critical patches are applied to all systems and applications?
CHNG-08	Have you implemented policies and procedures that guide how security risks are mitigated until patches can be applied?
CHNG-09	Do clients have the option to not participate in or postpone an upgrade to a new release?
CHNG-10	Do you have a fully implemented solution support strategy that defines how many concurrent versions you support?
CHNG-11	Do you have a release schedule for product updates?
CHNG-12	Do you have a technology roadmap, for at least the next two years, for enhancements and bug fixes for the solution being assessed?

CHNG-13	Can solution updates be completed without institutional involvement (i.e., technically or organizationally)?
CHNG-14	Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?
CHNG-15	Do procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval)?
CHNG-16	Do you have a systems management and configuration strategy that encompasses servers, appliances, cloud services, applications, and mobile devices (company and employee owned)?
Data	
DATA-01	Will the institution's data be stored on any devices (database servers, file servers, SAN, NAS, etc.) configured with non-RFC 1918/4193 (i.e., publicly routable) IP addresses?*
DATA-02	Is the transport of sensitive data encrypted using security protocols/algorithms (e.g., system-to-client)?*
DATA-03	Is the storage of sensitive data encrypted using security protocols/algorithms (e.g., disk encryption, at-rest, files, and within a running database)?*
DATA-04	Do all cryptographic modules in use in your solution conform to the Federal Information Processing Standards (FIPS PUB 140-2 or 140-3)?*

DATA-05	Will the institution's data be available within the system for a period of time at the completion of this contract?*
DATA-06	Are these rights retained even through a provider acquisition or bankruptcy event?*
DATA-07	Do backups containing the institution's data ever leave the institution's data zone either physically or via network routing?*
DATA-08	Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?*
DATA-09	At the completion of this contract, will data be returned to the institution and/or deleted from all your systems and archives?
DATA-10	Can the institution extract a full or partial backup of data?
DATA-11	Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?
DATA-12	Are you performing off-site backups (i.e., digitally moved off site)?

DATA-13	Are physical backups taken off-site (i.e., physically moved off site)?
DATA-14	Are data backups encrypted?
DATA-15	Do you have a media handling process that is documented and currently implemented that meets established business needs and regulatory requirements, including end-of-life, repurposing, and data-sanitization procedures?
DATA-16	Does the process described in DATA-15 adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?
DATA-17	Does your staff (or third party) have access to institutional data (e.g., financial, PHI, or other sensitive information) through any means?
DATA-18	Do you have a documented and currently implemented strategy for securing employee workstations when they work remotely (i.e., not in a trusted computing environment)?

DATA-19	Does the environment provide for dedicated single-tenant capabilities? If not, describe how your solution or environment separates data from different customers (e.g., logically, physically, single tenancy, multi-tenancy).
DATA-20	Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?
DATA-21	In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide 90 days for customers to get their data out of the system and migrate applications?
DATA-22	Are involatile backup copies made according to predefined schedules and securely stored and protected?
DATA-23	Do you have a cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement) that is documented and currently implemented, for all system components (e.g., database, system, web, etc.)?
Datacenter	
DCTR-01	Select your hosting option.

DCTR-02	Is a SOC 2 Type 2 report available for the hosting environment?
DCTR-03	Are you generally able to accommodate storing each institution's data within its geographic region?
DCTR-04	Are the data centers staffed 24 hours a day, seven days a week (i.e., 24 x 7 x 365)?
DCTR-05	Are your servers separated from other companies via a physical barrier, such as a cage or hard walls?
DCTR-06	Does a physical barrier fully enclose the physical space, preventing unauthorized physical contact with any of your devices?*

DCTR-07	Are your primary and secondary data centers geographically diverse?
DCTR-08	Is the service hosted in a high-availability environment?
DCTR-09	Is redundant power available for all data centers where institutional data will reside?
DCTR-10	Are redundant power strategies tested?*
DCTR-11	Does the center where the data will reside have cooling and fire-suppression systems that are active and regularly tested?
DCTR-12	Do you have Internet Service Provider (ISP) redundancy?
DCTR-13	Does every data center where the institution's data will reside have multiple telephone company or network provider entrances to the facility?
DCTR-14	Do you require multifactor authentication for all administrative accounts in your environment?
DCTR-15	Are you using your cloud provider's available hardening tools or pre-hardened images?

DCTR-16	Does your cloud solution provider have access to your encryption keys?
Firewalls, IDS, IPS, and Networking	
FIDP-01	Are you utilizing a stateful packet inspection (SPI) firewall?*
FIDP-02	Do you have a documented policy for firewall change requests?*
FIDP-03	Have you implemented an intrusion detection system (network-based)?*
FIDP-04	Do you employ host-based intrusion detection?*
FIDP-05	Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?*
FIDP-06	Is authority for firewall change approval documented? Please list approver names or titles in Additional Info.
FIDP-07	Have you implemented an intrusion prevention system (network-based)?

FIDP-08	Do you employ host-based intrusion prevention?
FIDP-09	Are you employing any next-generation persistent threat (NGPT) monitoring?
FIDP-10	Is intrusion monitoring performed internally or by a third-party service?
FIDP-11	Do you monitor for intrusions on a 24 x 7 x 365 basis?
Policies, Processes, and Procedures	
PPPR-01	Do you have a documented patch management process?*
PPPR-02	Can your organization comply with institutional policies on privacy and data protection with regard to users of institutional systems, if required?*
PPPR-03	Is your company subject to the institution's geographic region's laws and regulations?*

PPPR-04	Can you accommodate encryption requirements using open standards?
PPPR-05	Do you have a documented systems development life cycle (SDLC)?
PPPR-06	Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?
PPPR-07	Do you require new employees to fill out agreements and review policies?
PPPR-08	Do you have a documented information security policy?
PPPR-09	Are information security principles designed into the product lifecycle?
PPPR-10	Will you comply with applicable breach notification laws?

PPPR-11	Do you have an information security awareness program?
PPPR-12	Is security awareness training mandatory for all employees?
PPPR-13	Do you have process and procedure(s) documented, and currently followed, that require a review and update of the access list(s) for privileged accounts?
PPPR-14	Do you have documented, and currently implemented, internal audit processes and procedures?
PPPR-15	Does your organization have physical security controls and policies in place?

Incident Handling

HFIH-01	Do you have a formal incident response plan?
HFIH-02	Do you either have an internal incident response team or retain an external team?

HFIH-03	Do you have the capability to respond to incidents on a 24 x 7 x 365 basis?
HFIH-04	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?

