

# Sogei Societa' Generale D'informatica Spa E In Forma Abbreviato Sogei Spa

## Cyber Self-Assessment Response Documentation



# Contents

1.	Demographics .....	1
2.	Governance .....	3
3.	Data Protection .....	7
4.	Inventory and Control of Enterprise Assets .....	12
5.	Inventory and Control of Software Assets .....	14
6.	Secure Configuration of Enterprise Assets and Software ..	16
7.	Audit Log Management .....	18
8.	Network Monitoring and Defense .....	20
9.	Account Management .....	22
10.	Access Control Management .....	26
11.	Network Infrastructure Management .....	30
12.	Malware Defenses .....	32
13.	Continuous Vulnerability Management .....	34
14.	Security Awareness and Skills Training .....	36
15.	Data Recovery .....	38
16.	Service Provider Management .....	40
17.	Incident Response Management .....	42
18.	Technology in Use .....	46
19.	Event History .....	48
20.	Biometric Information .....	50
21.	HIPAA .....	51
22.	PCI .....	52
23.	Trending Topics .....	53
24.	External Partner Accompaniments .....	55

25.	Media .....	77
26.	Tech Errors and Omissions .....	79
27.	Operational Technology .....	85

## Demographics

#	Prompt	Response
<b>Basic Data</b>		
1.1.1	Firm Name	Sogei SPA
1.1.2	Address	via Mario Caruci 99, Roma
1.1.3	Country	Italy
1.1.4	Primary Website(s)	www.sogei.it
<b>Contact Information</b>		
1.2.1	Primary Contact Name	
1.2.2	Primary Contact Title	
1.2.3	Primary Contact Role	
1.2.4	Primary Contact Email	
1.2.5	Primary Contact Phone	
<b>ID Numbers</b>		
1.3.1	Ticker Symbol	
1.3.2	DUNS Number	
<b>Basic Demographics</b>		
1.4.1	Currency for all monetary responses.	
1.4.2	Revenue - Most Recent FY	
1.4.3	Employee Count (approx.)	
1.4.4	Primary Industry (NAICS Code <a href="#">Look up</a> )	
1.4.5	Secondary Industry (NAICS Code <a href="#">Look up</a> )	
1.4.6	Tertiary Industry (NAICS Code <a href="#">Look up</a> )	
1.4.7	Please select geographies and indicate your organization's revenue allocation.	

Sum of Revenue

1.4.8 Please select geographies and indicate your organization's employees allocation.

Total Employee Count

## Governance

#	Prompt	Response
<b>Security Organization</b>		
2.1.1	Please provide an overview of the organization's information/cybersecurity structure:	nell'ambito dell'organizzazione in materia di sicurezza delle informazioni /cybersicurezza le responsabilità sono suddivise tra due aree aziendali:SGD che assicura la governance della security e data protectionCYS che assicura la corretta implementazione dei presidi tecnologici di sicurezza
2.1.2	Overall Information Technology Budget (most recent FY)	544,892,782
2.1.3	Percentage of your IT budget allocated to information/cybersecurity (approx.).	7
2.1.4	Overall Information/Cybersecurity Budget (most recent FY)	40,662,933
2.1.5	Our information/cybersecurity organization is: <ul style="list-style-type: none"> <li>• Centralized (e.g. There is a centralized information/cybersecurity function which oversees all business units)</li> <li>• Decentralized (e.g. Business units are individually responsible for information /cybersecurity functions)</li> <li>• Federated/Hybrid (e.g. Business units have day-to-day management control, but there are centralized information/cybersecurity policies and standards)</li> </ul>	Yes
<b>Security Officers</b>		
2.2.1	The organization has a Chief Information Security Officer (CISO), Chief Security Officer (CSO) or functional equivalent. (If yes, please provide name in additional commentary) [ Yes , No ] <i>Comment</i>	No  <i>seppur non formalizzato il ruolo, in termini di responsabilità assegnate, è ricoperto dal responsabile dell'Area SGD</i>

2.2.4	The organization manages cyber/information security risks by: <i>(check all that apply)</i> .	
	<ul style="list-style-type: none"> <li>• Performing a cybersecurity risk assessment at least annually to identify risks, analyze risks, assess likelihood, assess impact, prioritize risks, plan response strategies, and monitor, evaluate, and adjust.</li> </ul>	Yes
	<ul style="list-style-type: none"> <li>• Documenting the results of the annual cybersecurity risk assessment/management in a report that includes prioritized risk response actions including accept, transfer, mitigate, or avoid.</li> </ul>	Yes
	<ul style="list-style-type: none"> <li>• Presenting the Cybersecurity Risk Assessment Report to the Board, or equivalent at least annually.</li> </ul>	Yes
2.2.5	<p>The organization has a Chief Privacy Officer (CPO) or a functional equivalent. (if yes, please provide name in additional commentary)</p> <p>[ Yes , No ]</p>	Yes

### Security Policies and Standards

2.3.1	The organization documents and implements enterprise or company-wide policies/programs (select all that apply):	
	<ul style="list-style-type: none"> <li>• Cyber / Information Security Policy.</li> </ul>	Yes
	<ul style="list-style-type: none"> <li>• Acceptable Use Policy (AUP) that defines for all parties the ranges of permitted use of organizationally-provided technologies; contains consequences for noncompliance /violation of the AUP.</li> </ul>	Yes
	<ul style="list-style-type: none"> <li>• Users are disallowed from surfing social media platforms from organizational assets except where this is a defined business need.</li> </ul>	
	<ul style="list-style-type: none"> <li>• Insider Threat Program coordinated capabilities to deter, detect, and mitigate insider threats.</li> </ul>	Yes

2.3.2	<p>The following cybersecurity standards, frameworks, or best practices are leveraged by the organization:</p> <ul style="list-style-type: none"> <li>• ISO/IEC 27001 'Information Security Management System (ISMS)'</li> <li>• NIST Special Publications aimed at computer /cyber/information security</li> <li>• Center for Internet Security 'Critical Security Controls'</li> <li>• ISACA 'COBIT'</li> <li>• FFIEC 'Cybersecurity Assessment Tools'</li> <li>• NIST Cybersecurity Framework (NIST CSF)</li> <li>• PCI-DSS</li> <li>• HIPAA Security</li> <li>• Information Security Forum (ISF), Standard of Good Practice for Information Security</li> <li>• Others (please describe below):</li> </ul>	<p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p>
2.3.3	<p>The organization has documented enterprise or company-wide Privacy Policies (please note policy titles, the version, and date released)</p> <p>[ Yes , No ]</p>	Yes
2.3.4	<p>The organization implements a physical security program with risk-based protections (e.g., CCTV, visitor access controls, badge access, and alarms for the perimeter) to secure offices and data center facilities.</p> <p>[ Yes , No ]</p>	Yes
2.3.5	<p>Our screening and background check requires background verification checks including criminal records, credit history, education and reference checks, and employment history as permitted by law. <i>(please check all that apply).</i></p> <ul style="list-style-type: none"> <li>• Employees</li> <li>• Contractors/ Consultants</li> </ul>	Yes

#### Independent Audit / Assessment



---

2.4.1	The organization engages with an independent service provider to: a) conduct an assessment of our information /cybersecurity program and associated controls. b) prepare and deliver a report that documents the results of the assessment and recommendations for improvement.	Yes
-------	---	-----

[ Yes , No ]

2.4.2	Our internal Audit department conducts risk-based audits or assessments of the information/cybersecurity program and associated controls on an annual or more frequent basis.	No
-------	---	----

[ Yes , No ]

*Comment*

*l'audit di sicurezza viene effettuato dalla struttura preposta alla governance della sicurezza delle informazioni*

## Data Protection

#	Prompt	Response
<b>Records</b>		
3.1.1	Number of <b>records in the custody</b> of the organization by PCI (Payment Card Industry /Information).	0
3.1.2	The PCI Information provided above is an estimation? [ Yes , No ]	No
3.1.3	Number of <b>records in the custody</b> of the organization by PHI (Protected Health Information) / Sensitive Personal Data.	61,000,000
3.1.4	The PHI Information provided above is an estimation? [ Yes , No ] <i>Comment</i>	Yes  <i>Si è una stima. Sogei rappresenta un' unicum nel panorama delle imprese attive nell'ambito dell'Information Technology, in quanto partner tecnologico unico del MEF, operante all' interno di un quadro di riferimento ampio, e in continua evoluzione, pertanto si ritiene che la sua valutazione in termini di esposizione al rischio possa essere validamente perfezionata in base alle informazioni reperibili dal sito istituzionale <a href="http://www.sogei.it">www.sogei.it</a></i>
3.1.5	Number of <b>records in the custody</b> of the organization by PII (Personally Identifiable Information) / Personal Data.	61,000,000

3.1.6	<p>The PII Information provided above is an estimation? [ Yes , No ]</p> <p><i>Comment</i></p>	<p>Yes</p> <p><i>Si è una stima. Sogei rappresenta un' unicum nel panorama delle imprese attive nell'ambito dell'Information Technology, in quanto partner tecnologico unico del MEF, operante all' interno di un quadro di riferimento ampio, e in continua evoluzione, pertanto si ritiene che la sua valutazione in termini di esposizione al rischio possa essere validamente perfezionata in base alle informazioni reperibili dal sito istituzionale <a href="http://www.sogei.it">www.sogei.it</a></i></p>
3.1.7	<p>Number of <b>records processed and/or transacted</b> by the organization annually by PCI (Payment Card Industry/Information).</p>	<p>0</p>
3.1.8	<p>The PCI Information provided above is an estimation? [ Yes , No ]</p>	<p>Yes</p>
3.1.9	<p>Number of <b>records processed and/or transacted</b> by the organization annually by PHI (Protected Health Information) / Sensitive Personal Data.</p> <p><i>Comment</i></p>	<p>61,000,000</p> <p><i>N.A. Sogei rappresenta un'unicum nel panorama delle imprese attive nell' ambito dell'Information Technology, in quanto partner tecnologico unico del MEF, operante all'interno di un quadro di riferimento ampio, e in continua evoluzione, pertanto si ritiene che la sua valutazione in termini di esposizione al rischio possa essere validamente perfezionata in base alle informazioni reperibili dal sito istituzionale <a href="http://www.sogei.it">www.sogei.it</a></i></p>

3.1.10	<p>The PHI Information provided above is an estimation? [ Yes , No ]</p> <p><i>Comment</i></p>	<p>Yes</p> <p><i>N.A. Sogei rappresenta un'unicum nel panorama delle imprese attive nell'ambito dell'Information Technology, in quanto partner tecnologico unico del MEF, operante all'interno di un quadro di riferimento ampio, e in continua evoluzione, pertanto si ritiene che la sua valutazione in termini di esposizione al rischio possa essere validamente perfezionata in base alle informazioni reperibili dal sito istituzionale <a href="http://www.sogei.it">www.sogei.it</a></i></p>
3.1.11	<p>Number of <b>records processed and/or transacted</b> by the organization annually by PII (Personally Identifiable Information) / Personal Data.</p> <p><i>Comment</i></p>	<p>61,000,000</p> <p><i>N.A. Sogei rappresenta un'unicum nel panorama delle imprese attive nell'ambito dell'Information Technology, in quanto partner tecnologico unico del MEF, operante all'interno di un quadro di riferimento ampio, e in continua evoluzione, pertanto si ritiene che la sua valutazione in termini di esposizione al rischio possa essere validamente perfezionata in base alle informazioni reperibili dal sito istituzionale <a href="http://www.sogei.it">www.sogei.it</a></i></p>
3.1.12	<p>The PII Information provided above is an estimation? [ Yes , No ]</p> <p><i>Comment</i></p>	<p>Yes</p> <p><i>N.A. Sogei rappresenta un'unicum nel panorama delle imprese attive nell'ambito dell'Information Technology, in quanto partner tecnologico unico del MEF, operante all'interno di un quadro di riferimento ampio, e in continua evoluzione, pertanto si ritiene che la sua valutazione in termini di esposizione al rischio possa essere validamente perfezionata in base alle informazioni reperibili dal sito istituzionale <a href="http://www.sogei.it">www.sogei.it</a></i></p>

