

Biosecurity Evaluation Questionnaire

Welcome

Under the leadership of Vincent Cervone, of Purple Raven Cybersecurity, and Jess Smith, PhD, of Pacific Northwest National Laboratory, the Hardware and Software Security Working Group at BIO-ISAC published **Fortifying the Bioeconomy**, an in-depth resource about shared responsibility in hardware and software lifecycle management within the bioeconomy.

Featured in this report is this resource, the **Biosecurity Evaluation Questionnaire**, or BSEQ. The BSEQ is designed to complement the objectives of the report and provide a tool to walk decision makers through a safer, more defined, equipment acquisition process, with a focus on building stronger expectations from manufacturers and firms when it comes to instrument security.

BIO-ISAC, together with its members and workgroup leadership, will continue to release the tools, materials, and resources shaping the conversations around secure, safe advancement of discovery, development, and delivery in the bioeconomy.

BSEQ Guidance

This questionnaire is broken into categories that pertain to Organizational Security, General Product Security, Software Development Lifecycle (SDLC), and targeted questions based on the hosting location of a product or service.

This questionnaire provides the ability to:

1. As an **Asset Owner**, evaluate the security practices utilized by an Original Equipment Manufacturer (OEM) to secure their organization and for creating and maintaining an asset.
2. As an **Original Equipment Manufacturer**, evaluate your internal security practices utilized to secure your organization and for creating and maintaining a secure asset.

Systems lacking functionality or hardware to connect to a corporate network would not be in scope for this document, but should always follow secure coding practices and have vulnerability management procedures in place. This structure is intended to reduce inapplicable questions. While the questionnaire only asks yes or no responses, it will require an in-depth understanding of a product, the associated development lifecycles, and general security controls within your organization. In most organizations, the stakeholders completing this document would be your application development, security, and SDLC infrastructure teams.

Instructions for Use


Step 1. Select the **Categories** and **Tiering Level** that apply for the asset in scope.

 **Tip** Questions may be required for all, or several, tiers. Follow the coded key in the corner of each response field.


Step 2. Complete the questionnaire sections for Organizational Security, General Product Security, and Software Development Lifecycle (SDLC) sections and the Categories that apply to the asset in scope.

SDLCB: Are user activity logs from your source code repository sent to your organizational SIEM for security monitoring?

Comments	M
Consensus Response	H

 **Tip** Only complete questions that align to the Tiering Level you selected in Step 1. Example: This question would be for Medium and High Tiers.

Step 3. Questions are most often written in a format where "Yes" or "No" is the expected response. If "Yes" was selected then your control is in good standing. Where "No" has been selected, teams should document the risk and a remediation plan should be created. Unique circumstances do exist and the asset or organization may have other compensating controls causing the question to not apply.

 **Tip** If you are not able to answer "Yes" or "No" to a particular question, it is most likely signaling that the team needs to establish or define its own specific organizational risk tolerance before answering the question.

Once the BSEQ is completed, review your risk tolerance regarding the project and the responses collected and determine the appropriate next steps for information, acquisition, or revised workflows.

Questionnaire Categories: Choose all that apply.

Evaluate the asset and its placement or role in the following Categories. The team should answer the questions in each of the related Categories. In most cases, all teams will need to review all questions in Organizational Security, General Product Security, and the Software Development Lifecycle.

- Organizational Security:** The generalized people, processes, and technologies that apply to your entire enterprise.
- General Product Security:** The product in scope regardless of hosting location & components.
- Software Development Lifecycle (SDLC):** The controls utilized within your software development lifecycle and associated tooling (source code repository, secrets manager, etc.)
- Asset Owner Hosted - Single-Tier Application Security:** A product which is hosted by an Asset Owner in a manner where the backend logic, database, and user interface lies in the same machine. This will describe the minimum security controls and functionality that should be within the application.
- Asset Owner Hosted- Multi-Tier Application Security:** A product which is hosted by an Asset Owner in a manner the system is split into multiple pieces and/or machines. This commonly includes a database server that is separate from the application server and so on. This will describe the minimum security controls and functionality that should be within the application.
- Programmable Logic Controller (PLC) Security:** The security requirements that should be utilized within a PLC that is part of a system.
- Human-Machine Interface (HMI) Security:** The security requirements that should be utilized with an HMI that is part of a system.
- Desktop Computer Security:** The security requirements that should be utilized with a desktop computer that's part of a system. This will vary on who is providing the PC and what modifications are supported without voiding a warranty.
- System Network Security:** The controls which should be in place on networking devices as part of a system. This is intended to address packaged systems.
- Cloud Application Security:** The security controls that should be in place for Software-as-a-Service (SaaS) within the cloud environment as well as functionality offered within the application.