Vulnerability Management

VULN-01	Are your systems and applications scanned with an authenticated user account for vulnerabilities (that are remediated) prior to new releases?*
VULN-02	Will you provide results of application and system vulnerability scans to the institution?*
VULN-03	Will you allow the institution to perform its own vulnerability testing and/or scanning of your systems and/or application, provided that testing is performed at a mutually agreed upon time and date?*
VULN-04	Have your systems and applications had a third-party security assessment completed in the last year?
VULN-05	Do you regularly scan for common web application security vulnerabilities (e.g., SQL injection, XSS, XSRF, etc.)?

VULN-06	Are your systems and applications regularly scanned externally for vulnerabilities?
HIPAA Compliance	
HIPA-01	Do your workforce members receive regular training related to the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules and the HITECH Act?*
HIPA-02	Have you identified areas of risk?*
HIPA-03	Have the relevant policies/plans been tested?*
HIPA-04	Have you entered into a Business Associate Agreements with all subcontractors who may have access to protected health information (PHI)?*
HIPA-05	Do you monitor or receive information regarding changes in HIPAA regulations?
HIPA-06	Has your organization designated HIPAA Privacy and Security officers as required by the rules?
HIPA-07	Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)?
HIPA-08	Have you conducted a risk analysis as required under the HIPAA Security Rule?
HIPA-09	Have you taken actions to mitigate the identified risks?
HIPA-10	Does your application require user and system administrator password changes at a frequency no greater than 90 days?

HIPA-11	Does your application require users to set their own password after an administrator reset or on first use of the account?
HIPA-12	Does your application lock out an account after a number of failed login attempts?
HIPA-13	Does your application automatically lock or log-out an account after a period of inactivity?
HIPA-14	Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e., database accounts, etc.)?
HIPA-15	If the application is institution-hosted, can all service level and administrative account passwords be changed by the institution?
HIPA-16	Does your application provide the ability to define user access levels?
HIPA-17	Does your application support varying levels of access to administrative tasks defined individually per user?
HIPA-18	Does your application support varying levels of access to records based on user ID?
HIPA-19	Is there a limit to the number of groups to which a user can be assigned?
HIPA-20	Do accounts used for solution provider-supplied remote support abide by the same authentication policies and access logging as the rest of the system?
HIPA-21	Does the application log record access including specific user, date/time of access, and originating IP or device?
HIPA-22	Does the application log administrative activity, such as user account access changes and password changes, including specific user, date/time of changes, and originating IP or device?
HIPA-23	Do you retain logs for at least as long as required by HIPAA regulations?
HIPA-24	Can the application logs be archived?

HIPA-25	Can the application logs be saved externally?
HIPA-26	Do you have a disaster recovery plan and emergency mode operation plan?
HIPA-27	Can you provide a HIPAA compliance attestation document?
HIPA-28	Are you willing to enter into a Business Associate Agreement (BAA)?
HIPA-29	Do your data backup and retention policies and practices meet HIPAA requirements?
Payment Card Industry Data Security Standard (PCI DSS)	
PCID-01	Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?*
PCID-02	Is the application listed as an approved Payment Application Data Security Standard (PA-DSS) application?*
PCID-03	Does the system or solutions use a third party to collect, store, process, or transmit cardholder (payment/credit/debt card) data?*
PCID-04	Do your systems or solutions store, process, or transmit cardholder (payment/credit/debt card) data?
PCID-05	Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?
PCID-06	Are you classified as a service provider?
PCID-07	Are you on the list of Visa approved service providers?
PCID-08	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?
PCID-09	Describe the architecture employed by the system to verify and authorize credit card transactions.
PCID-10	What payment processors/gateways does the system support?

PCID-11	Can the application be installed in a PCI DSS–compliant manner?
PCID-12	Include documentation describing the system's abilities to comply with the PCI DSS and any features or capabilities of the system that must be added or changed in order to operate in compliance with the standards.
On-Premises Data Solutions	
OPEM-01	Do you support role-based access control (RBAC) for system administrators?
OPEM-02	Can your employees access customer systems remotely?
OPEM-03	Can you provide overall system and/or application architecture diagrams including a full description of the data communications architecture for all components of the system?
OPEM-04	Do you require remote management of the system?
OPEM-05	If you answered "yes" to OPEM-04, are your remote actions and changes logged or otherwise visible to the campus?
OPEM-06	If you maintain remote access to the system, will you handle data in a FERPA-compliant manner?

OPEM-07	Do you support campus status monitoring through SNMPv3 or other means?
OPEM-08	Describe or provide a reference to any other safeguards used to monitor for malicious activity.
OPEM-09	Describe how long your organization has conducted business in this area.
OPEM-10	Do you have existing higher education customers?
General Privacy	
PRGN-01	Does your solution process FERPA-related data?
PRGN-02	Does your solution process GDPR-related or PIPL-related data?
PRGN-03	Does your solution process personal data regulated by state law(s) (e.g., CCPA)?
PRGN-04	Does your solution process user-provided data that may contain regulated information?
PRGN-05	Web Link to Product/Service Privacy Notice
Privacy-Specific Company Details	
PCOM-01	Have you had a personal data breach in the past three years that involved reporting to a governmental agency, notice to individuals (including voluntary notice), or notice to another organization or institution?*
PCOM-02	Use this area to share information about your privacy practices that will assist those who are assessing your company data privacy program.*
PCOM-03	Have you had any data privacy policy or law violations in the past 36 months?

PCOM-04	Do you have a dedicated data privacy staff or office?
Privacy-Specific Documentation	
PDOC-01	If you have completed a SOC 2 audit, does it include the Privacy Trust Service Principle?
PDOC-02	Do you conform with a specific industry-standard privacy framework (e.g., NIST Privacy Framework, GDPR, ISO 27701)?
PDOC-03	Does your employee onboarding and offboarding policy include training of employees on information security and data privacy?
Privacy of Third Parties	
PTHP-01	Do you have contractual agreements with third parties that require them to maintain standards and to comply with all regulatory requirements?*
PTHP-02	Do you perform privacy impact assesments of third parties that collect, process, or have access to personal data to ensure they meet industry and regulatory standards and to mitigate harmful, unethical, or discriminatory impacts on data subjects?
Privacy Change Management	
PCHG-01	Does your change management process include privacy review and approval?
PCHG-02	Do you have policy and procedure, currently implemented, guiding how privacy risks are mitigated until they can be resolved?
Privacy of Sensitive Data	
PDAT-01	Do you collect, process, or store demographic information?*
PDAT-02	Do you capture or create genetic, biometric, or behaviometric information (e.g., facial recognition or fingerprints)?*