3.2.1	<p>The organization regularly handles or processes information owned by other organizations, unrelated companies, or external customers (<i>please check all that apply</i>).</p> <ul style="list-style-type: none"> <li>• Personally Identifiable Information (PII) Yes</li> <li>• Protected Health Information (PHI) Yes</li> <li>• Intellectual Property/Trade Secrets/Marked Confidential Information Yes</li> <li>• Sales/Business Projections</li> <li>• Merger &amp; Acquisition/Business Development</li> <li>• Insider Financial Information (e.g., non-public information related to a publically traded company's earnings, forecasts, and acquisition and divestiture plans) Yes</li> <li>• Product Development / Research &amp; Development Yes</li> <li>• Advertising / Marketing / Product Roadmaps</li> <li>• Government Classified Data Yes</li> <li>• Other (please describe below):</li> </ul>	
3.2.2	<p>We encrypt account usernames and authentication credentials during transmission over an IT network (i.e., we do not permit clear text usernames and authentication credentials across networks).</p> <p>[ Yes , No ]</p>	Yes
3.2.3	<p>The organization utilizes mandatory encryption to protect critical information and other sensitive information (e.g., PII, PHI, etc.) as defined by information classification and protection policies.</p> <ul style="list-style-type: none"> <li>• Data at Rest Yes</li> <li>• Data in Transit Yes</li> <li>• Corporate laptops and desktops Yes</li> <li>• Data on Removable media</li> <li>• Mobile Devices (e.g., Mobile phones and tablets)</li> <li>• Backups Yes</li> </ul>	

### Media Disposal

3.3.1	<p>Our organization maintains data disposal/sanitization policies that define media (e.g., hard drives, CDs, USB storage devices, etc.) sanitization requirements and techniques.</p> <p>[ Yes , No ]</p>	Yes
-------	---	-----

---

3.3.2	We have procedures or contracts with service providers to sanitize items or media with sensitive/confidential information prior to reuse or to disposal. [ Yes , No ]	Yes
3.3.3	Our procedure or service provider retains an audit trail - chain of custody process and proof of media destruction/disposal (i.e., certificate of disposal or destruction). [ Yes , No ]	Yes

## Inventory and Control of Enterprise Assets

#	Prompt	Response
<b>Inventory all hardware devices</b>		
4.1.1	The following percentage of hardware connected to the organization's network is inventoried: [ 0-24% , 25-49% , 50-74% , 75-100% , N/A ]	75-100%
4.1.2	The organization's hardware asset inventory is updated: [ Bi-annually , Annually , Other ]	Other
<b>Track all hardware devices</b>		
4.2.1	The organization's hardware inventory is documented: [ Manual , Auto , None ]	Auto
4.2.2	An automated asset inventory and discovery tool provides visibility to the following percentage of hardware across the enterprise? [ 0-24% , 25-49% , 50-74% , 75-100% , N/A ]	75-100%
4.2.3	We leverage our automated asset inventory tool's discovery capabilities to help detect unknown or unauthorized devices, and to improve the accuracy of our inventory. [ Yes , No ]	Yes
4.2.4	Our active discovery tool is configured to execute at least: [ Daily , Weekly , Monthly , No ]	Weekly
<b>End of Life (EOL) Technology</b>		
4.3.1	Our organization relies on operating systems, software, or hardware that is no longer supported or is considered "end-of-life" (EOL) by the manufacturers. (If yes, summarize EOL cases) [ Yes , No ]	Yes

- 
- 4.3.2 End-of-life technologies in use by the organization: (select all that apply)
- Are segregated from the rest of the network
  - Have additionally purchased extended support for the software, where available. Yes
  - Other (please add comments describing compensating controls, or summarize milestone dates or target dates to upgrade to a supported platform)



## Inventory and Control of Software Assets

#	Prompt	Response
<b>Inventory all Software</b>		
5.1.1	We maintain an inventory of software in use across the organization. [ Yes , No ]	Yes
5.1.2	If yes to statement 5.1.1, the inventory captures what percentage of software, including version, that is in use throughout the enterprise. [ 0-24% , 25-49% , 50-74% , 75-100% , N/A ]	75-100%
5.1.3	Our inventory of software installed on enterprise assets is updated at least: [ Bi-annually , Annually , Other ]	Annually
<b>Software and Hardware Inventory Tools</b>		
5.2.1	The organization's software inventory is documented: [ Yes , No ]	Yes
5.2.2	An automated software inventory tool provides visibility to the following percentage of information systems across the enterprise: [ 0-24% , 25-49% , 50-74% , 75-100% , N/A ]	75-100%
5.2.3	Our inventory of software is: <ul style="list-style-type: none"> <li>• All supported.</li> <li>• All supported, other than those with documented exception with mitigating controls.</li> <li>• Updated with a process repeated at least monthly.</li> </ul>	Yes
<b>File Integrity Tools (Allowlisting)</b>		
5.3.1	In concert with the software inventory, our file integrity checking tools validate software has not been modified prior to execution on a system. [ Yes , No ]	No

---

5.3.2	Our application allowlisting technology is configured to allow critical systems to run software only if it is included on our allowlist. (Describe the allowlisting solution and indicate the name of the solution provider below). [ Yes , No ]	Yes
-------	---	-----

## Secure Configuration of Enterprise Assets and Software

#	Prompt	Response
<b>Standard Secure Baseline Configurations</b>		
6.1.1	We implement standard secure configuration images for operating systems and software applications. [ Yes , No ]	Yes
6.1.2	Our standard secure configurations for operating systems and software applications incorporate industry recognized security hardening techniques (e.g., Center for Internet Security (CIS) Security Configuration Benchmarks or NIST security configuration checklists, etc.). [ Yes , No ]	Yes
6.1.3	We implement secure configurations (incorporating industry recognized security hardening techniques) for the following percentage of our operating systems and software applications: [ 0-24% , 25-49% , 50-74% , 75-100% , N/A ]	75-100%
<b>System Configuration Management Tools</b>		
6.2.1	Our system configuration management tools (e.g., Active Directory Group Policy, etc.) enforce and redeploy configuration settings to systems. [ Yes , No ]	Yes
<b>Information System Change Tools</b>		
6.3.1	In our organization, the development, testing, and production IT environments are separated. [ Yes , No ]	Yes
6.3.2	Our formal system/application change control policy requires risk assessment, security testing, authorization, and establishment of roll-back procedures prior to deployment into our production environment. [ Yes , No ]	Yes

---

**Screen Lockout / Inactivity Logout**

- |       |  |     |
|-------|--|-----|
| 6.4.1 | Our system configuration automatically engages screensaver lockout after a set period of inactivity to limit access to unattended computers.<br>[ Yes , No ] | Yes |
| 6.4.2 | In our organization, user accounts are automatically logged off after a standard period of inactivity.<br>[ Yes , No ]                                       | Yes |

**Unsuccessful Logon Attempts / Automatic Account Lock**

- |       |   |     |
|-------|---|-----|
| 6.5.1 | In our organization, accounts are locked out after a set number of failed login attempts and accounts either automatically unlock after a standard period of time or end-users contact the helpdesk to unlock accounts.<br>[ Yes , No ] | Yes |
|-------|---|-----|

## Audit Log Management

#	Prompt	Response
<b>Audit Logs and Records</b>		
7.1.1	We implement standard audit logging policies for hardware devices and software. [ Yes , No ]	Yes
7.1.2	Our audit logging policies require a timestamp, source addresses, destination addresses, and other useful data elements. [ Yes , No ]	Yes
7.1.3	Whenever possible, our system logs are kept in a standardized format, such as syslog entries or the Common Event Expression. [ Yes , No ]	Yes
7.1.4	We utilize at least two synchronized time sources to provide uniform timestamps. [ Yes , No ]	Yes
7.1.5	We maintain audit logs for a period of no less than (select from list):	6 months
7.1.6	The organization enforces detailed audit logging of access or changes to sensitive data. [ Yes , No ]	Yes
<b>Audit Storage Capacity</b>		
7.2.1	We configure our network boundary devices including: firewalls, network-based Intrusion Prevention System (IPS), and inbound and outbound proxies to "verbosely log" traffic both allowed and blocked. [ Yes , No ]	Yes

7.2.2	Select all of the Audit Policies enabled on Domain Controllers:	
	• Audit Credential Validation (Failure)	Yes
	• Audit Process Creation (Success)	Yes
	• Audit Security Group Management (Success and Failure)	Yes
	• Audit User Account Management (Success and Failure)	Yes
	• Audit Other Account Management Events (Success and Failure)	
	• Audit Sensitive Privilege Use (Success and Failure)	
	• Audit Logon (Success and Failure)	Yes
	• Audit Special Logon (Success)	Yes
	• None of the above	
	• Using Active Directory	Yes

#### Audit Anomaly Reviews

7.3.1	Our organization analyzes audit logs/reports /alerts on a regular basis to identify anomalies or unusual activities.	SIEM
7.3.2	Our security personnel and/or system administrators actively review anomalies to identify unauthorized activities and resolve incidents via our incident response and management processes. [ Yes , No ]	Yes

## Network Monitoring and Defense

#	Prompt	Response
Security Operations Center / SIEUM		
8.1.1	<p>The organization operates its own Security Operations Center (SOC) and/or has an outsourced Managed Security Service Provider (MSSP) with the following capabilities at a minimum:</p> <ul style="list-style-type: none"> <li>a) Established incident alert thresholds</li> <li>b) Security Incident and Event Management (SIEM) monitoring and alerting for unauthorized access connections, devices, and software.</li> </ul> <p>[ Own , MSSP , No ]</p>	Own
8.1.2	<p>The SOC/MSSP capabilities include, but are not limited to, the following:</p> <ul style="list-style-type: none"> <li>a) 24x7 operations</li> <li>b) mix of signature and heuristic-based detection</li> <li>c) incident response, containment, and remediation capabilities</li> <li>d) active threat intelligence and analytics delivering rapid alerts/notification and/or countermeasures</li> <li>e) processes are continuously improved.</li> </ul> <p>[ Yes , No ]</p>	Yes
8.1.3	<p>We implement a SIEM (Security Information and Event Management) or log analytic tool for unified aggregation, consolidation, correlation, analysis, and alerting.</p> <p>[ Yes , No ]</p>	Yes
8.1.4	<p>We continuously refine and tune our SIEM (e. g., profiling common system events to tune detection towards unusual activity) to minimize false positives and insignificant alerts.</p> <p>[ Yes , No ]</p>	Yes

---

8.1.5	Our Security Operations Center / Managed Security Service Provider (SOC/MSSP) obtains relevant indicators of compromise (IOCs) combined with leveraging threat intelligence feeds to rapidly discover and respond to threats. (e.g., correlate IOC and identify and alert on threat actors targeting the organization). [ Yes , No ]	Yes
-------	---	-----

#### Intrusion Detection and Prevention Systems

8.2.1	Our organization deploys intrusion detection and prevention security devices at network egress points to detect and prevent attacks through the use of signatures, network behavior analysis, and other mechanisms. [ Yes , No ]	Yes
8.2.2	Our intrusion prevention systems (IPS) are deployed in an active block mode - to block known bad signatures, malicious activities/ code, and sophisticated attack behaviors. [ Yes , No ]	Yes
8.2.3	Our organization routes all outbound web requests through a web proxy which monitors for and blocks potentially malicious content. [ Yes , No ]	Yes