Tiering Level: Choose the option of best fit.

Evaluate the ways by which the asset requires or connects to the public internet. Inside the matched, selected Categories, the team should answer the questions marked for the selected tiering level.

LOW: The system supports connections to a corporate network and does not require the public internet.

MEDIUM: The system supports connections to a corporate network and requires connections to the public internet.

HIGH: The system is used for regulated purposes (GxP, etc.), supports connections to a corporate network, and requires connections to the public internet.

This document provides references to tools and solutions that can support an entity achieving certain security protections. These protections do not eliminate all cybersecurity or compliance risk. If a tool or solution is chosen from the results of this document, it remains the entity's responsibility to ensure such tool or solution complies with their regulatory requirements.

VENDOR REVIEW & INTERNAL REVIEW

Section 1: Organizational Security (OS)

OS1: Does the organization have a formal Information Protection and Cyber Security Program?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS2: Does the organization have an Information Security and Privacy Policy?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS3: Does the organization have a Vulnerability Management policy?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS4: Are all of your Information Protection and Cyber Security policies reviewed and approved by leadership every 12 months?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS5: Do all your Employees, Third Party Workers, including Vendors, Contractors and Consultants undergo training on your Information Protection and Cyber Security policies?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS5.1: Do you have a programmatic inventory process that tracks the onboarding and offboarding of all staff types?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS6: Are user accounts disabled within 12 hours of a user resignation or termination? Please provide timelines.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS7: Does the organization have a formal cyber security risk management process?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS7.1: Are cyber security risk assessments performed at least annually?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS8: Does the organization perform scheduled security reviews on essential third parties that support the solution/services? Examples of essential third parties include: Cloud or Data Hosting providers & Software/hardware providers.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS9: Do you have an Identity and Access Management solution to manage internal user access?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS10: Are identities/credentials audited, provisioned and deprovisioned for authorized individuals, processes, and devices at least quarterly?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS11: Does the organization follow a least privileged approach when creating access for all users and machine-to-machine communications (APIs, Service Accounts, etc.)?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS12: Is Multi-factor authentication (MFA) enabled for all users accessing organizational resources remotely?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS12.1: Do you utilize a push button or physical access key for the secondary form of authentication?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS13: Does you have an organizational password policy that meets or exceeds NIST recommendations?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS14: Does the organization provide staff with a commercial grade password manager?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS15: Does the organization have a formal information security awareness and training program?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS15.1: Are quarterly phishing simulations performed?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS16: Does the organization have Business Email Compromise Protection?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS17: Does the organization have a process to classify data based on data type, sensitivity and criticality?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS18: If a corporate/enterprise network exists, are firewalls used to protect the network?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS18.1: Are firewall rules reviewed or least privileged on an annual basis?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS18.2: Are firewall rules set to deny by default and allow explicitly required network communications traffic?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS18.3: Are any-any rules explicitly prohibited?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS19: Does the organization utilize a commercial grade Anti-virus(AV)/Anti-malware(AM) solutions on all workstations and servers?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS20: Does the organization have a Security Information and Event Management (SIEM) solution?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS20.1: Are rules built to ensure anomalies trigger notification to relevant personnel?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS20.2: Is a programmatic solution in place which continuously escalates (Email, SMS, phone call, etc.) alerts until human intervention?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS21: Do you aggregate syslog, security event logs, and other relevant logs from all organizational assets (workstations, servers, network devices, domain controllers, etc.) in a SIEM for security monitoring?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS22: Does the organization retain logs for at least two (2) years?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS23: Does the organization perform vulnerability scans on infrastructure facing the public internet?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS24: Does the organization have an approved Incident Response (IR) Team/Plan/Procedure?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS26: Does the organization have cyber security insurance? (Provide details.)

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS27: Has the organization had a security breach in the last 3 years?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS28: Does the organization have a formal Business Continuity (BCP) and Disaster Recovery Plan (DRP)?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS28.1: Are the BCP and DRP tested at least annually?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS28.2: When was the last BCP/DR test performed?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS29: Does your organization use technical controls to block the use of removable media on corporate owned workstations?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS30: Does your organization remove admin rights to corporate workstations (laptops, desktops, etc.) for all staff?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

OS31: Are all operating system images for corporate workstations (laptops, desktops, etc.) using security hardened images? Examples may include CIS or STIG images

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

Section 2: General Product Security (GPS)

GPS1: Do you have an updated software build of materials for the application/system(s) in scope (SBOM)? If yes, please attach.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

GPS2: Is the product covered under any security certifications held by your organization? If yes, please attach.