PDAT-03	Do you combine institutional data (including "de-identified," "anonymized," or otherwise masked data) with personal data from any other sources?*
PDAT-04	Is institutional data coming into or going out of the United States at any point during collection, processing, storage, or archiving?
PDAT-05	Do you capture device information (e.g., IP address, MAC address)?
PDAT-06	Does any part of this service/project involve a web/app tracking component (e.g., use of web-tracking pixels, cookies)?
PDAT-07	Does your staff (or a third party) have access to institutional data (e.g., financial, PHI, or other sensitive information) through any means?
PDAT-08	Will you handle personal data in a manner compliant with all relevant laws, regulations, and applicable institution policies?
Privacy Policies and Procedures	
PRPO-01	Do you have a documented privacy management process?
PRPO-02	Are privacy principles designed into the product lifecycle (i.e., privacy-by-design)?
PRPO-03	Will you comply with applicable breach notification laws?
PRPO-04	Will you comply with the institution's policies regarding user privacy and data protection?
PRPO-05	Is your company subject to the laws and regulations of the institution's geographic region?
PRPO-06	Do you have a privacy awareness/training program?*
PRPO-07	Is privacy awareness training mandatory for all employees?
PRPO-08	Is AI privacy and ethics awareness/training required for all employees who work with AI?
PRPO-09	Do you have any decision-making processes that are completely automated (i.e., there is no human involvement)?

PRPO-10	Do you have a documented process for managing automated processing, including validations, monitoring, and data subject requests?
PRPO-11	Do you have a documented policy for sharing information with law enforcement?
PRPO-12	Do you share any institutional data with law enforcement without a valid warrant?*
PRPO-13	Does your incident response team include a privacy analyst/officer?
International Privacy	
INTL-01	Will data be collected from or processed in or stored in the European Economic Area (EEA)?
INTL-02	Do you have a data protection officer (DPO)?
INTL-03	Will you sign appropriate GDPR Standard Contractual Clauses (SCCs) with the institution?
INTL-04	Will data be collected from or processed in or stored in China?
INTL-05	Do you comply with PIPL security, privacy, and data localization requirements?
Data Privacy	
DRPV-01	Have you performed a Data Privacy Impact Assesssment for the solution/project?
DRPV-02	Do you provide an end-user privacy notice about privacy policies and procedures that identify the purpose(s) for which personal information is
DRPV-03	Do you describe the choices available to the individual and obtain implicit or explicit consent with respect to the collection, use, and disclosure of personal
DRPV-04	Do you collect personal information only for the purpose(s) identified in the agreement with an institution or, if there is none, the purpose(s) identified in
DRPV-05	Do you have a documented list of personal data your service maintains?
DRPV-06	Do you retain personal information for only as long as necessary to fulfill the stated purpose(s) or as required by law or regulation and thereafter
DRPV-07	Do you provide individuals with access to their personal information for review and update (i.e., data subject rights)?
DRPV-08	Do you disclose personal information to third parties only for the purpose(s) identified in the privacy notice or with the implicit or explicit consent of the
DRPV-09	Do you protect personal information against unauthorized access (both physical and logical)?
DRPV-10	Do you maintain accurate, complete, and relevant personal information for the purposes identified in the privacy notice?

DRPV-11	Do you have procedures to address privacy-related noncompliance complaints and disputes?
DRPV-12	Do you "anonymize," "de-identify," or otherwise mask personal data?
DRPV-13	Do you or your subprocessors use or disclose "anonymized," "de-identified," or otherwise masked data for any purpose other than those identified in the agreement with an institution (e.g., sharing with ad networks or data brokers, marketing, creation of profiles, analytics unrelated to services provided to institution)?
DRPV-14	Do you certify stop-processing requests, including any data that is processed by a third party on your behalf?
DRPV-15	Do you have a process to review code for ethical considerations?
Privacy and AI	
DPAI-01	Does your service use AI for the processing of institutional data?
DPAI-02	Is any institutional data retained in AI processing?*
DPAI-03	Do you have agreements in place with third parties or subprocessors regarding the protection of customer data and use of AI?*
DPAI-04	Will institutional data be processed through a third party or subprocessor that also uses AI?
DPAI-05	Is AI processing limited to fully licensed commercial enterprise AI services?
DPAI-06	Will institutional data be used or processed by any shared AI services?
DPAI-07	Do you have safeguards in place to protect institutional data and data privacy from unintended AI queries or processing?

DPAI-08	Do you provide choice to the user to opt out of AI use?

AI Qualifying Questions

AIQU-01	Does your solution leverage machine learning (ML) or do you plan to do so in the next 12 months?
AIQU-02	Does your solution leverage a large language model (LLM) or do you plan to do so in the next 12 months?

General AI Questions

AIGN-01	Does your solution have an AI risk model when developing or implementing your solution's AI model?*
AIGN-02	Can your solution's AI features be disabled by tenant and/or user?*
AIGN-03	Have your staff completed responsible AI training?*
AIGN-04	Please describe the capabilities of your solution's AI features.
AIGN-05	Does your solution support business rules to protect sensitive data from being ingested by the AI model?

AI Policy

AIPL-01	Are your AI developer's policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks conspicuously posted, unambiguous, and implemented effectively?*
AIPL-02	Have you identified and measured AI risks?*
AIPL-03	In the event of an incident, can your solution's AI features be disabled in a timely manner?*
AIPL-04	If disabled because of an incident, can your solution's AI features be re-enabled in a timely manner?*
AIPL-05	Do you have documented technical and procedural processes to address potential negative impacts of AI as described by the AI Risk Management Framework (RMF)?
AI Data Security	
AISC-01	If sensitive data is introduced to your solution's AI model, can the data be removed from the AI model by request?*
AISC-02	Is user input data used to influence your solution's AI model?*
AISC-03	Do you provide logging for your solution's AI feature(s) that includes user, date, and action taken?*
AISC-04	Please describe how you validate user inputs.
AISC-05	Do you plan for and mitigate supply-chain risk related to your AI features?

AI Machine Learning

AIML-01	Do you separate ML training data from your ML solution data?*
AIML-02	Do you authenticate and verify your ML model's feedback?*
AIML-03	Is your ML training data vetted, validated, and verified before training the solution's AI model?
AIML-04	Is your ML training data monitored and audited?
AIML-05	Have you limited access to your ML training data to only staff with an explicit business need?
AIML-06	Have you implemented adversarial training or other model defense mechanisms to protect your ML-related features?
AIML-07	Do you make your ML model transparent through documentation and log inputs and outputs?
AIML-08	Do you watermark your ML training data?