## Account Management

#	Prompt	Response
<b>Identity and Access Management</b>		
9.1.1	Please describe the organization's remote access protocols (e.g., Remote Desktop Protocol RDP, VPN, Telnet, etc.) to the corporate network and how the organization secures remote access for each protocol.	HTTPS to VDI
9.1.2	Select all responses that are true: Which of the following tools does the Applicant use for directory services, identity providers (IdP), federation and/or rights management?	
	• Microsoft Active Directory (Active Directory)	Yes
	• Azure Active Directory (Azure AD)	Yes
	• Okta	
	• Ping	
	• Active Directory Federation Services	Yes
	• Google Workspaces	
	• Other (details required – provide in the comments below)	Yes
	• None of the above/Don't Know.	
	<i>Comment</i>	<i>Oracle OUD</i>
9.1.3	Select one response: What is the source of identity for the majority of Applicant's users?	Microsoft Active Directory (Active Directory)
	[ Microsoft Active Directory (Active Directory) , Azure Active Directory (Azure AD) , Active Directory and Azure AD (Active Directory is authoritative) , Azure AD and Active Directory (Azure AD is authoritative) , An Identity Provider ("IdP"; e.g., Okta or Ping) , Cloud-based collaboration (e.g., Google Workspaces) , Other (details required – provide in the comments below) , No centralized identity management or don't know. ]	



9.1.7	Indicate the number of users who have persistent administrative access to servers and/or workstations other than their own.	0
	<i>Comment</i>	<i>We use PAM solution</i>

### Account Management and Review

9.2.1	We review user accounts at least annually to confirm all accounts are associated with a valid end-user. [ Yes , No ]	Yes
9.2.2	We review service/system accounts at least annually and disable any account that cannot be associated with a valid business process and owner. [ Yes , No ]	Yes
9.2.3	We review user, administrative, and privileged accounts at least (select from list) to confirm all accounts are associated with a valid user. [ Quarterly , Annually , No ]	Annually
9.2.4	We monitor user accounts and flag dormant accounts (e.g., accounts with no activity for over 60 calendar days) and consult with the corresponding manager prior to disabling the account. [ Yes , No ]	Yes

### Password Policies

9.3.1	Our organization's technical controls enforce the following password requirements (select all that apply):	
	• Minimum number of characters	Yes
	• Complexity (e.g., lowercase, uppercase, numbers, or symbols) requirements	Yes
	• Prohibit reuse	Yes
	• Blocking known weak passwords (e.g., "1q2w3e4r5t" and "Passw0rd!")	Yes
	• Detects known compromised/breached passwords from dark web and other sources, and enforces a password reset	
	• Passwords expiration (change is required) at least annually	Yes

---

9.3.2	If there are technological limitations preventing multi-factor authentication, then we enforce complex long passwords (i.e., longer than 14 characters). [ Yes , No ]	Yes
-------	--	-----

## Access Control Management

#	Prompt	Response
<b>Identity and Access Management</b>		
10.1.1	Select all responses that are true: With regards to how the Applicant protects user accounts with domain administrative privileges ("Domain Administrator Accounts"):	
	• System administrators have a unique, privileged credential for administrative tasks (separate from their user credentials for everyday access, email, etc.).	Yes
	• Domain Administrator Accounts require multifactor authentication.	
	• Domain Administrator Accounts are managed and monitored through just-in-time access, are time bound, and require approvals to provide privileged access.	Yes
	• Domain Administrator Accounts are kept in a password safe that requires the user to "check out" the credential (which is rotated afterwards).	Yes
	• In addition to being kept in a password safe, Domain Administrator Accounts are not exposed to the administrative user when "checked out", and access is recorded through a session manager.	Yes
	• Domain Administrator Accounts can only be used from Privileged Access Workstations (workstations that do not have access to internet or email).	Yes
	• There is a log of all actions by "Domain Administrator Accounts" for at least the last thirty days.	Yes
	• None of the above/Don't Know.	

10.1.2	<p>The organization's posture with respect to access controls for member servers is best described as:</p> <p><i>Note: This question is regarding employees' everyday user accounts; where the Applicant provisions employees with separate credentials for administrative access, those accounts should not be considered for the purposes of this question.</i></p> <p>[ No employees are in the Administrator's group or have local admin access to member servers. , Applicant's policy is that employees by default are not in the Administrators' group and do not have local admin access; all exceptions to the policy are documented. , Some of the Applicant's employees are in the Administrators' group or are local admins. , Do not know. ]</p>	No employees are in the Administrator's group or have local admin access to member servers.
--------	---	---

#### Account Monitoring

10.2.1	<p>In our organization, user accounts have an expiration date which is monitored and enforced.</p> <p>[ Yes , No ]</p>	Yes
10.2.2	<p>In our organization, system accounts have an expiration date which is monitored and enforced.</p> <p>[ Yes , No ]</p>	Yes

#### Account Revocation

10.3.1	<p>We follow a process to disable user accounts upon termination of an employee, contractor /consultant, or third party user.</p> <p>[ Yes , No ]</p>	Yes
10.3.2	<p>We follow a process to disable system accounts upon termination of an employee, contractor/consultant, or third party user.</p> <p>[ Yes , No ]</p>	Yes

#### Privileged Access Management

10.4.1	We limit the use and distribution of administrator or privileged accounts (select all that apply): <ul style="list-style-type: none"><li>• Via an account authorization process requiring senior management approval.</li><li>• Administrative/Privileged credentials are separate from credentials used to perform day-to-day tasks.</li><li>• Administrators are explicitly disallowed from surfing the internet or accessing personal email from their privileged accounts.</li></ul>	Yes  Yes
10.4.2	The organization manages Desktop / Local Administrator privileges via: Please check all that apply and indicate the name of the solution(s) below: <ul style="list-style-type: none"><li>• Endpoint Privilege Management (EPM)</li><li>• Local Administrator Password Solution (LAPS) or an equivalent solution that sets a different, random password for the common local administrator account across all domain-attached computers.</li><li>• Privileged Access or Account Management (PAM)</li><li>• Other (please describe below):</li></ul>	Yes
10.4.3	The organization implements a Privileged Account Management (PAM) solution that, (select all that apply, and add a comment with the name of your PAM solution) <ul style="list-style-type: none"><li>• Controls access to administrative/privileged accounts</li><li>• Monitor, record, audit and analyze administrative/privileged access, sessions, and actions</li><li>• Automated credential management (i.e., credentials automatically rotate after each use or the use of temporary one-time use passwords)</li></ul>	Yes  Yes

### Multi-Factor Authentication

---

10.5.1	<p>The scope of our PAM implementation includes, (check all that apply):</p> <ul style="list-style-type: none"><li>• Application Accounts</li><li>• Break glass (emergency or firecall) accounts</li><li>• Domain administrative accounts</li><li>• Service accounts</li><li>• Windows local accounts</li><li>• Windows server local accounts</li></ul>	<p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p>
10.5.2	<p>Our organization uses the following secondary factor methods for MFA:</p> <ul style="list-style-type: none"><li>• SMS</li><li>• Biometric authentication</li><li>• Authenticator application</li><li>• Secondary email</li><li>• Endpoint certificate</li><li>• Physical security keys</li></ul>	<p>Yes</p> <p>Yes</p>
10.5.3	<p>Irrespective of a user's location, we require multi-factor authentication for access to our most critical or sensitive data or systems.</p> <p>[ Yes , No ]</p>	<p>No</p>
10.5.4	<p>We require multi-factor authentication for all remote login access to the corporate network (e.g., Virtual Private Network (VPN), Remote Desktop Protocol (RDP), or other secure remote access, etc.).</p> <p>[ Yes , No ]</p>	<p>Yes</p>
10.5.5	<p>Irrespective of a user's location, we require multi-factor authentication and encrypted channels for all administrative account access.</p> <p>[ Yes , No ]</p>	<p>No</p>



## Network Infrastructure Management

#	Prompt	Response
<b>Firewall</b>		
11.1.1	The organization configures firewalls to prevent unauthorized access, and the firewall configurations are reviewed at least annually. [ Yes , No ]	Yes
11.1.2	Our formal firewall policy is to deny-all by default, permit-by-exception to ensure only explicitly approved incoming/outgoing traffic is permitted. [ Yes , No ]	Yes
<b>Wireless Network Security</b>		
11.2.1	We implement wireless security policies and protocols that require strong encryption standards. [ Yes , No ]	Yes
11.2.2	Our organization maintains a completely separate (logically or physically) wireless network for guests, Bring Your Own Device (BYOD) users, and other untrusted devices. [ Yes , No ]	Yes
<b>Network Segmentation</b>		
11.3.1	In our organization, the network is segmented based on: (select the answer(s) that best reflects your network segmentation approach): <ul style="list-style-type: none"> <li>• Business unit</li> <li>• Geographic/regional</li> <li>• Classification level of the information stored on the servers</li> <li>• Data processing and storage based on the sensitivity of the data</li> <li>• Isolating critical systems, functions, or resources</li> <li>• Role and functionality</li> </ul>	Yes

---

11.3.2	To mitigate risks/threats and increase our operational resilience, we implement enhanced security controls /protections (select all that apply):	
	• Perform traffic filtering between network segments.	Yes
	• Use network appliances to filter ingress or egress traffic and perform protocol filtering.	Yes
	• Deploy a network intrusion prevention solution to block known malicious traffic at network boundaries.	Yes
	• Implement port-level access control utilizing 802.1x or similar Network Access Control (NAC) protocols for authenticating and authorizing device.	
	• Configure software on user workstations, with a default-deny rule to drops all traffic except those services and ports that are explicitly allowed.	

## Malware Defenses

#	Prompt	Response
<b>Malware Protection</b>		
12.1.1	The organization implements the following malware protections:	
	• Incoming emails are filtered/scanned for known malicious attachments and suspicious file types, including executable	Yes
	• Macro-enabled files cannot be run by default.	Yes
	• A quarantine service is provided.	Yes
	• Email attachments are evaluated in a sandbox to determine if malicious prior to delivery.	Yes
	• Emails are filtered to block suspicious messages based on their content or attributes of the sender.	Yes
12.1.2	The organization installs and regularly updates anti-malware solutions (e.g., anti-virus, anti-spyware, advanced endpoint security) to the following percentage of assets, and exceptions are documented.	
	Workstations and laptops.	96-100%
	Servers, excluding hypervisor hosts.	96-100%
	Mobile devices, including tablets and phones but excluding laptops.	0-24%
12.1.3	Specify the endpoint security tool(s) used. If multiple, please add in commentary area.	
	Solution provider name (e.g. "CrowdStrike", "Microsoft", or "VMware", etc.):	Trend Micro
	Solution/product name and included options ("Falcon Complete", "Microsoft Defender for Endpoint P2" or "Carbon Black EDR"):	Apex One

---

12.1.4	The endpoint security tool(s) are configured to:(select all that apply)	
	• For those tools which require updated definitions, such tools are updating at least daily.	Yes
	• Block (as opposed to solely notify of) suspected malicious processes and files.	Yes
	• Find unmanaged assets, which are addressed at least weekly.	
	• Enable anti-tamper features.	Yes

## Continuous Vulnerability Management

#	Prompt	Response
<b>Vulnerability and Patch Management</b>		
13.1.1	Vulnerability scans are performed at least <i>(select from dropdown list)</i>	Monthly
13.1.2	Our organization deploys automated patch management processes/tools to update operating systems, software/applications, and other application software or firmware. [ Yes , No ]	Yes
13.1.3	Our organization deploys vulnerability patches:	Monthly
13.1.4	The organization's target timeframe to patch Common Vulnerability Scoring System (CVSS) v3 Critical Severity 9.0-10.0 vulnerabilities across your enterprise is:	Within 7 calendar days of release
13.1.5	In the most recent full quarter, the organization was successful at achieving the target timeframe selected above in statement 13.1.4 to patch (select from list) CVSS Critical Severity vulnerabilities across the enterprise.	>95%
13.1.6	The organization's target timeframe to patch Common Vulnerability Scoring System (CVSS) v3 High Severity 7.0-8.9 vulnerabilities across your enterprise is:	Within 30 calendar days of release
<b>Penetration Testing</b>		
13.2.1	In our organization, annual or more frequent penetration testing (i.e., testing that emulates adversary actions and hostile cyber attacks) is conducted on the network and critical systems. [ Yes , No ]	Yes