Certifications held by a Cloud Service Provider (CSP) should not be used to respond to this question.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

Section 3: Software Development Lifecycle (SDLC)

SDLC1: Does the organization have a defined change management process?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SDLC2: Does your Source Code Repository require Single Sign-on and Multi-Factor Authentication (MFA) for access via the GUI?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SDLC3: Does your Source Code Repository require Single Sign-on and Multi-Factor Authentication (MFA) for access via CLI?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SDLC4: Do you perform secure code scanning?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SDLC4.1: Does your organization perform Static Application Security Testing (SAST) scans before promoting code to production?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SDLC4.2: Does your organization perform Software Composition Analysis (SCA) scans before promoting code to production?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SDLC4.3: Web Applications Only: Does your organization perform Dynamic Application Security Testing (DAST) scans before promoting code to production?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SDLC4.4: Is the entire code base scanned for before each release?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SDLC5: Do you have a policy which does not permit High or Critical vulnerabilities to be released to production without mitigations or remediation?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SDLC6: Do you receive notifications for new vulnerabilities that impact your proprietary and open source code that require investigation?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SDLC7: Do you use a trusted Certificate Authority (CA) to sign your code prior to release?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SDLC8: Are user activity logs from your source code repository sent to your organizational SIEM for security monitoring?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SDLC9: Are technical data input and output integrity routines implemented for application interfaces and databases to prevent manual or systematic processing error, corruption of data, or injection attacks (SQL, OS, etc.)?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SDLC10: Do you utilize a commercial grade secrets management solution?

Secrets would include SSH keys, API tokens, TLS certificates, etc.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SDLC11: Are application secrets programmatically rotated? If Yes, how often?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SDLC12: Are credentials hardcoded in source code?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SDLC12.1: If credentials are hard coded, do you encrypt hard coded credentials?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SDLC12.2: If credentials are hardcoded, do you use environmental variables to retrieve credentials?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SDLC13: Do you have secrets detection scanning enabled within your source code repository to detect hard coded secrets?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SDLC14: Are developers required to take secure code training?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SDLC15: Do you prevent the utilization of protocols with known, unresolvable, vulnerabilities? (Ex. SMBv1, TLS 1.0, SNMPv1, etc.)

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

Section 4: Asset Owner Hosted – Single-Tier Application Security (STAS)

STAS1: Does the application and/or instrument have a deployment manual? If yes, please attach.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

STAS2: Does this application or equipment **require** connection to the internet? If yes, please explain why a connection to the internet is required

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

STAS3: Does your product application support user specific accounts?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

STAS4: Can any default passwords be rotated?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

STAS5: Does the application have technical controls to enforce the complex passphrase requirements below?

1. Passphrases shall be at least 12 characters in length.
2. Passphrases shall contain 3 of the 4 character types:
3. Uppercase letters (e.g., A-Z)
4. Lowercase letters (e.g., a-z)
5. Numbers (e.g., 0-9)
6. Special Characters (e.g., !,*,@,#)
7. Passphrases shall be unique and shall not be reused for multiple systems, with the exception of Single Sign-on (SSO) support.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

STAS6: Does the product allow for limitations to be set on unsuccessful login attempts?

Note: Software Enabled Solutions must enforce account lockouts after 5 invalid/failed login attempts

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

STAS7: Does your product salt + hash passwords before transfer and/or storage?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

STAS8: Does the application/service support Single Sign-On (SSO)?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

STAS8.1: Does the protocol used to support SSO prevent transmissions of credentials in clear text? For example, LDAP (port 389) does not encrypt credentials, LDAPS (port 636) does.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

STAS9: Does the application and/or instrument have embedded remote access functionality?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

STAS10: If SMB functionality exists within the product, does it support the use of Server Message Block (SMB) with less than version 3.0?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

STAS11: Does the product have logic which prevents logs from collecting sensitive data? For example: PII, PHI, Passwords, etc.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

STAS12: Are files within the application package that contain credentials supporting product functionality stored with technical controls that prevent viewing and tampering?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

Section 5: Asset Owner Hosted – Multi-Tier Application Security (SMAS)

SMAS1: Does the application and/or instrument have a deployment manual? If yes, please attach.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS2: Can you provide Application Architecture for the solution in scope? If yes, please attach

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS3: Does this application or equipment **require** connection to the internet? If yes, please explain why a connection to the internet is required

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS4: Does your product/application support user specific accounts?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS5: Does your product/application support different levels of authorization (permissions) for different roles?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS6: Can default passwords be rotated?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS7: Does the application have technical controls to enforce the complex passphrase requirements below?