AI Large Language Model (LLM)

AILM-01	Do you limit your solution's LLM privileges by default?*

AILM-02	Is your LLM training data vetted, validated, and verified before training the solution's AI model?*
AILM-03	Do any actions taken by your solution's LLM features or plugins require human intervention?*
AILM-04	Do you limit multiple LLM model plugins being called as part of a single input?*
AILM-05	Do you limit your solution's LLM resource use per request, per step, and per action?
AILM-06	Do you leverage LLM model tuning or other model validation mechanisms?

nity Group

ns. In most cases, you will find a reason for each question as well as follow-up inquir
question code

Reason for Question
Determines where solution provider employees will be physically located.
Reason for Question
Understanding the development team size (and capabilities) of a solution provider has a significant impact on their ability to produce and maintain code, adhering to secure coding best
This information defines the scale of company (support, resources, skillsets), general information about the organization that may be concerning.
We want transparency from the solution provider, and an honest answer to this question, regardless of the response, is a good step in building trust.
The size and capabilities of a solution provider's security program have a significant impact on its ability to respond effectively to a security incident. The size of a solution provider will determine their security operation size or lack thereof. Use the knowledge of this response when evaluating other solution provider statements.
For the 20% that HECVAT may not cover, this gives the solution provider a chance to support their other responses. Beware when this area is populated with sales hype or other irrelevant information. Thorough documentation, supporting evidence, and/or robust responses go a long way in building trust in this assessment process.

Reason for Question
duct or service.
The answer to this question indicates if the "Product" and "Infrastructure" tabs are required
The answer to this question indicates if the "IT Accessibility" questions are required
The answer to this question indicates if the "Consulting" questions are required
The answer to this question indicates if the "AI" questions are required
The answer to this question indicates if the "HIPAA" questions are required
The answer to this question indicates if the "PCI DSS" questions are required
The answer to this question indicates if the "On-Premises Data Solutions" questions are required

Reason for Question
SSAE 18 and SOC2 audits are standard documentation, relevant to institutions requiring a solution provider to undergo SSAE 18 audits.
The details of the standard are not the focus here; it is the fact that a solution provider builds their environment around a standard and that they continually evaluate and assess their security
Managing and protecting institution data is the reason organizations perform security and risk assessments. Privacy policies outline how solution providers will obtain, use, share, and protect institutional data and as such, should be robust in its language. Beware of vaguely worded privacy policies.

Managing and protecting institutional data is the reason organizations perform security and risk assessments. Privacy policies outline how solution providers will obtain, use, share, and protect institutional data and as such, should be robust in its language. Beware of vaguely worded privacy policies.
Managing and protecting a solution provider's assets through appropriate human resource management is of upmost importance. Knowing how roles and access controls are implemented (directed by policy) within a solution provider's infrastructure during the onboarding and offboarding processes is indicative of how access control is regarded in other areas on the provider (solution provider).
Reason for Question
VPATs (Voluntary Product Accessibility Template) / ACRs (Accessibility Conformance Report, a completed VPAT) are standard accessibility reporting formats from the ITIC
Federal regulation requires that technology products conform to WCAG 2.1 AA. Technology platforms that do not substantially conform to this standard put schools at risk of not complying with these requirements.
Federal regulation requires that technology products conform to WCAG 2.1 AA. Technology platforms that do not substantially conform to this standard put schools at risk of not complying with these requirements.
Has the solution provider documented any additional information needed by users in order to create accessible products with the solution? Are there tutorials, if needed, on how assistive technology users can best use the solution (platforms tested and works best, shortcuts) etc.? In other words, are they taking care of the end users? Accessibility is more than completing checklists.

Third-party test results lend more credence to accessibility claims in documentation. It is possible that well-qualified first parties may still deliver meaningful results via a VPAT/ACR. Ensuring results for the most recent versions means purchasing decisions are not made with outdated information.
The goal of accessibility is ultimately usability by persons with disabilities. Expert staff and automated testing are important, but automated tools can only detect ~25% of issues so must be supplemented with additional methodologies. Best practice would include testing by people with disabilities. At minimum, some manual testing needs to be conducted in the verification process. The use of overlays or AI plugin solutions to help products "automatically conform" with accessibility guidelines is presently inadequate and should impact scores negatively.
Knowing the standard solution providers aim for ensures aligned goals. For example, WCAG 2.0 or §508 specify accessibility standards from 2008 that may not meet present needs. WCAG 2.2 is the most current, and 2.1 AA is the most commonly cited current technical accessibility standard.
If solution do not fully conform to accessibility standards, it is important that solution providers have a roadmap specifying how they will work to achieve it. A roadmap with delivery timelines is best supported by evidence of prior delivery on such timelines. Analysts can better predict time to conformance and institutions can plan accordingly.
Having accessibility expertise within the staff supports the proactive development of accessible solutions. If staff lack sufficient accessibility expertise, then accessibility improvements may only be the result of the solution provider reacting to issues or reports of access barriers submitted by clients of the solution provider.
This question is designed to understand how accessibility is included in new versions and features of solutions, particularly with solution providers that implement Agile or similar methodologies where software is updated frequently and continuously.
One critical accessibility requirement is the full use of a product using only the keyboard, -no mouse or trackpad. This requirement is easy for a nontechnical or non-accessibility expert to understand and verify.
Third-party overlays or add-ons are not sufficient for products to conform with accessibility Standards (more information at <https://overlayfactsheet.com>). Lite or alternate versions for

Reason for Question
In the context of the CIA triad, this question is focused on system integrity, ensuring that system changes are only executed by authorized users. Additionally, it is expected that devices (for administrators, solution provider staff, and affiliates) that are used to access the solution provider's systems are properly managed and secured.
The sharing of institutional data to fourth-parties may increase the risk to the institutation and thus, we want to know who gets what data, when they get that data, and why they get that data.
Knowing the protections and legal agreements in place for third-party data sharing may assist analysts in determininng residual risk.
Every organization needs to actively understand and manage its supply chain. The solution provider's understanding of who their third-party partners are and their ability to manage those relationships effectively and consistently speaks to the amount of risk your institution is taking on by contracting with them. Modern technologies allow for rapid deployment of features and with them come changes to an established code environment. The focus of this question is to verify a solution provider's practice of regression testing their code and verifying that previously nonexistent risks are not introduced into a known, secured environment.
Understanding a solution provider's hardware supply chain can reveal infrastructure risks that may not be apparent by other means. In some cases, the use of trusted components may be favorable. In others, it may initiate the assessment of the solution provider's environment in more detail and/or expand the scope of the institution's assessment.

Reason for Question
Consultants are often used to implement, maintain, fix, and assess technology environments. In these cases, third-party consultants have access to institutional data, and appropriate access, whether remote or onsite, must be protected during the consulting engagement.