---

13.2.2	<p>Our processes require penetration testing activities that include, but are not limited to, the following:</p> <ul style="list-style-type: none"><li>a) annual assessment(s)</li><li>b) independent penetration agents simulate adversary actions</li><li>c) testing scope includes the network and business critical systems/ applications</li><li>d) penetration test results and recommendations are risk-rated and/or prioritized to mitigate or remediate vulnerabilities and weaknesses identified.</li></ul> <p>[ Yes , No ]</p>	Yes
--------	---	-----

## Security Awareness and Skills Training

#	Prompt	Response
<b>Security Training</b>		
14.1.1	In our organization, cybersecurity training is mandatory for all employees (select period from list). <i>Comment</i>	No  <i>vengono svolte sessioni formative al personale preposto. In media sono erogate circa 5 sessioni l'anno a circa 400 discenti.</i>
14.1.2	Cybersecurity training is mandatory for vendors/contractors and third party partners with access to the corporate network (select period from list). <i>Comment</i>	No  <i>ai fornitori sono rese disponibili istruzioni operative e le politiche di sicurezza da rispettare nell'erogazione del servizio</i>
14.1.3	We perform an annual analysis to identify gaps in our cybersecurity skillset, and develop and implement training roadmaps and/or project plans to close identified gaps. [ Yes , No ]	No
<b>Security Awareness Program</b>		
14.2.1	Our cybersecurity awareness program materials train users to avoid common cyber-risks and threats, such as social engineering and phishing. [ Yes , No ]	Yes
14.2.2	We update cybersecurity awareness training and communications content frequently (at least annually) to embody the latest attack and social engineering techniques. [ Yes , No ] <i>Comment</i>	No  <i>la formazione è aggiornata con maggior frequenza</i>
14.2.3	Our organization tags external emails to alert employees that the email originated from outside the organization. [ Yes , No ]	Yes

---

14.2.4	The organization conducts internal phishing campaigns at least annually. [ Yes , No ] <i>Comment</i>	No  <i>sono eseguite con maggior frequenza</i>
14.2.5	Our organization has a documented process to report suspicious emails to an internal security team to investigate. [ Yes , No ]	Yes



## Data Recovery

#	Prompt	Response
<b>Recovery Processes and Procedures</b>		
15.1.1	Our organization conducts backups for <b>Applications</b>	Continuously
15.1.2	Our organization conducts backups for <b>Databases</b>	Continuously
15.1.3	Our organization conducts backups for <b>Servers</b>	Continuously
15.1.4	Our organization conducts backups for <b>Workstations/laptops and endpoints</b>	Other (please describe)
15.1.5	Our organization conducts backups for <b>Critical Information</b> (Critical Information means critical information as defined by the organization's information classification or business continuity / disaster recovery plans/policies)	Continuously
15.1.6	We test system restoration capabilities by performing a full restoration from a sample set of backup data at least. [ Quarterly , Bi-Annually , Annually , Other , No ]	Annually
15.1.7	To strengthen recovery from malicious encryption (e.g., crypto-ransomware attack), we isolate backup files from the network (i.e., backup files are not continuously accessible from the network).	
	• Isolate backup files from the network (i.e., backup files are not continuously accessible from the network).	Yes
	• Store offline (archive) backups onsite.	Yes
	• Store offline (archive) backups offsite.	Yes
15.1.8	• Backups are immutable (i.e., cannot be altered or deleted)	Yes
	After an incident is contained, the organization implements procedures /processes to remediate affected systems and restore systems to our normal or fully operational state. [ Yes , No ]	Yes

---

**Business Continuity**

15.2.1	The organization maintains a business continuity/disaster recovery plan, and the plan is tested: [ Quarterly , Semi-annually , Annually , Biennially (once every 2 years) , Other or N/A ]	Annually
15.2.2	The organization's Recovery Time Objective (RTO), defined as the maximum target period IT functionality may be lost due to an incident, is the following for critical systems: [ Less than 5 hours , Less than 12 hours , Less than 24 hours , Greater than or equal to 24 hours , Other or N/A ]	Less than 5 hours
15.2.3	Our organization reviews and updates IT disaster recovery plans quarterly to address system/organizational changes, lessons learned, or problems encountered during the most recent restoration. [ Yes , No ]	Yes
15.2.4	The organization maintains an alternate backup IT facility which would be categorized as: [ A cold site , A warm site , A hot site , Other or N/A ]	A hot site
15.2.5	The organization has the capability to immediately failover to redundant or standby information systems. [ Yes , No ]	Yes
15.2.6	We review and revise IT disaster recovery plans on an annual basis; revisions incorporate lessons learned from IT disaster recovery plan tests and previous restoration activities. [ Yes , No ]	Yes

## Service Provider Management

#	Prompt	Response
<b>Outsourced Services</b>		
16.1.1	The organization conducts security assessments and periodic re-assessments on third party partners and other service providers with access to information assets. [ Yes , No ]	Yes
16.1.2	The organization reviews independent audit reports (e.g., SSAE 18 SOC 2, HITRUST certification, or Standardized Information Gathering (SIG), Agreed Upon Procedures (AUP)*) from third party partners and other service providers with access to information assets at least annually. * The most recent version of the standards listed. [ Yes , No ]	Yes
16.1.3	Our organization requires confirmation from our cloud vendors that they are compliant with any applicable laws related to data storage and data transfer. [ Yes , No ] <i>Comment</i>	Yes  <i>si sulla base degli obblighi di legge in materia di codice degli appalti</i>
16.1.4	Our cloud provider utilizes DDoS mitigation solutions. [ Yes , No ]	Yes
<b>Third Party Risk Management Oversight</b>		
16.2.1	Our organization requires vendors to maintain insurance or another means of indemnification for losses caused by the provider, including from a privacy breach. [ Yes , No ]	Yes
16.2.2	The organization requires interconnection agreements for connections between the organization's network and external networks (e.g., third-parties, vendors, etc.). [ Yes , No ]	Yes

---

16.2.3	If interconnection security agreements are required, the organization's agreements contain information/cybersecurity requirements including risk-based monitoring for anomalous activities. [ Yes , No ]	Yes
16.2.4	The organization has a process or technical solution to identify, assess, manage, monitor, and reduce the risks from third party partners and other service providers. [ Yes , No ]	Yes
16.2.5	We maintain an inventory of what percentage of third party or vendor managed information systems (residing outside of the organization's boundaries and not under the organization's direct control) that have access to or process our information assets (e.g., cloud, SaaS, etc.). [ 0-24% , 25-49% , 50-74% , 75-100% , N/A ]	25-49%

## Incident Response Management

#	Prompt	Response
<b>Incident or Breach Response Plan(s)</b>		
17.1.1	<p>Our incident response or breach response plan is (select all that apply):</p> <ul style="list-style-type: none"> <li>• Formally documented.</li> <li>• Aligned with the National Institute of Standards and Technology (NIST) Special Publication 800-61.</li> <li>• Aligned with ISO/IEC 27035 guidance</li> <li>• Aligned with an other governmental authority (e.g. US-CERT or ANSSI) – please describe in comments.</li> </ul> <p><i>Comment</i></p>	<p>Yes</p> <p>Yes</p> <p><i>Aligned with Italian Data Protection Authority rules, Italian National Security Perimeter rules and policy and recommendations from our Customers, owners of Data handled by Sogei.</i></p>
17.1.2	<p>Our incident response program requires incident response and reporting instructions within contracts for third party partners or service providers that manage or have access to corporate/organizational data via contract riders or agreed-upon terms and conditions.</p> <p>[ Yes , No ]</p> <p><i>Comment</i></p>	<p>Yes</p> <p><i>There is a specific Data Protection annex in contracts to deal with Data Breaches.</i></p>
17.1.3	<p>We have internal resources and/or an active contract with incident response service providers to accomplish incident containment, eradication (e.g., eliminate malware and return systems to normal operations), and orchestrate recovery.</p> <p>[ Yes , No ]</p>	<p>Yes</p>

17.1.4	Our incident response program encompasses the following core capabilities:	
	<ul style="list-style-type: none"> <li>Processes/procedures for performing incident classification, prioritization, handling, reporting, and recovery.</li> </ul>	Yes
	<ul style="list-style-type: none"> <li>Ransomware response playbook.</li> </ul>	
	<ul style="list-style-type: none"> <li>Playbook for a ransomware incident of 3rd parties/MSPs.</li> </ul>	
	<ul style="list-style-type: none"> <li>A defined response team structure.</li> </ul>	Yes
	<ul style="list-style-type: none"> <li>Plan testing or exercise requirements.</li> </ul>	
	<ul style="list-style-type: none"> <li>Plan review and update schedule.</li> </ul>	Yes
	<ul style="list-style-type: none"> <li>Process to resume business operations by restoration of known clean backups</li> </ul>	
	<ul style="list-style-type: none"> <li>Process/procedures for recovery, such as activating the IT disaster recovery plan</li> </ul>	Yes
	<ul style="list-style-type: none"> <li>Names and contact information for relevant authorities, including law enforcement</li> </ul>	Yes

### Incident Response Exercises

17.2.1	Our organization conducts incident/breach response scenario-based exercises that: (select all that apply)	
	<ul style="list-style-type: none"> <li>Include Cyber Incident response tabletop reviews.</li> </ul>	
	<ul style="list-style-type: none"> <li>Requires participation from cyber incident response and senior management personnel defined in our plan to refresh their responsibilities.</li> </ul>	
	<ul style="list-style-type: none"> <li>Reflect current threats and risks faced by our industry or similar organizations, including facing threats from ransomware actors.</li> </ul>	
	<ul style="list-style-type: none"> <li>Results in documentation of lessons learned and revisions/improvements required.</li> </ul>	Yes

### Incident Containment and Mitigation Activities

17.3.1	Our security operations center or third party provider monitors the US-CERT, industry-related Information Sharing and Analysis Center (ISAC), and other feeds for alert and threat information; this information is reviewed and actions taken to mitigate risks. [ Yes , No ]	Yes
--------	---	-----

*Comment*

*Sogei's CERT has several threat intelligence sources and providers.*

17.3.2	Our incident response strategy is integrated with organization/corporate business continuity plans and IT disaster recovery capabilities. [ Yes , No ]	Yes
17.3.3	What is the Applicant's average time to triage and contain security incidents of workstations for the most recent completed quarter?	Applicant does not track this metric/Don't know.
17.3.4	Our incident monitoring/ handling practices require incident documentation [ Yes , No ]	Yes
17.3.5	We have qualified forensics personnel or an active contract with a forensics service provider to conduct investigations, determine the scope of a breach, and establish what data was compromised. [ Yes , No ]	Yes

#### Forensics are performed

17.4.1	We review and revise incident/breach response plans to address system /organizational changes, lessons learned, or problems encountered during previous incident detection and response activities. [ Yes , No ]	Yes
17.4.2	We have a documented crisis communication plan that addresses communications activities such as, but not limited to, the following: a) emergency contact information for senior personnel, such as senior executives, corporate communications, the general counsel, and the CIO/CISO, etc. b) identification and contact information for key audiences, such as customer/ investor relations managers, employee unions, and state and federal regulators, etc. [ Yes , No ]	Yes

---

17.4.3	<p>Our crisis communication plan includes, but is not limited to:</p> <ul style="list-style-type: none"><li>a) cyber insurance policy documentation and contact information</li><li>b) guidelines and procedures for establishing a corporate spokesperson</li><li>c) approval and escalation procedures to clear information or press releases prior to external release</li><li>d) breach notification template and consultation process with external legal counsel to review and approve notices prior to release</li></ul> <p>[ Yes , No ]</p>	Yes
--------	---	-----