1. Passphrases shall be at least 12 characters in length.
2. Passphrases shall contain 3 of the 4 character types:
3. Uppercase letters (e.g., A-Z)
4. Lowercase letters (e.g., a-z)
5. Numbers (e.g., 0-9)
6. Special Characters (e.g., !,*,@,#)
7. Passphrases shall be unique and shall not be reused for multiple systems, with the exception of Single Sign-on (SSO) support.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS8: Does the product allow for limitations to be set on unsuccessful login attempts?

Note: Software Enabled Solutions must enforce account lockouts after 5 invalid/failed login attempts

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS9: Does your product salt + hash user passwords with non-vulnerable hashing algorithms before transfer and/or storage?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS10: Does your product encrypt service account passwords?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS11: Does the application/service support Single Sign-On?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS11.1: Does the protocol used to support SSO prevent transmissions of credentials in clear text? For example, LDAP (port 389) does not encrypt credentials, LDAPS (port 636) does.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS12: Is encryption at rest supported? If yes, where can encryption be applied that is supported by the system? (Disk, File, Database, Table, Column, Field etc.)

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS13: Does this system use or support at least AES 256 for encryption at rest?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS14: Does the product have logic which prevents logs from collecting sensitive data? For example: PII, PHI, Passwords, etc.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS15: Are application logs encrypted in transit and at rest by default?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS16: Are logs stored with technical controls that prevent tampering?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS17: Is the system tested against the OWASP Top 10 for security control effectiveness?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS18: If SMB functionality exists within the product, does it support the use of Server Message Protocol (SMB) with less than version 3.0?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS19: Does the organization perform Penetration Tests on the network and the application(s) in scope at least annually?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS19.1: Provide a summary report of the latest Penetration Test Results.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS19.2: Have all the critical and high issues identified in the results above, been remediated?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS19.3: Has a retest been performed to validate successful remediation?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SMAS20: Does the application and/or instrument have embedded remote access functionality?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

Section 6: Programmable Logic Controller Security (PLC)

PLC1: Are any PLCs included with your product running the latest firmware provided by the OEM?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

PLC2: Do all PLCs utilize the Top 20 Secure PLC Coding Practices? <https://plc-security.com>

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

Section 7: Human-Machine Interface Security (HMI)

HMI1: What Operating System (OS) is installed on the HMI(s)?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

HMI1.1: Is the installed OS still receiving security updates from the OEM?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

HMI2: Can all default passwords be rotated?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

HMI3: Does the HMI have technical controls to enforce the complex passphrase requirements below?

1. Passphrases shall be at least 12 characters in length.
2. Passphrases shall contain 3 of the 4 character types:
3. Uppercase letters (e.g., A-Z)
4. Lowercase letters (e.g., a-z)
5. Numbers (e.g., 0-9)
6. Special Characters (e.g., !,*,@,#)
7. Passphrases shall be unique and shall not be reused for multiple systems, with the exception of Single Sign-on (SSO) support.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

HMI4: Does the HMI allow for limitations to be set on unsuccessful login attempts?

Note: Software Enabled Solutions must enforce account lockouts after 5 invalid/failed login attempts

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

HMI5: Does the HMI's OS utilize secure boot?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

HMI6: Has the HMI OS undergone security hardening? Examples may include CIS or STIG policies

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

Section 8: Desktop Computer Security (DCS)

DCS1: What Operating System (OS) is installed on the desktop computer?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

DCS2: Is the installed OS still receiving security updates from the OEM?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

DCS3: Can all default passwords be rotated?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

DCS4: Does the computer have technical controls to enforce the complex passphrase requirements below?

1. Passphrases shall be at least 12 characters in length.
2. Passphrases shall contain 3 of the 4 character types:
3. Uppercase letters (e.g., A-Z)
4. Lowercase letters (e.g., a-z)
5. Numbers (e.g., 0-9)
6. Special Characters (e.g., !,*,@,#)
7. Passphrases shall be unique and shall not be reused for multiple systems, with the exception of Single Sign-on (SSO) support.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

DCS5: Does the HMI allow for limitations to be set on unsuccessful login attempts?