Consultants are often used to implement, maintain, fix, and assess technology environments. In these cases, third-party consultants have access to institutional data, and appropriate access, whether remote or onsite, must be protected during the consulting engagement.
Consultants are often used to implement, maintain, fix, and assess technology environments. In these cases, third-party consultants have access to institutional data, and appropriate access, whether remote or onsite, must be protected during the consulting engagement.
Consultants are often used to implement, maintain, fix, and assess technology environments. In these cases, third-party consultants have access to institutional data, and appropriate access, whether remote or onsite, must be protected during the consulting engagement.
Consultants are often used to implement, maintain, fix, and assess technology environments. In these cases, third-party consultants have access to institutional data, and appropriate access, whether remote or onsite, must be protected during the consulting engagement.
Consultants are often used to implement, maintain, fix, and assess technology environments. In these cases, third-party consultants have access to institutional data, and appropriate access, whether remote or onsite, must be protected during the consulting engagement.
Consultants are often used to implement, maintain, fix, and assess technology environments. In these cases, third-party consultants have access to institutional data, and appropriate access, whether remote or onsite, must be protected during the consulting engagement.
Consultants are often used to implement, maintain, fix, and assess technology environments. In these cases, third-party consultants have access to institutional data, and appropriate access, whether remote or onsite, must be protected during the consulting engagement.

Consultants are often used to implement, maintain, fix, and assess technology environments. In these cases, third-party consultants have access to institutional data, and appropriate access, whether remote or onsite, must be protected during the consulting engagement.

Reason for Question

Understanding access control capabilities allows an institution to estimate the type of maintenance efforts will be involved to manage a system. Depending on the users, concerns may or not be elevated. The value of this question is largely determined by the deployment strategy and use case of the solution under review. This question is specific to end users.

The use case, solution provider infrastructure, and types of services offered will greatly affect the need for various firewalling devices. The focus of this question is integrity, ensuring that the systems hosting institutional data are limited in need-only communications. The use of a WAF is important in systems in which a solution provider has limited access to the code infrastructure.

Solution Provider responses to this question provide clarity on environment constraints that may exist and/or influence future development, configurations, infrastructure, etc. Although the solution provider response may not directly affect end users, the risks of the underlying infrastructure are better understood.

Sharing location data significantly increases risk factors for users. It's important to understand if this is required.

Managing a solution may rely on various teams to administrate a system. In this question, it is security operations and systems administration. This question is focused on how system(s) administration, and the segregation of duties, are implemented in the solution provider's organization, so that system administrators do not also have security responsibilities (e.g., monitoring, mitigating, reporting, etc.).

Code analysis (prior to implementation) can decrease the number of vulnerabilities within a system. Depending on the insight a solution provider has into their code, code testing should be expected. When a solution provider outsources their coding efforts, the use of a web application firewall may be appropriate. In this case, reference the solution provider's response to their use of a WAF.
Code analysis (prior to implementation) can decrease the number of vulnerabilities within a system. Depending on the insight a solution provider has into their code, code testing should be expected.
Managing a solution may rely on various professionals to administer a system. This question is focused on how administration, and the segregation of functions, is implemented within the solution provider's infrastructure.
Input validation is a secure coding best practice, so confirming its implementation is normally a high priority. Error messages (to the system and user) can be used to detect abnormal use and to better protect institutional data. Depending on the criticality of data and the flow of said data, an institution's risk tolerance will be unique to their environment.
Understanding system requirements and/or dependencies (e.g., libraries, repositories, frameworks, toolkits, modules, etc.) can reveal infrastructure risks that may not be apparent by other means. In some cases, the use of trusted components may be favorable. In others, it may initiate the assessment of the solution provider's environment in more detail and/or expand the scope of the institution's assessment.
The adherence to secure coding best practices better positions a solution provider to maintain the CIA triad. Use the knowledge of this response when evaluating other solution provider statements, particularly those focused on development and the protection of communications.

The adherence to secure coding best practices better positions a solution provider to maintain the CIA triad. Use the knowledge of this response when evaluating other solution provider statements, particularly those focused on development and the protection of communications.

Distributing application via known, moderately vetted application platform decreases the chances of malicious code distribution. Stand-alone deployments (nontrusted sources) should be looked at more closely.

Protecting administrative accounts is crucial to maintaining system integrity in any environment. This question is targeting privilege creep and unmanaged privileged acccounts to determine if the solution provider properly manages access control in their application/system environments.

Reason for Question

This question is to set account management expectations for the institution. A system that can integrate with existing, vetted solutions has its advantages and may have less administrative overhead. Also, adherence to standards here gives credit to other standards-oriented questions/responses.

The purpose of this question is understand the solution provider's authentication infrastructure so that additional questions can be formulated for the institution's use case. If you will be using SSO, consider marking this question as "Do Not Score" in column J of the evaluation tab.

Many institutions have a policy focused on passwords/passphrases, and this question confirms the capacity of a solution provider's solution to comply. If you will be using SSO, consider marking this question as "Do Not Score" in column J of the evaluation tab.

Many institutions have a policy focused on passwords/passphrases, and this question confirms the capacity of a solution provider's solution to comply. If you will be using SSO, consider marking this question as "Do Not Score" in column J of the evaluation tab.

Account management can be a time-consuming part of an information system. Account reset capabilities, built into a system, can reduce burden on institutional support services. If you will be using SSO, consider marking this question as "Do Not Score" in column J of the evaluation tab.

This question defines the solution provider's scope of federated identity practices and their willingness to embrace higher education requirements.

The response to this question can reveal the use (or not) of coding best practices. If passwords/passphrases are hard-coded into systems/productions, the solution provider should provide robust details supporting why this is required.

The focus of this question is confidentiality. It is a straightforward question confirming the encryption of user authentication details.

Strong logging capabilities are vital to the proper management of a system. Implementing an immature system that lacks sufficient logging capabilities exposes an institution to great risk. Depending on your risk tolerance and the use case, your institution may or may not be concerned. The focus of this question is end-user logs.

Strong logging capabilities are vital to the proper management of a system. Implementing an immature system that lacks sufficient logging capabilities exposes an institution to great risk. Depending on your risk tolerance and the use case, your institution may or may not be concerned. The focus of this question is system-related logs (including but not limited to events, state changes, control modification, etc.).

There are multiple components of this question. When assessing, ensure that the solution provider responds to them all. Logs that are not properly managed may not be available when needed. The purpose of this question is to ensure that the solution provider has a proper security mindset to ensure proper monitoring practices.

This question is to set account management expectations for the institution. A system that can integrate with existing, vetted solutions has its advantages and may have less administrative overhead. Also, adherence to standards here gives credit to other standards-oriented questions/responses. If you will be using SSO, consider marking this question as "Do Not Score" in column J of the evaluation tab.

This questions allows an institution to know solution provider system limitations and to help them gauge the resources (that may be needed to implement) required to successfully integrate the solution with institution systems.