#### Incident Response Plan Improvement

17.5.1	<p>In concert with our incident/ breach response plans, we maintain pre-negotiated contracts with data breach response/ resolution providers (e.g., call centers, notices and communications, and credit monitoring services).</p> <p>[ Yes , No ]</p>	Yes
17.5.2	<p>Our organization retains pre-approved reputational risk advisors to develop an action plan to improve public relations, enhance customer trust, and monitor the effectiveness of these plans.</p> <p>[ Yes , No ]</p>	Yes



## Technology in Use

#	Prompt	Response
<b>Microsoft 365 Protections</b>		
18.1.1	The organization uses Microsoft 365. [ Yes , No ]	Yes
18.1.2	The organization uses the following protections with Microsoft 365. <ul style="list-style-type: none"> <li>• Microsoft 365 Advanced Threat Protection.</li> <li>• Multi-Factor Authentication is required at all times.</li> <li>• Other (please describe email security capabilities in commentary).</li> <li>• Not applicable.</li> </ul>	Yes
<b>Cloud Utilization</b>		
18.2.1	The organization utilizes cloud computing in the following way(s): <i>(please check all that apply)</i> <ul style="list-style-type: none"> <li>• Public cloud</li> <li>• Private cloud</li> <li>• Hybrid of public/private cloud</li> <li>• The organization does not utilize cloud computing</li> </ul>	Yes Yes Yes
18.2.2	Please describe the types of business processes, applications or functions which the organization relies on for cloud computing.	Collaboration & Communication, IaaS

## Information / Cybersecurity Capabilities and Tools

18.3.1	<p>The organization operates the following Information Technology (IT) and Information/Cybersecurity tools and capabilities <i>(please check all that apply and indicate key vendors)</i>:</p> <ul style="list-style-type: none"> <li>• Network Intrusion Detection/Prevention Systems (IDPS) Yes</li> <li>• Unified Threat Management (UTM)/ Threat Prevention/ Protection Systems (TPS)</li> <li>• Network Data Loss Prevention (DLP) solution</li> <li>• Protective Domain Name Service (PDNS) Yes</li> <li>• Security Information and Event Management (SIEM) Yes</li> <li>• Email DLP solution</li> <li>• Enforce Sender Policy Framework (SPF) Yes</li> <li>• DomainKeys Identified Mail (DKIM) Yes</li> <li>• Domain-based Message Authentication, Reporting and Conformance (DMARC) Yes</li> <li>• Block malicious and phishing URLs Yes</li> <li>• Multi-Factor Authentication to on-premise backups</li> <li>• Multi-Factor Authentication to cloud-based backups</li> <li>• Host Intrusion Prevention Systems (HIPS) Yes</li> <li>• File Integrity Tools (Whitelisting)</li> <li>• Endpoint DLP solution</li> <li>• Endpoint Detection and Response (EDR) solutions Yes</li> <li>• Advanced Endpoint Security Yes</li> <li>• Network Detection and Response (NDR) solutions Yes</li> <li>• Identity and Access Management solutions Yes</li> <li>• Bring Your Own Device (BYOD) security solutions</li> <li>• Password management software Yes</li> <li>• Wireless Network Security solutions</li> <li>• Network Intrusion Detection Systems (NIDS) Yes</li> <li>• DDoS mitigation solutions Yes</li> <li>• Please describe other tools or capabilities that support the organization's cyber /information security program</li> </ul>
--------	---

## Event History

#	Prompt	Response
Event History		
19.1.1	<p>Within the past 5 years, has the organization sustained any network security incidents or data incidents that resulted in a material financial loss to the organization? If yes, please describe in detail below.</p> <p>[ Yes , No ]</p>	No
19.1.2	<p>Within the past 5 year, has the organization received any demands or claims relating to allegations of theft of information or breach of information security? If yes, please describe in detail below.</p> <p>[ Yes , No ]</p>	Yes
19.1.3	<p>Within the past 5 years has the organization been required to notify any individuals or entities because of a breach of information security? If yes, please describe in detail below.</p> <p>[ Yes , No ]</p> <p><i>Comment</i></p>	<p>Yes</p> <p><i>We've had several Data Breaches.</i></p>
19.1.4	<p>Within the past 5 years, has the organization been the subject of any government action, regulatory investigation or subpoena regarding any alleged violation of any privacy /data security law or regulation? If yes, please describe in detail below.</p> <p>[ Yes , No ]</p> <p><i>Comment</i></p>	<p>Yes</p> <p><i>We've had investigations from the Italian Data Protection Authority.</i></p>
19.1.5	<p>Within the past 5 years, has the organization experienced a network outage, or substantial loss of IT functionality for more than 6 hours? If yes, please describe in detail below.</p> <p>[ Yes , No ]</p> <p><i>Comment</i></p>	<p>Yes</p> <p><i>We've had two events of power and network outage in our Data Center, lasting more than 6 hours.</i></p>

---

19.1.6	<p>Within the past 5 years has the organization sustained any network security incidents, or outages as the result of the actions of a 3rd party vendor (e.g. cloud vendors, IT consultants, payroll, data processing)? If yes, please describe in detail below.</p> <p>[ Yes , No ]</p> <p><i>Comment</i></p>	<p>Yes</p> <p><i>We've had a breach sustained by Microsoft that impacted our mail operations.</i></p>
--------	--	---

Biometric Information

#	Prompt	Response
Biometric Information		
20.1.1	The organization uses or provides technology that scans biometric identifiers, e.g. fingerprints, fingers, hands, faces, eyes. [ Yes , No ]	No

## HIPAA

#	Prompt	Response
HIPAA		
21.1.1	Your organization is considered a Covered Entity under the Health Insurance Portability and Accountability (HIPAA) Act and the Health Information Technology for Economic and Clinical Health (HITECH) Act. [ Yes , No ]	No
21.1.2	Your organization is considered a Business Associate under the HIPAA/HITECH Acts. [ Yes , No ]	No

**PCI**

#	Prompt	Response
<b>PCI</b>		
22.1.1	Your organization is required to be compliant with Payment Card DSS Standards (PCI-DSS). [ Yes , No ]	No

## Trending Topics

#	Prompt	Response
<b>SolarWinds</b>		
23.1.1	The organization runs a version of SolarWinds Orion vulnerable to the SUNBURST or SUPERNOVA backdoors. [ Yes , No ]	No
23.1.2	The organization at any time ran a version of SolarWinds Orion vulnerable to the SUNBURST or SUPERNOVA backdoors. [ Yes , No ]	No
<b>Microsoft Exchange / Hafnium</b>		
23.2.1	The organization runs a version of Microsoft Exchange Server 2010 through to 2019 vulnerable to the zero-day exploits being targeted. [ Yes , No ]	No
23.2.2	The organization at any time ran a version of Microsoft Exchange Server 2010 through to 2019 vulnerable to the zero-day exploits being targeted. [ Yes , No ]	No
<b>Pulse Connect Secure VPN</b>		
23.3.1	The organization uses Pulse Connect Secure VPN products. [ Yes , No ]	No
23.3.2	The organization has run the KB44755 Pulse Connect Secure (PCS) Integrity Assurance tool to check for the possibility of compromise. [ Yes , No , Not Applicable ]	Not Applicable
<b>Accellion FTA</b>		
23.4.1	The organization uses the Accellion FTA product. [ Yes , No ]	No
23.4.2	The organization at any time used the Accellion FTA product. [ Yes , No ]	No



---

23.4.3	Your organization is not aware of your data being exposed as a result of the Accellion FTA incident. [ Yes , No ]	Yes
 <b>Log4j</b>		
23.5.1	The organization identified vulnerable versions of Log4j in enterprise systems, including but not limited to: applications, on-premise software components, cloud software components, in-house software development, and third-party technology providers. [ Yes , No ]	Yes
23.5.2	The organization developed software affected by the Log4j vulnerability. [ Yes , No , N/A ]	Yes
23.5.3	Please describe the measures undertaken to investigate and remediate any potential malicious activity in your organization's system.	i sistemi sono stati aggiornati e applicate le patch ove necessario
23.5.4	Please describe the timelines for remediation of impacted systems.	circa 6 mesi
23.5.5	Please describe the measures for detection implemented.	le aree di business hanno verificato la presenza della vulnerabilità in tutti i servizi
23.5.6	The organization has contacted critical suppliers and vendors to determine if they have identified and remediated the Log4j vulnerability in their systems and services. [ Yes , No ]	Yes

**Data Tracking & Collection Tools**

23.6.1	In the last twelve months, has a review been undertaken regarding whether any tracking tools are used on public-facing websites? [ Yes , No ]	Yes
23.6.3	Can you confirm tracking tools are not currently being used and have never previously been used? [ Yes , No ]	Yes

## External Partner Accompaniments

#	Prompt	Response
AIG   Data Security & Business Continuity		
EPA.1.1	<p>Select one response: How centralized is the Applicant's information security program?</p> <p>[ Information security at the Applicant is centrally managed, and the policies apply to all operations. Where exceptions are made, it's by asset only (as opposed to by operation/legal entity). , Information security at the Applicant is centrally managed, but exceptions are made for certain operation/legal entities. The controls as outlined in the Marsh CSA and below apply to greater than or equal to 98% of total endpoints. , Information security at the Applicant is centrally managed, but exceptions are made for certain operation/legal entities. The controls as outlined in the Marsh CSA and below apply to less than 98% of total endpoints. , Information security at the Applicant is federated, but the controls outlined in the Marsh CSA and below apply to greater than or equal to 98% of total endpoints. , Information security at the Applicant is federated, and the controls outlined in the Marsh CSA and below apply to greater than 50% of total endpoints, but less than 98% of total endpoints. , Information security is managed by individual legal entities or operating units. The controls in the Marsh CSA and below are based on a survey of all entities and operating units. , Other (indicate to the right and describe in comments section at end of Data Security &amp; Business Continuity section). , Don't know. ]</p>	<p>Information security at the Applicant is centrally managed, and the policies apply to all operations. Where exceptions are made, it's by asset only (as opposed to by operation/legal entity).</p>

## EPA.1.2

Select all responses that are true: With regards to the Applicant's management of information technology assets (hardware and software):

- The Applicant has an inventory of all enterprise hardware assets - including end-user devices, network devices, appliances, IoT devices, and servers - that includes the network address (if static), hardware address, machine name, and enterprise asset owner, and updates it at least bi-annually. Yes
- The Applicant has an inventory of all enterprise hardware assets - including end-user devices, network devices, appliances, IoT devices, and servers - that includes the network address (if static), hardware address, machine name, and enterprise asset owner, and updates it at least annually.
- The Applicant has a process to discover and identify hardware assets on its network and does so at least daily.
- The Applicant has a process to discover and identify hardware assets on its network and does so at least weekly.
- The Applicant has a process to update its hardware asset inventory at least weekly based on discovery tools or IP Address Management (IPAM) software. Yes
- The Applicant has an inventory of all licensed software installed on enterprise assets and updates it at least bi-annually.
- The Applicant has a process to ensure all software is either supported or is a documented exception with mitigating controls, and the process is repeated at least monthly. Yes
- None of the above.