Note: Software Enabled Solutions must enforce account lockouts after 5 invalid/failed login attempts.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

DCS6: Does the instrument utilize secure boot?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

DCS7: Has the HMI OS undergone security hardening? Examples may include CIS or STIG policies

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

Section 9: System Network Security (SNS)

SNS1: For products with multiple components (HMI, PLC, etc.) do they communicate with a managed switch?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SNS1.1: For access to the switch is the user ID and password unique to each client?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SNS2: Does the switch come with the latest Operating System & Firmware release from the OEM?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SNS3: Are unused ports administratively disabled by default?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

SNS4: Are patches provided for networking components within the product?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

Section 10: Cloud Application Security (CAS)

CAS1: Can you provide Application Architecture for the solution in scope? If yes, please attach.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS2: Is the application setup as a single tenant or multi-tenant?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS3: Is your Cloud Service Provider (CSP) root account separate from day-to-day functions?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS4: Does your CSP root account require MFA?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS4.1: If multi-tenant, does the application use a dedicated or shared database?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS5: Does your product support user specific accounts?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS6: Can any default passwords be rotated?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS7: Does the application have technical controls to enforce the complex passphrase requirements below?

1. Passphrases shall be at least 12 characters in length.
2. Passphrases shall contain 3 of the 4 character types:
3. Uppercase letters (e.g., A-Z)
4. Lowercase letters (e.g., a-z)
5. Numbers (e.g., 0-9)
6. Special Characters (e.g., !,*,@,#)
7. Passphrases shall be unique and shall not be reused for multiple systems, with the exception of Single Sign-on (SSO) support.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS8: Does the application/service support Single Sign-On?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS9: Is encryption at rest supported? If yes, where can encryption be applied that is supported by the system? (Disk, File, Database, Table, Column, Field etc.)

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS10: Are encryption keys rotated at least every two years?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS10.1: Are encryption keys managed programmatically?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS11: Does the application have end-to-end encryption in transit for all data and logs with TLS 1.2 or greater?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS11.1: Do you prevent the use of downward negotiations? (Utilization of TLS 1.0, 1.1, etc.)

Example: If a client browser defaults to TLS 1.0 or 1.1, the server should refuse the connections requesting TLS 1.0 or 1.1 if configured correctly.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS12: Have you deployed HTTP Strict Transport Security (HSTS) on all servers in scope?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS13: Does each service within the application utilize a unique identity that is not shared?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS14: Do service identities require authentication and authorization with each call?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS15: If containers are utilized, are they running with least privilege? i.e. not root.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS16: If connecting to a product at a client location (benchtop lab equipment, etc.), are technical controls in place to prevent spoofing that would allow unauthorized communications with the cloud environment?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS17: Are your backups encrypted?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS18: Are backups performed with dedicated credentials?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS19: Do your backups use different encryption keys than production environments?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS20: Does your product salt + hash passwords with non-vulnerable hashing algorithms before transfer and/or storage?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS21: Are all operating system images for cloud infrastructure using security hardened images?

Examples may include CIS or STIG images

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS22: Does the organization prevent production data from being used in non-production environments (dev, test, etc.)?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS23: Are all uploads/attachments scanned for viruses?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS24: Does the application have a Web Application Firewall (WAF)?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS25: Is programmatic exportation of company application level logs supported? (API, S3 Bucket replication, etc.) Examples: User activity with the company application instance. NOT host logs or log information pertaining to other clients

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS26: Do application logs contain sensitive data? Sensitive Data: PII, PHI, Passwords, Secrets, etc.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS27: Does the organization have a technical solution in production environments to monitor for configuration drift? Ex. AWS Config, Prisma, etc.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS28: Can clients perform penetration testing on the application/system?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS29: Does the application have at least two availability zone (data centers) failovers?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS30: Does the application have multi geographical failover?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS31: Do you use auto scaling tools to scale your application under periods of high load?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS32: Are backups performed automatically?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS32.1: How frequently is data backed up for the systems in scope?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS32.2: Do you test and restore your backups annually?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS33: Are recovery processes fully automated?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS34: Does the organization isolate Backups from the production environment?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS35: What is your service availability rating? (99.XXX%)

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS35.1: What is your Recovery Point Objective (RPO)? RPO is your goal for the maximum amount of data the organization can tolerate losing.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS35.2: What is your Recovery Time Objective (RTO)? RTO is the goal your organization sets for the maximum length of time it should take to restore normal operations following an outage or data loss.

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	

CAS36: Can data be returned in a usable format within 10 business days?

<i>Comments</i>	L
	M
	H
<i>Consensus Response</i>	