System (technical and security) administration is complex, and it is important to understand a system's capabilities to integrate with existing security and access systems. Having to maintain additional accounts increases overhead and may impact your institution's risk footprint. If you will be using SSO, consider marking this question as "Do Not Score" in column J of the evaluation tab.
This question is to set account management expectations for the institution. A system that can integrate with existing, vetted solutions has its advantages and may have less administrative overhead. Also, adherence to standards here gives credit to other standards-oriented questions/responses.
This questions allows an institution to know solution provider system limitations and to help them gauge the resources (that may be needed to implement) required to successfully integrate the solution with institution systems.
2FA/MFA, implemented correctly, strengthens the security state of a system. 2FA/MFA is commonly implemented and in many use cases is a requirement for account protection purposes. If you will be using SSO, consider marking this question as "Do Not Score" in column J of the evaluation tab.
This is a question to ensure account integrity and institutional data confidentiality.

Reason for Question
Notification expectations should be set earlier in the contract/assessment process. Timelines, correspondence medium, and playbook details are all aspects to keep in mind when assessing this response.
The solution provider's solution characteristics and the institution's use case will determine the relevancy of this question. The purpose of this question is to understand the underlying infrastructure and how it is maintained across all customers.
Hardware lifecycles and continuous software updates creates an always-changing landscape in information technology. The focus of this question is the integrity of a solution provider's infrastructure. Mismanagement of system configurations can lead to breakdowns in layers of security.

The lack of a change management function is indicative of immature program processes. Answers to this question can provide insight into how well their responses (on the HECVAT) represent their actual environment(s).
This question outlines a mature change management process. Changes should be analyzed for impact, officially approved, tested, and performed by authorized users.
This question is fundamentally about supply chain. The solution provider should be able to document its procedures around tracking libraries maintained by third parties.
Answers to this question will reveal the solution provider’s knowledge of their IT assets and their ability to respond to notifications about their systems and software.
New vulnerabilities are published every day, and solution providers have a responsibility to maintain their software(s). The fundamental nature of operation will expose some risks to the system, but it is crucial that a solution provider recognize its responsibilities and have a plan to implement them, when this time arrives.
Unplanned and/or unexpected changes in a complex environment can introduce intolerable risks to the institution. Based on the operating environment of the institution, it may be necessary to postpone (or properly plan) the change to a system. The solution provider's response should clarify their use of a "one code base" method or the ability to run multiple versions concurrently.
Supporting multiple versions of a solution is challenging. Understanding the solution provider's strategy and resources will provide insight into its ability to adequately support their customers
Answers to this question will reveal the solution provider’s ability to plan in the short term. This is valuable information for customers so they can anticipate updates and potential bug fixes.
Answers to this question will reveal the solution provider’s ability to plan for the future of their solution.

The response to this question allows the institution to understand the information technology resources required to properly maintain the solution provider's system. Initial acquisition and setup is important to assess, but the long-term maintenance (and the risks that come with it) should be clearly defined. Use the response to this question to pivot to other questions and/or verify other solution provider responses.
Restricting system updates to a standard maintenance timeframe is important for ensuring that changes to production systems do not impact operations. It’s also important for troubleshooting any problems that may occur as a result of the changes.
In the context of the CIA triad, this question is focused on system integrity, ensuring that system changes are only executed by authorized users. In the event of emergency changes, accountability and post-action review are expected.
In the context of the CIA triad, this question is focused on system integrity, ensuring that system changes are only executed by authorized users. Additionally, it is expected that devices (for administrators, solution provider staff, and affiliates) that are used to access the solution provider's systems are properly managed and secured.

Reason for Question
Systems that are directly exposed to public internet resources are at greater risk than those that are not. Understanding the requirements for this configuration is important, particularly when assessing compensating controls.
The need for encryption in transport is unique to your institution's implementation of a system. In particular, the data flow between the system and the end users of the solution.
The need for encryption at-rest is unique to your institution's implementation of a system. In particular, system components, architectures, and data flows all factor into the need for this control.
Beware the use of proprietary encryption implementations. Open standard encryption, preferably mature, is often preferred. Although there may be cases in which that is not the case, be sure to understand the solution provider's infrastructure and the true security of a solution provider's solution.

When cancelling a solution, an institution will commonly want all institutional data that was provided to a solution provider. This questions allows the solution provider to state their general practices when a customer leaves their environment.
This question clarifies the position of the institution in the case of acquisition or bankruptcy. Expect clear responses to this question. If they are vague, be sure to follow up based on institutional counsel guidance.
Data exposure is a risk if sensitive data is in any way transported (physically or electronically) into a data zone that is not authorized by the institution. Depending on the criticality of data and institution policy, full control of data confidentiality may be highly valued.
Managing media (and the data within) throughout its lifecycle is crucial to the protection of institutional data. The focus of this question is confidentiality, ensuring that media that may store institutional data is protected by well-established policy and procedure.
When cancelling a solution, an institution will commonly want all institutional data that was provided to a solution provider. This question allows the solution provider to state its general practices when a customer leaves its environment.
When cancelling a solution, an institution will commonly want all institutional data that was provided to a solution provider. The solution provider's response should verify if the institution can extract data or if it is a manual extraction by solution provider staff.
The purpose of this question is to define the scope of backup operations and the scope at which a solution provider may readily recover when backup restoration is required.
When data is moved digitally (e.g., cloud provider, solution provider-owned facility, etc.) off-site, the policies and implemented procedures are important to know. The protections implemented to prevent compromise will be technical in nature and should be well-documented.

When data is moved physically (e.g.,HDD, print, etc.) off-site, the policies and implemented procedures are important to know. Unencrypted data taken outside secured areas introduces unnecessary risks.
The need for encryption at rest (for backups) is unique to your institution's implementation of a system. In particular, system components, architectures, and data flows all factor into the need for this control.
Managing media (and the data within) throughout its lifecycle is crucial to the protection of institutional data. The focus of this question is confidentiality, ensuring that media that may store institutional data is protected by well-established policy and procedure.
Managing media (and the data within) throughout its lifecycle is crucial to the protection of institutional data. The focus of this question is confidentiality, ensuring that media that may store institutional data is protected by well-established policy and procedure.
Confidentiality is the focus of this question. Based on the capabilities of solution provider administrators, the institution may require additional safeguards to protect the confidentiality of data stored by or shared with a solution provider (e.g., additional layer of encryption, etc.).
Telecommuting in the IT world is the norm, and an institution should know that proper safeguards are in place when remote access is allowed. Solution Provider responses vary greatly, so confirm the context of the response if it is not clear. Many cloud services can only be managed remotely, so there is often a gray area to interpret for this response. In the context of the CIA triad, this question is focused on confidentiality. Printed documents, mobile device use, and remote access are all relevant to this question. A solution provider's response to this question will provide insight into their overall business process. Solution Provider business activity that poses additional security risks should be met with increased concern.