---

EPA.1.3	Select all responses that are true: With regards to the Applicant's management of "Vital Assets":	
	<ul style="list-style-type: none"><li>• The Applicant has an inventory of all data stores - including data owner, the asset it's stored on, sensitivity, retention limits and disposal requirements - for at least all sensitive data and updates it at least annually.</li></ul>	Yes
	<ul style="list-style-type: none"><li>• The Applicant has defined and documented all "Vital Assets".</li></ul>	Yes
	<ul style="list-style-type: none"><li>• The Applicant has a process to actively identify "Vital Assets" and update the inventory of "Vital Assets" at least quarterly</li></ul>	
	<ul style="list-style-type: none"><li>• The Applicant prioritizes "Vital Assets" by importance to business operations.</li></ul>	Yes
	<ul style="list-style-type: none"><li>• None of the above.</li></ul>	
EPA.1.4	What is the "Recovery Time Objective" (RTO) for "Vital Assets"? "RTO" means the amount of time in which "Vital Assets" are expected to be restored by an organization after a disaster /disruption.	< 5 hours.
EPA.1.5	Select all responses that are true: With respect to the Applicant's disaster recovery capabilities:	
	<ul style="list-style-type: none"><li>• A process for creating backups exists (even if it is undocumented and/or ad hoc).</li></ul>	
	<ul style="list-style-type: none"><li>• Applicant's documented Disaster Recovery Policy requires weekly or more frequent automated backups and standards for backups based on information criticality.</li></ul>	Yes
	<ul style="list-style-type: none"><li>• At least quarterly, Applicant tests its ability to restore different "Vital Assets" in accordance with the Recovery Time Objective (RTO).</li></ul>	
	<ul style="list-style-type: none"><li>• None of the above/Don't know.</li></ul>	

EPA.1.6	Select all responses that are true: With respect to the Applicant's backup capabilities:	
	• Applicant's backup strategy includes offline (archive) backups stored onsite.	
	• Applicant's backup strategy includes offline (archive) backups stored offsite.	Yes
	• Applicant's backup strategy includes onsite, regular backups.	Yes
	• Applicant's backup strategy includes offsite, regular backups (Cloud or Continuity of Operations Site).	Yes
	• Applicant's backups are isolated and separate from the production domain (i.e., they are accessed via an authentication mechanism outside of Active Directory or are otherwise available even if the production domain is compromised) or they are immutable.	Yes
	• None of the above/Don't know.	
EPA.1.7	Select all responses that are true: With respect to the Applicant's policies for the use of encryption to protect data:	
	• The Applicant requires that all data on portable devices - including phones, tablets, and laptops – is encrypted (using full disk encryption or file-based encryption).	
	• The Applicant requires that all end user devices - even if not portable - containing sensitive data must use full disk encryption.	
	• The Applicant requires that all removable media - USB sticks, CDs, etc. - is encrypted.	Yes
	• The Applicant requires that all sensitive data at rest is encrypted (at either the storage layer or application layer).	Yes
	• None of the above/Don't know.	

EPA.1.8	Select all responses that are true: With respect to the Applicant's monitoring of "Vital Assets":	
	• The Applicant has an internal function and/or has an outsourced Managed Security Service Provider ("MSSP") charged with monitoring security event alerts, including alerts on "Vital Assets" (a "Security Operations Center" or "SOC").	Yes
	• The Applicant's SOC/MSSP is provided an updated list of "Vital Assets" at least quarterly.	Yes
	• The Applicant's SOC/MSSP uses a Security Information and Event Monitoring (SIEM) solution to automate the collection of logs from "Vital Assets".	Yes
	• None of the above/Don't know.	
EPA.1.9	If Applicant has any additional commentary on any specific question or response in this section, please provide below:	

#### AIG | Identity, Credential, and Access Management Security

EPA.2.1	Select all responses that are true: Which of the following tools does the Applicant use for directory services, identity providers (IdP), federation and/or rights management?	
	• Microsoft Active Directory (Active Directory)	Yes
	• Azure Active Directory (Azure AD)	Yes
	• Okta	
	• Ping	
	• Active Directory Federation Services	Yes
	• Google Workspaces	
	• Other (details required – provide in the comments below)	Yes
	• None of the above/Don't Know.	
	<i>Comment</i>	<i>Oracle OUD</i>

EPA.2.2	<p>Select one response: What is the source of identity for the majority of Applicant's users?</p> <p>[ Microsoft Active Directory (Active Directory) , Azure Active Directory (Azure AD) , Active Directory and Azure AD (Active Directory is authoritative) , Azure AD and Active Directory (Azure AD is authoritative) , An Identity Provider ("IdP"; e.g., Okta or Ping) , Cloud-based collaboration (e.g., Google Workspaces) , Other (details required – provide in the comments below) , No centralized identity management or don't know. ]</p>	Microsoft Active Directory (Active Directory)
EPA.2.3	<p>Select all responses that are true: With respect to the Applicant's account management:</p> <ul style="list-style-type: none"><li>• The Applicant has an inventory of all user and administrative accounts.</li><li>• The Applicant's inventory of accounts includes the individual's name, username, start/stop dates, and department.</li><li>• The Applicant validates that all active accounts are authorized, at least annually.</li><li>• The Applicant validates that all active accounts are authorized, at least quarterly.</li><li>• None of the above.</li></ul>	<p>Yes</p> <p>Yes</p> <p>Yes</p>

EPA.2.4	Select all responses that are true: With respect to the Applicant's policies and technical controls on passwords:	
	• The Applicant educates users on the risks of password reuse and has a policy against it.	Yes
	• The Applicant has a solution to prevent users from setting common and known-breached passwords, even if they meet complexity requirements (such as "1q2w3e4r5t" and "Passw0rd!").	Yes
	• The Applicant provides a password manager to its employees.	
	• The Applicant has implemented a solution to set different, random passwords across all domain-attached computers for local administrator accounts (i.e., Local Administrator Password Solution - Reference: <a href="https://support.microsoft.com/en-us/topic/microsoft-security-advisory-local-administrator-password-solution-laps-now-available-may-1-2015-404369c3-ea1e-80ff-1e14-5caafb832f53">https://support.microsoft.com/en-us/topic/microsoft-security-advisory-local-administrator-password-solution-laps-now-available-may-1-2015-404369c3-ea1e-80ff-1e14-5caafb832f53</a> ).	
	• None of the above.	



EPA.2.5	<p>Select all responses that are true: With regards to how the Applicant protects user accounts with domain administrative privileges ("Domain Administrator Accounts"):</p> <ul style="list-style-type: none"> <li>• System administrators have a unique, privileged credential for administrative tasks (separate from their user credentials for everyday access, email, etc.).</li> <li>• Domain Administrator Accounts require multifactor authentication.</li> <li>• Domain Administrator Accounts are managed and monitored through just-in-time access, are time bound, and require approvals to provide privileged access.</li> <li>• Domain Administrator Accounts are kept in a password safe that requires the user to "check out" the credential (which is rotated afterwards).</li> <li>• In addition to being kept in a password safe, Domain Administrator Accounts are not exposed to the administrative user when "checked out", and access is recorded through a session manager.</li> <li>• Domain Administrator Accounts can only be used from Privileged Access Workstations (workstations that do not have access to internet or email).</li> <li>• There is a log of all actions by "Domain Administrator Accounts" for at least the last thirty days.</li> <li>• None of the above/Don't Know.</li> </ul>	Yes
		Yes
		Yes
		Yes
		Yes
		Yes
EPA.2.6	<p>Select one response: How do the Applicant's employees authenticate to remotely access the corporate network?</p> <p>[ Remote access to the corporate network generally only requires a valid username and password (single factor authentication). , Multi-factor authentication (MFA) is in place for some types of remote access to the corporate network, but not others. , MFA is required by policy for all remote access to the corporate network, and all exceptions to the policy are documented. , Applicant does not provide remote access to any employees. ]</p>	<p>MFA is required by policy for all remote access to the corporate network, and all exceptions to the policy are documented.</p>

EPA.2.7

Select one response: How do vendors of the Applicant authenticate to remotely access the corporate network?

MFA is required by policy for all remote access to the corporate network, and all exceptions to the policy are documented.

[ Remote access to the corporate network generally only requires a valid username and password (single factor authentication). , MFA is in place for some types of remote access to the corporate network, but not others. , MFA is required by policy for all remote access to the corporate network, and all exceptions to the policy are documented. , Applicant does not provide remote access to any vendors. ]

EPA.2.8

Select one response: How do both employees and vendors of the Applicant authenticate to those Vital Assets which are SaaS/3rd party applications?

MFA is required by policy for all access to externally hosted Vital Assets, and all exceptions to the policy are documented.

[ Access to externally hosted Vital Assets generally only requires a valid username and password (single factor authentication). , MFA is in place for some types of access to externally hosted Vital Assets, but not others. , MFA is required by policy for all access to externally hosted Vital Assets, and all exceptions to the policy are documented. , Applicant does not use SaaS/3rd party hosted applications which would be considered Vital Assets. ]

EPA.2.9	Select all responses that are true: With regards to how the Applicant protects "Privileged" "Service Accounts":	
	• There is an inventory of all "Privileged" "Service Accounts", and it is updated at least quarterly.	Yes
	• "Privileged" "Service Accounts" have password lengths of at least 25 characters.	
	• "Privileged" "Service Accounts" have their passwords rotated at least annually.	
	• "Privileged" "Service Accounts" have their passwords rotated at least quarterly.	
	• "Privileged" "Service Accounts" are configured using the principle of least privilege.	Yes
	• "Privileged" "Service Accounts" are configured to deny interactive logins.	Yes
	• Specific monitoring rules are in place for Privileged Service Accounts to alert your Security Operations Center (SOC) of any abnormal behavior.	
	• Service Accounts are tiered such that different accounts are used to interact with workstations, servers, and authentication servers, even for the same service.	Yes
	• There is a process in place to review at least annually the current requirements for each service associated with "Privileged" "Service Accounts" to verify the service still requires the permissions the service account has (and deprive if not).	Yes
	• None of the above/Don't know.	
EPA.2.10	Select one response: Authenticator Assurance Level (AAL) which best represents the Applicant's authentication solution(s). NIST Special Publication 800-63B defines the Authenticator Assurance Levels.	Don't know.

EPA.2.11 Use separate rows in the text box provided below for each "Privileged" "Service Account" (the number of active Privileged Service Accounts is provided in the Marsh Cyber Self-Assessment | Identity and Access Management section | question 1.6). Within each row indicate the following attributes for each "Privileged" "Service Account":

- a. The name of the account
- b. The privileges it has,
- c. The software product it supports,
- d. What hosts the service account is authenticating to, and
- e. Why those entitlements are required

EPA.2.12 Select one response: Which description below best reflects the Applicant's posture with respect to access controls for each user's workstation? For the purposes of this question, where the Applicant is using an endpoint privilege manager or other similar technology to allow users to temporarily request administrative access for certain activities, that should not be considered "admin access".

[ No user's regular, every day account is in the Administrator's group or has local admin access to their workstation. , Applicant's policy is that employees by default are not in the Administrators' group and do not have local admin access; all exceptions to the policy are documented. , Some of the Applicant's employees are in the Administrators' group or are local admins. , Don't know. ]

Applicant's policy is that employees by default are not in the Administrators' group and do not have local admin access; all exceptions to the policy are documented.

EPA.2.13	<p>Select one response: Which description best reflects the Applicant's posture with respect to access controls for member servers? This question is regarding employees' everyday user accounts; where the Applicant provisions employees with separate credentials for administrative access, those accounts should not be considered for the purposes of this question.</p> <p>[ No employees are in the Administrator's group or have local admin access to member servers. , Applicant's policy is that employees by default are not in the Administrators' group and do not have local admin access; all exceptions to the policy are documented. , Some of the Applicant's employees are in the Administrators' group or are local admins. , Don't know. ]</p>	No employees are in the Administrator's group or have local admin access to member servers.
EPA.2.14	<p>How many of the Applicant's users have persistent administrative access to servers and/or workstations other than their own? For the purposes of this question, "administrative access" means entitlements to configure, manage and otherwise support these endpoints, including through the use of a unique administrative account (separate from their everyday user account). Users who must "check out" credentials for administrative access should not be included.</p>	0
EPA.2.15	<p>Does the Applicant ingest security logs from all Domain Controllers into their SIEM solution for analysis?</p> <p>[ Yes. , No – Applicant doesn't have a SIEM or doesn't ingest security logs into SIEM. , Not Applicable - not using directory services, IdP, rights management. ]</p>	Yes.

- EPA.2.16 Select all responses that are true: What Audit Policies has the Applicant enabled on Domain Controllers?
- Audit Credential Validation (Failure)
  - Audit Process Creation (Success)
  - Audit Security Group Management (Success and Failure)
  - Audit User Account Management (Success and Failure)
  - Audit Other Account Management Events (Success and Failure)
  - Audit Sensitive Privilege Use (Success and Failure)
  - Audit Logon (Success and Failure)
  - Audit Special Logon (Success)
  - None of the above/Don't know.
  - Not applicable (not using Active Directory).
- Yes

EPA.2.17 If Applicant has any additional commentary on any specific question or response in this section, please provide below:

#### AIG | Security Monitoring and Incident Response

- EPA.3.1 Select one response: Which description best reflects the Applicant's security operations program?
- [ Applicant does not have anyone (internal or external) dedicated to monitoring security operations (a "Security Operations Center" or SOC). , Applicant has a SOC, but it's not 24 /7 (can be internal or external). , Applicant has 24/7 monitoring of security operations by a 3rd party (such as a Managed Security Services Provider). , Applicant has 24/7 monitoring of security operations internally (regardless of whether or not a 3rd party is also used). ]
- Applicant has 24/7 monitoring of security operations internally (regardless of whether or not a 3rd party is also used).

EPA.3.2	Select all responses that are true: With respect to the Applicant's security and network monitoring capabilities:	
	• Applicant uses a "Security Information and Event Monitoring" or SIEM tool to correlate the output of multiple security tools.	Yes
	• Applicant monitors network traffic for anomalous and potentially suspicious data transfers.	Yes
	• Applicant monitors for performance and storage capacity issues on all servers (such as high memory or processor usage, or no free disk space).	Yes
	• Applicant has tools to monitor for data loss (DLP) and they are in blocking mode.	
	• Applicant has tools to monitor for data loss (DLP), but they are not in blocking mode.	Yes
	• None of the above/Don't know.	
EPA.3.3	What is the Applicant's average time to triage and contain security incidents of workstations for the most recent completed quarter?	Applicant does not track this metric/Don't know.
EPA.3.4	What percentage of the Applicant's "Vital Assets" are being logged and forwarded to a SIEM solution?	100
EPA.3.5	How long does the Applicant's SIEM solution retain logs?	90 days or more.
EPA.3.6	Select all responses that are true: With respect to how the Applicant validates the efficiency and effectiveness of security controls:	
	• Applicant uses Breach and Attack Simulation (BAS) software to verify the effectiveness of security controls.	Yes
	• Applicant has a "red team" on staff to test security controls, or at least annually engages experts to perform a penetration test focused on internal systems.	Yes
	• Applicant has engaged an external party to simulate threat actors and test security controls in the last year.	Yes
	• None of the above.	

EPA.3.7	Select all responses that are true: With respect to the Applicant's incident response program and procedures: <ul style="list-style-type: none"><li>• Applicant has a documented incident response plan.</li><li>• Applicant's incident response plan includes a playbook specifically for a ransomware incident at the organization.</li><li>• Applicant's incident response plan includes a playbook specifically for a ransomware incident of 3rd parties/MSPs.</li><li>• Applicant's incident response plan includes contact of law enforcement once a ransomware incident is confirmed.</li><li>• Applicant's response plan includes a process to resume business operations by restoration of known clean backups.</li><li>• None of the above.</li></ul>	Yes Yes  Yes Yes
EPA.3.8	Does the Applicant have a documented process to respond to phishing incidents (whether targeted specifically at the Applicant or its employees, or not)? [ Yes , No ]	No
EPA.3.9	If Applicant has any additional commentary on any specific question or response in this section, please provide below:	

#### AIG | Risk Management

EPA.4.1	Does the Applicant have a vulnerability scanning program which identifies and manages vulnerabilities across "Vital Assets"? [ Yes , No ]	Yes
---------	--	-----



EPA.4.2	Select all responses that are true: With respect to the factors the Applicant uses to prioritize patching:	
	• Common Vulnerability Scoring System (CVSS) score.	Yes
	• Correlation with whether the vulnerability affects the Applicant's "Vital Assets".	Yes
	• Generic threat intelligence (e.g., that threat actors are exploiting a given vulnerability; this includes tools like CISA's Known Exploited Vulnerability Catalog).	Yes
	• Threat intelligence specific to the Applicant (including intelligence that threat actors may be targeting the Applicant specifically via exploitation of a certain vulnerability, or data from the Applicant's environment which indicates where threat actors are focused).	
	• None of the above/Don't know.	
EPA.4.3	What is the Applicant's target time to deploy the highest priority patches?	3-7 days.
EPA.4.4	What is the Applicant's compliance rate with its own standards for deploying the most important patches in the most recent completed quarter?	>95%
EPA.4.5	Select all responses that are true: With respect to the Applicant's policies for the use of organizational IT assets:	
	• The Applicant has an "Acceptable Use Policy" (AUP) outlining users' obligations and constraints.	Yes
	• The AUP describes consequences for policy violations.	Yes
	• Users are disallowed from surfing social media platforms from organizational assets except where this is a defined business need.	
	• Users are disallowed from accessing personal email from organizational assets.	
	• Administrators are explicitly disallowed from surfing the internet or accessing personal email from their privileged accounts.	
	• Users and administrators are responsible for keeping their computer and accounts safe from common risks or issues.	Yes
	• Users and administrators are required to report suspected violations.	Yes
	• None of the above/Don't know.	

EPA.4.6	Select all responses that are true: With respect to the Applicant's capabilities to monitor for risky behavior and malicious insiders:	
	• Applicant has an insider threat program.	
	• Applicant monitors for when a user or administrator account sets an insecure password.	
	• Applicant monitors for when "Privileged" accounts access unauthorized websites and services.	
	• Applicant monitors for unauthorized remote access to "Vital Assets".	Yes
	• Applicant monitors both user and administrator accounts for communication with known malicious websites, IP addresses, and other well-known threat group resources.	Yes
	• None of the above/Don't know.	
EPA.4.7	If Applicant has any additional commentary on any specific question or response in this section, please provide below:	

#### AIG | Phishing Defense

EPA.5.1	Select all responses that are true: With respect to the Applicant's capabilities for mitigating phishing incidents:	
	• Applicant provides security awareness training, including phishing awareness training, to employees at least annually.	Yes
	• Applicant uses simulated phishing attacks to test employees' cybersecurity awareness at least annually.	
	• Where the Applicant is conducting simulated phishing attacks, the success ratio was less than 15% on the last test (less than 15% of employees were successfully phished).	
	• Applicant 'tags' or otherwise marks e-mails from outside the organization.	Yes
	• Applicant has a documented process to report suspicious e-mails to an internal security team to investigate and publishes the process to users.	Yes
	• None of the above/Don't know.	

- EPA.5.2 Select all responses that are true: With respect to the Applicant's capabilities to block potentially harmful websites and/or email:
- Applicant uses an e-mail filtering solution which blocks known malicious attachments and suspicious file types, including executables. Yes
  - Applicant uses an e-mail filtering solution which blocks suspicious messages based on their content or attributes of the sender.
  - Applicant uses a web-filtering solution which stops employees from visiting known malicious or suspicious web pages. Yes
  - Applicant blocks uncategorized and newly registered domains using web proxies or DNS filters.
  - Applicant uses a web-filtering solution which blocks known malicious or suspicious downloads, including executables. Yes
  - Applicant's e-mail filtering solution has the capability to run suspicious attachments in a sandbox. Yes
  - Applicant's web filtering capabilities are effective on all organization assets, even if the asset is not on the organization's network (e.g., assets are configured to utilize cloud-based web filters or require a VPN connection to browse the internet). Yes
  - None of the above/Don't know.

EPA.5.3 If Applicant has any additional commentary on any specific question or response in this section, please provide below:

AIG | Malware Defense

EPA.6.1 Select all responses that are true: With respect to the Applicant's endpoint security tool's capabilities:

- Applicant's endpoint security solution includes antivirus with heuristic capabilities.
- Applicant uses endpoint security tools with behavioral-detection and exploit-mitigation capabilities.
- Applicant uses an endpoint threat detection and response (ETDR or EDR) tool which does all the following: monitors for threat indicators; identifies patterns which match known threats; automatically responds by removing or containing threats; alerts security personnel of incidents; provides forensic and analysis capabilities to allow analysts to perform threat hunting activities.
- Applicant implements application controls across workstations to only allow for execution of authorized applications. Unauthorized applications are blocked, and the list of authorized applications is reassessed at least bi-annually.
- Applicant has an internal group and/or MSSP which monitors the output of endpoint security tools and investigates any anomalies.
- None of the above/Don't know.

EPA.6.2 Select all responses that are true: With respect to the Applicant's deployment of its endpoint security tool(s) (as described above):

- |  |     |
|--|-----|
| • Applicant's endpoint security tool(s) is/are deployed on all workstations & laptops; all exceptions are documented.  | Yes |
| • Applicant's endpoint security tool(s) is/are deployed on all servers (excluding hypervisor hosts); all exceptions are documented.                                  | Yes |
| • Applicant's endpoint security tool(s) is/are deployed on all mobile devices (including tablets, phones, etc. but excludes laptops); all exceptions are documented. |     |
| • None of the above/Don't know.  |     |

EPA.6.3	Select all responses that are true: With respect to the Applicant's configuration of its endpoint security tool(s) (as described above):	
	• For those tools which require updated definitions, such tools are updating at least daily.	Yes
	• Tool(s) is/are configured to block (vs. just notify of) suspected malicious processes /files.	Yes
	• Tool(s) is/are configured to find unmanaged assets, which are addressed at least weekly.	
	• Anti-tamper features are enabled.	Yes
	• None of the above/Don't know.	
EPA.6.4	Identify the endpoint security tool(s) used (please be as specific as possible, e.g., "Falcon Prevent, Insight and Overwatch", not "CrowdStrike"):	Trend Micro Vision One
EPA.6.5	Select all responses that are true: With respect to the Applicant's capabilities to limit lateral movement:	
	• Applicant has segmented the network by geography (i.e., traffic between offices in different locations is denied unless required to support a specific business requirement).	
	• Applicant has segmented the network by business function (i.e., traffic between assets supporting different functions - HR and Finance for example - is denied unless required to support a specific business requirement).	
	• Applicant has implemented host firewall rules that prevent the use of RDP to log into workstations.	
	• Applicant has configured all service accounts to deny interactive logons.	
	• None of the above/Don't know.	Yes
EPA.6.6	Has the Applicant conducted an exercise simulating the tactics, techniques, and procedures of ransomware actors in the last year? [ Yes , No ]	Yes
EPA.6.7	If Applicant has any additional commentary on any specific question or response in this section, please provide below:	

- Applicant utilizes an MSP for administration of "Vital Assets".

- Applicant utilizes an MSP for security operations.

Yes

- Applicant utilizes an MSP for data backup and recovery.

- Applicant utilizes an MSP for cloud transformation.

- Applicant utilizes an MSP for software development.

- Applicant provides third parties persistent ("always on") access to corporate resources (access does not require Applicant's authorization).

Yes

- None of the above/Don't know.

EPA.7.2 Does the Applicant have a process or technical solution to identify, assess, manage, monitor, and reduce the risks from MSPs and third parties?