A solution provider's response to this question can reveal a system's infrastructure quickly. Off-point responses are common here, so general follow-up is often needed. Understanding how a solution provider segments its customers' data (or doesn't) affects various other controls, including network settings, use of encryption, access controls, etc. A solution provider's response here will influence potential follow-up inquiries for other HECVAT questions.
This question clarifies the operating model of a solution provider and provides insight into the solution provider-customer paradigm of a company. Knowing whether the institution is of value to a solution provider or if the institution's data is of value to a solution provider should weigh heavily in the decision-making process.
This question clarifies the position of the institution in the case of acquisition or bankruptcy. Expect clear responses to this question. If they are vague, be sure to follow up based on institutional counsel guidance.
Restricting system updates to a standard maintenance timeframe is important for ensuring that changes to production systems do not impact operations. It’s also important for troubleshooting any problems that may occur as a result of the changes. Availability is the focus of this question.
Understanding how key management is handled and the safeguards implemented by the solution provider to ensure key confidentiality in all components of a system(s) can provide insight into other complex details of a solution provider's infrastructure. Use solution provider responses to this question as a way to pivot to other infrastructure specifics, as needed to clarify potential risks.
Reason for Question
Understanding the hosting environment may reveal infrastructure risks that may not be apparent by other means and provides context to the responses provided throughout this HECVAT.

This question is relative to the response above. Understanding the ownership structure of the facility that will host institutional data is important for setting availability expectations and ensuring that proper contract terms are in place to protect the institution due to use of third parties. If a solution provider uses a third-party solution provider to provide data center solutions, having that solution provider's SOC 2 Type 2 provides additional insight. The ability to assess these "forth-party" solution providers is based on your institution's resources. The solution provider is responsible for providing this information; ensure that they handle their solution providers properly.
An institution's location will dictate what laws and regulations apply. Because solution providers may not know where all of their customers reside, it is imperative that solution providers are able to accommodate geographic requirements for their customers. Although it is unfair to expect support for all geographic regions in common infrastructure/platform/software-as-a-service, solution providers are expected to be absolutely clear about the regions they leverage and/or support.
Solution Providers that operate their own datacenter(s) can implement their own monitoring strategy. Use the solution provider's response to this questions to verify/validate other responses related to ownership/co-location/physical security.
This question is primarily focused on system integrity. If institutional data is stored in a system that is not physically secured from unauthorized access, the need for compensating controls is often higher. Depending on the use case or solution provider infrastructure, this may not be relevant.
This question is primarily focused on system integrity. If institutional data is stored in a system that is not physically secured from unauthorized access, the need for compensating controls is often higher. Depending on the use case or solution provider infrastructure, this may not be relevant.

When planning for business continuity and disaster recovery, considering geographic diversity of a solution provider's operating environment will help analysts better understand risk due to widespread technical issues as well as weather and environmental considerations.
In the context of the CIA triad, this question is focused on the availability of a system (or set of systems).
In the context of the CIA triad, this question is focused on the availability of a system (or set of systems).
Installing (potential) redundant power and regularly testing strategies to ensure they will work when needed are very different. Vague responses to this question should be met with concern and appropriate follow up, based on your institution's risk tolerance.
Installing appropriate environmental controls is crucial to maintaining the integrity of the hosting site. Vague responses to this question should be met with concern and appropriate follow up, based on your institutions risk tolerance.
In the context of the CIA triad, this question is focused on the availability of a system (or set of systems).
In the context of the CIA triad, this question is focused on the availability of a system (or set of systems).
2FA/MFA, implemented correctly, strengthens the security state of a system. 2FA/MFA is commonly implemented and in many use cases is a requirement for account protection purposes.
In the context of the CIA triad, this question is focused on the integrity of a system (or set of systems).

Understanding how key management is handled and the safeguards implemented by the solution provider to ensure key confidentiality in all components of a system(s) can provide insight into other complex details of a solution provider's infrastructure. Use solution provider responses to this question as a way to pivot to other infrastructure specifics, as needed to clarify potential risks.

Reason for Question

The use case, vendor infrastructure, and types of services offered will greatly affect the need for various firewalling devices. The focus of this question is integrity, ensuring that the systems

In the context of the CIA triad, this question is focused on system integrity, ensuring that system changes are only executed by authorized users. Any change to a verified, known, secure environment should be carefully evaluated by stakeholders in a structured manner.

It is important to have detective capabilities in an information system to protect institutional data. Because this is somewhat expected in information systems, solution providers without IDSs implemented should raise concerns. Compensating controls need future evaluation, if provided by the solution provider.

It is important to have detective capabilities in an information system to protect institutional data. Because this is somewhat expected in information systems, solution providers without IDSs implemented should raise concerns. Compensating controls need future evaluation, if provided by the solution provider.

Strong logging capabilities are vital to the proper management of a network. Implementing an immature system that lacks sufficient logging capabilities exposes an institution to great risk.

Modifications to firewall rule sets can have significant repercussions. To ensure the integrity of the rule set, this question targets the individual (or responsible party) for changes and the reasoning behind their authority.

It is important to have preventive capabilities in an information system to protect institutional data. Because this is somewhat expected in information systems, solution providers without IPSs implemented should raise concerns. Compensating controls need future evaluation, if provided by the solution provider.

It is important to have preventive capabilities in an information system to protect institutional data. Because this is somewhat expected in information systems, solution providers without IPSs implemented should raise concerns. Compensating controls need future evaluation, if provided by the solution provider.
This question is primarily focused on determining the maturity of a solution provider's security program and their ability to implement and operate cutting-edge technologies. Investment in advanced technologies may indicate appropriate security program capabilities.
This question is primarily focused on the capability of a solution provider's security program. Understanding the size and skillsets of a solution provider (taken from other responses) is needed to determine the appropriateness of the solution provider's response to this question.
This question is primarily focused on system(s) integrity. If institutional data is stored in a system that is not physically secured from unauthorized access, the need for compensating controls is often higher. Depending on the use case or solution provider infrastructure, this may not be relevant.

Reason for Question
In the context of the CIA triad, this question is focused on system integrity, ensuring that system changes are only executed according to policy. Additionally, it is expected that devices used to access the solution provider's systems are properly managed and secured.
This is a general inquiry to determine if the solution provider has reviewed the institution's policies and is committed to complying with them.
This is a general inquiry to determine if the solution provider is well-versed in applicable laws and regulations that apply in the institution's region of business operation.

Beware the use of proprietary encryption implementations. Open standard encryption, preferably mature, is often preferred. Although there may be cases in which that is not the case, be sure to understand the solution provider's infrastructure and the true security of a solution provider's solution.
Mature solution lifecycle management can position a solution provider to sufficiently plan, implement, and manage systems that better protect institutional data.
The use of detective and preventive controls in the hiring process serves a valuable role in protecting institutional data. As these are often HR documented policies, a solution provider should have their practices well-documented and ready for review, upon request.
Setting the expectation of performance and increasing awareness of security-related responsibilities are part of these initial-hiring documents. Oftentimes these agreements and reviews are conducted during orientation for new employees.
A shared security [responsibility] environment is expected of solution providers in today's world. Security offices alone cannot protect an institution's data. Information security, ingrained in an organization, is the best case scenario for the protection of institutional data. Security awareness and practice start in a solution provider's policies. The ability for the solution provider to respond effectively (and quickly) to a security incident is of the utmost importance. The size of a solution provider's security office will determine its capabilities during a security incident, but the incident response plan will oftentimes determine its effectiveness. Use the knowledge of this response when evaluating other solution provider statements, particularly when discussing degraded operation states.
The adherence to secure coding best practices better positions a solution provider to maintain the CIA triad. Use the knowledge of this response when evaluating other solution provider statements, particularly those focused on development and the protection of communications.
This is a general inquiry to determine if the solution provider is well-versed in applicable laws and regulations that apply in the institution's region of business operation.

Setting the expectation of security-related responsibilities throughout an organization is favored in an information security awareness program. Solution Providers without an information security awareness campaign should be met with scrutiny on how security policies and procedures are implemented in their environment.
Setting the expectation of security-related responsibilities throughout an organzation is favored in an information security awareness program. Solution Providers without an information security awareness campaign should be met with scrutiny on how security policies and procedures are implemented in their environment.
Protecting privileged accounts is crucial to maintaining system integrity in any environment. This question is targeting privilege creep and unmanaged privileged acccounts to determine if the solution provider properly manages access control in their application/system environments.
The role of an internal auditor is to verify implemented controls and highlight areas in need of improvement. Solution Providers without internal audit processes and procedures should be met with scrutiny on how security policies and procedures are monitored and verified in their environment.
This question aims to understand the physical security state of the solution provider's operating environment and whether or not physical assets are appropriately protected.

Reason for Question
The ability for the solution provider to respond effectively (and quickly) to a security incident is of the utmost importance. The size of a solution provider's security office will determine their capabilities during a security incident, but the incident response plan will oftentimes determine their effectiveness. Use the knowledge of this response when evaluating other solution provider statements, particularly when discussing degraded operation states.
The ability for the solution provider to investigate security incidents is of the utmost importance. Reviewing alerts but then taking no action is not security, only compliance. Incident reports and indications of compromise must be reviewed by qualified staff, and they must have the capability to investigate further, as needed.

The incident team structure (internal vs. external), size, and capabilities of a solution provider have a significant impact on their ability to respond to and protect an institution's data. Use the knowledge of this response when evaluating other solution provider statements.

The capacity for the solution provider to respond effectively (and quickly) to a security incident is of the utmost importance. The size and talent of a solution provider's incident response team will determine their capabilities during a security incident. Use the knowledge of this response when evaluating other solution provider statements, particularly when discussing degraded operation states.

Reason for Question

Modern technologies allow for rapid deployment of features, and with them come changes to an established code environment. The focus of this question is to verify a solution provider's practice

If a solution provider is scanning its applications and/or systems, oftentimes an institution will want to review the report, if possible. Preferably, any finding on the reports will have a matching mitigation action.

Many higher education institutions are capable of performing vulnerability assessments and/or penetration testing on their solution providers' infrastructures. This question confirms the possibility of conducting these actions against the solution provider's infrastructure.

External verification of system and application security controls are important when managing a system. Trust, but verify, is the focus of this question. HECVAT responses are taken at face value and verified within reason, in most cases. When a solution provider can attest to and provide externally provided evidence supporting that attestation, it goes a long way in building trust that the solution provider will appropriately protect institutional data.

The adherence to secure coding best practices better positions a solution provider to maintain the CIA triad. Use the knowledge of this response when evaluating other solution provider statements, particularly those focused on development and the protection of communications. Solution Providers should be monitoring for and addressing these issues in their solutions.

External verification of application security controls is important when managing a system. Trust, but verify, is the focus of this question. HECVAT responses are taken at face value and verified within reason, in most cases. When a solution provider can attest to and provide externally provided evidence supporting that attestation, it goes a long way in building trust that the solution provider will appropriately protect institutional data.

Reason for Question
HIPAA
HIPAA
HIPAA
HIPAA
HIPAA
HIPAA
HIPAA
HIPAA
HIPAA
HIPAA

HIPAA
HIPAA
HIPAA
HIPAA
HIPAA
HIPAA
HIPAA
HIPAA
HIPAA
HIPAA
HIPAA
HIPAA
HIPAA
HIPAA

HIPAA
HIPAA
HIPAA
HIPAA
HIPAA

Reason for Question
PCI DSS
PCI DSS
PCI DSS
PCI DSS
PCI DSS
PCI DSS
PCI DSS
PCI DSS
PCI DSS
PCI DSS

PCI DSS
PCI DSS

Reason for Question
Managing a solution may rely on various professionals to administer a system. This question is focused on how administration, and the segregation of functions, can be implemented within the system. Securing the administration portion of a system has additional implications (e.g., logging, administration, etc.) beyond that of end users.
Telecommuting in the IT world is common. An institution should know that proper safeguards are in place if remote access is allowed. Solution Provider responses vary greatly on this, so confirm the context of the response if it is not clear. Many cloud services can only be managed remotely, so there is often a gray area to interpret for this response.
Many systems can be used a variety of ways. We want these implementation type diagrams so that we can understand the "real" use of the solution.
Telecommuting in the IT world is common. An institution should know that proper safeguards are in place, if remote access is allowed. Solution Provider responses vary greatly on this, so confirm the context of the response if it is not clear. Many cloud services can only be managed remotely, so there is often a gray area to interpret for this response.
Strong logging capabilities are vital to the proper management of a system. Implementing an immature system that lacks sufficient logging capabilities exposes an institution to great risk. Depending on your risk tolerance and the use case, your institution may or may not be concerned. The focus of this question is remote access logging.
This is standard documentation, relevant to institution implementations requiring FERPA compliance.

Standard documentation question. With an on-premise device, the possibility to tie-in with existing monitoring/management systems is beneficial. The solution provider's response should be clear and concise.

This question is primarily focused on system(s) integrity and confidentiality. The solution provider's response should clearly state the system(s) capabilities to properly monitor for (and alert for) malicious activity.

We want to establish longevity of a solution and whether or not a solution provider is new to the higher education space.

Higher education is a unique vertical. A solution provider's response to this question can help an analyst set the context for all solution provider responses. Established and/or mature solutions are more likely to have current higher education customers, and therefore understand the environment that we operate in.

Reason for Question

To be added in a later version

Reason for Question

To be added in a later version