Yes

[ Yes , No ]

EPA.7.3 If Applicant has any additional commentary on any specific question or response in this section, please provide below:

## AI G | Perimeter and Internet Defense

---

EPA.8.1	Select all responses that are true: With respect to the Applicant's capabilities to secure externally-exposed systems, including internet-facing systems:	
	• Applicant maintains an inventory of externally-exposed assets.	Yes
	• Applicant performs regular vulnerability scans of externally-exposed assets.	Yes
	• Applicant has a Web Application Firewall (WAF) in front of all externally-exposed applications, and it is in blocking mode.	Yes
	• Applicant scans externally-exposed assets for vulnerabilities at least monthly.	Yes
	• Applicant uses an external service to monitor its attack surface (internet-facing systems).	Yes
	• Applicant disables or blocks on externally-exposed systems those ports, services, and protocols known to allow the spread of ransomware, including, but not limited to RDP, SMBv1, and SMBv2.	Yes
	• Applicant's externally-exposed assets are segmented within a demilitarized zone (DMZ), and the DMZ is not directly routable to the corporate network. Users requiring access to DMZ services are routed to the internet for access.	Yes
	• Applicant can detect and respond to threats through endpoint and network monitoring solutions.	Yes
	• None of the above/Don't Know.	
EPA.8.2	If Applicant has any additional commentary on any specific question or response in this section, please provide below:	

## Media

#	Prompt	Response
<b>Media</b>		
ME.1.1	<p>The organization's media activities include: (select all that apply)</p> <ul style="list-style-type: none"> <li>• Television</li> <li>• Radio</li> <li>• Print</li> <li>• The organization's website(s). (If selected, please list domain names in commentary box)</li> <li>• Internet advertising</li> <li>• Social media</li> <li>• Marketing materials</li> <li>• Audio or video streaming</li> <li>• Other (If selected, please describe in commentary box)</li> </ul>	
ME.1.2	<p>The organization has a formal review process conducted with legal counsel to screen and clear material for intellectual property and compliance prior to any publication, broadcast, distribution, or use.</p> <p>[ Yes , No ]</p>	
ME.1.3	<p>The formal review process includes any published or broadcast material, including digital content, and titles, trademarks and/or service marks for all domain names, service names, designs, and logos.</p> <p>[ Yes , No ]</p>	
ME.1.4	<p>The organization allows third-party generated content to be displayed on its website(s).</p> <p>[ Yes , No ]</p>	
ME.1.5	<p>Protections with third-party content providers and contributors – including freelancers, independent contractors, and other talent – include: (select all that apply)</p> <ul style="list-style-type: none"> <li>• Written permissions or releases are obtained.</li> <li>• Indemnification or hold harmless agreements in the organization's favor are required.</li> </ul>	



- ME.1.6      The organization has established an  
employee education program for issues  
relating to intellectual property, defamation,  
privacy, and information gathering.  
[ Yes ,   No ]
- ME.1.7      Please describe the policies and procedures  
for addressing controversial or potentially  
defamatory or infringing content on the  
organization's website(s).

## Tech Errors and Omissions

#	Prompt	Response
<b>Technology Products and Services</b>		
TE.1.1	Indicate the products and services the organization offers, and the annual revenues (nominal or as a percentage) associated with each service.  Organization's Associated Annual Revenues  Cloud Services (including Platform, Software and Infrastructure)  Managed Security Service Provider (MSSP)  Custom Software Development and Design  Packaged Software Development and Design  Software Services (including Sales, Installation and Maintenance)  Hardware Services (including Sales, Installation and Maintenance)  Manufacturing and Design (including Hardware, Components and Equipment)  Data and Transaction Processing  IT Systems Consulting, Analysis and Design  Business Process Outsourcing  Telecommunication Services  Other	

## Business Structure

---

TE.2.1      The organization has made significant changes in business activities/structure within the last 12 months, or anticipates significant changes in business activities/structure within the next 12 months. If yes, please provide detail in commentary.  
[ Yes ,   No ]

### Client Contracts

TE.3.1      The number of clients the organization currently has:

TE.3.2      The average contract size of the organization with current clients:

TE.3.3      The length of the organization's average contract:

TE.3.4      Indicate the contract value and duration of the organization's top 5 clients.

Client's Name

Client 1

Client 2

Client 3

Client 4

Client 5

Description of Client's Services

Client 1

Client 2

Client 3

Client 4

Client 5

Contract Value

Client 1

Client 2

Client 3

Client 4

Client 5

Contract Duration

Client 1

Client 2

Client 3

Client 4

Client 5

- TE.3.5      The organization's percentage of professional services provided by written contract is:  
[ 0-24% ,   25-49% ,   50-74% ,   75-100% ,  
N/A ]
- TE.3.6      The following risk mitigation clauses are included in your standard terms and conditions: (select all that apply)
- Customer Acceptance/Final Sign Off
  - Force Majeure
  - Limitation of Liability
  - Monetary Cap on Direct Damages
  - Exclusion of Consequential Damages
  - Hold Harmless Agreements
  - Payment Terms
  - Disclaimer of Warranties
  - Indemnification Clause
  - Dispute Resolution or Escalation Procedure
  - Project Phases/Milestones
- TE.3.7      The percentage of contracts that the organization enters into with standard terms and conditions and without modifications is:  
[ 0-24% ,   25-49% ,   50-74% ,   75-100% ,  
N/A ]

- 
- TE.3.8 The organization's customer facing colleagues are able to modify standard contractual terms and conditions within certain parameters.  
[ Yes , No , N/A ]
- TE.3.9 Further modifications to standard contract agreements are approved by legal counsel.  
[ Yes , No , N/A ]
- TE.3.10 The organization's policy is not to enter into contracts with uncapped liability.  
[ Yes , No , N/A ]

### Subcontracting

- TE.4.1 The percentage of the organization's services involving subcontracting is: (e.g. independent contractors, temporary workers, or other non-employees)  
[ 0-1% , 2-10% , 11-50% , >50% ]
- TE.4.2 The percentage of subcontractors with whom the organization has written contracts is:  
[ 0-24% , 25-49% , 50-74% , 75-100% , N/A ]
- TE.4.3 Written contracts for agreements between subcontractors:
- Uses standardized contract language.
  - Contains indemnification or hold harmless agreements in favor of your organization.
  - Identifies work product as 'work made for hire' or includes other provisions for the ownership of intellectual property.
  - Includes requirements to follow the organization's standard cybersecurity control protocols.
- TE.4.4 The organization requires subcontractors to carry: (select all that apply, and indicate standard insurance limit requirements in comments)
- Professional liability insurance
  - Cyber insurance
- TE.4.5 Please describe the organization's formal vetting procedure for subcontractors.

### Quality Control

- 
- TE.5.1 The organization has an escalation procedure for customer or product-support complaints. If yes, please describe your escalation procedure.  
[ Yes , No ]
- TE.5.2 The organization uses the following practices in quality control and customer support procedures. (select all that apply)
- Alpha and Beta Testing Procedures
  - Vendor or VAR Certification Process
  - Final Customer Sign off Requirements
  - User Acceptance Testing Measures
  - Documented Project Milestone Procedures
  - 24/7 Customer Support
  - Pre-Release Screening for Design Errors /Flaws
  - Documented Customer Complaint /Escalation Process
  - Written Functional Specification Requirements
  - Internal Post Project Review Procedures
  - Written Product Recall Process
  - Other

### Intellectual Property Rights

- TE.6.1 The organization has written policies and procedures in place for:
- Auditing the organization's use of software licenses.
  - Avoiding copyright infringement with regard to software/computer code.
  - Responding to allegations of copyright infringement with regard to software /computer code.
  - Determining if open source code is used during the organization's software development efforts.
  - Other formal safeguard procedure against infringing on IP. (describe below)

- TE.6.2      Those who provide software code to the organization, including developers and independent contractors, are required to:
- Assign or license the Applicant their rights to the use of the code.
  - Warrant that their work does not violate another party's IP rights.
  - Indemnify the Applicant when an IP infringement claim is made against them based on the code provided.

## Operational Technology

#	Prompt	Response
<b>Access Control</b>		
OT.1.1	Does your organization have a policy to govern remote and third party access for employees, contractors and third parties? [ Yes , No ]	
OT.1.2	Your OT environment is segmented from your Information Technology (IT) environments in the following ways: (select all that apply) <ul style="list-style-type: none"><li>• Unidirectional Security Gateways</li><li>• VLANs</li><li>• DMZs</li><li>• Other</li></ul>	
OT.1.3	Can employees remotely access the OT environment [ Yes , No ]	
OT.1.4	Do you permit employees remote access to your OT environment? [ Yes , No , N/A ]	
OT.1.5	Can third-parties remotely access the OT environment? [ Yes , No ]	
OT.1.6	Is MFA enforced for third-party remote access to the OT environment? [ Yes , No , N/A ]	
OT.1.7	Does your organization monitor and alert when ICS, SCADA, and OT administrative credentials are used for non-administrative functions? [ Yes , No ]	



- 
- OT.1.8 Does your organization scan all enterprise devices remotely logging into the organization's ICS, SCADA, and OT network prior to accessing the ICS, SCADA, and OT network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices?  
[ Yes , No ]
- OT.1.9 Where possible, does your organization configure access for all ICS, SCADA, and OT accounts through as few centralized points of authentication as possible, including network, security, and cloud systems?  
[ Yes , No ]
- OT.1.10 How do you manage domain controllers?
- OT.1.11 Do you block internet access to domain controllers?  
[ Yes , No ]
- OT.1.12 Do you maintain a list of assets which are under the scope of Domain controller and which are not?  
[ Yes , No ]
- OT.1.13 Does your organization manage OT credentials separately from IT credentials? ie. Are there separate credentials for IT versus OT users.  
[ Yes , No ]

#### ICS Network / Endpoint Monitoring

- OT.2.1 Does your organization utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur within your organizations ICS, SCADA, and OT environments?  
[ Yes , No ]

- 
- OT.2.2 Does your organization configure monitoring systems to record network packets passing through the boundary at each of the organization's ICS, SCADA, and OT network boundaries?  
[ Yes , No ]
- OT.2.3 Does your organization deploy network-based Intrusion Detection Systems (IDS) sensors within ICS, SCADA and OT environments to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's ICS, SCADA and OT network boundaries?  
[ Yes , No ]
- OT.2.4 For your critical ICS, SCADA, and OT, does your organization enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring)?  
[ Yes , No ]
- OT.2.5 Does your organization ensure that all ICS, SCADA, and OT accounts have an expiration date that is monitored and enforced?  
[ Yes , No ]
- OT.2.6 Does your organization use a network based data loss prevention (DLP) solution to monitor and control the flow of data within the ICS, SCADA, and OT environment?  
[ Yes , No ]
- OT.2.7 Does your organization monitor attempts to use deactivated ICS, SCADA, and OT accounts through audit logging?  
[ Yes , No ]
- OT.2.8 For your critical ICS, SCADA, and OT assets, does your organization receive an alert when ICS, SCADA, and OT users deviate from normal login behavior (such as unusual login hours, login duration, login from unexpected regions, inconsistent login frequency, and simultaneous logins)?  
[ Yes , No ]

---

OT.2.9 Does your organization employ an Endpoint detection and response on supported workstations, servers and endpoints?  
[ Yes , No ]

OT.2.10 Does your OT security monitoring feed into a Security Operations Center?  
[ Yes , No ]

### Business Continuity & Incident Response Planning

OT.3.1 Do you have a documented Business continuity/Disaster recovery Plan? How frequently is it reviewed? Does your Business Continuity Plan account for plans to recover from an ICS\_SCADA\_OT cybersecurity event?

OT.3.2 Does your organization use any of the following techniques for ICS\_SCADA\_OT data recovery? (Please select all that apply)

- Where applicable, ensure that all system data is automatically backed up on a regular basis
- Where applicable, ensure that configuration exports are conducted on a regular basis
- On a regular basis, perform system restoration exercises to ensure that the backups are properly working
- Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network
- Ensure that system backups and recovery procedures are documented
- In cases where devices are not capable of complete backups, all software, settings, and configurations are captured in order to perform a restoration process

OT.3.3 Does your organization ensure that all ICS, SCADA, and OT backups have at least one backup destination that is not continuously addressable through operating system calls?  
[ Yes , No ]

- OT.3.4 As related to ICS\_SCADA\_OT, does your organization use any of the following incident response and management techniques? (Please select all that apply)
- Written incident response plans define roles of personnel and phases of incident handling /management
  - Job titles and duties for handling incidents are assigned to certain individuals and ensure tracking and documentation occur throughout the incident
  - Designated management personnel, as well as backups, who will support the incident handling process
  - Assemble and maintain information on third-party contact information to be used for reporting an security incident
  - The Incident Response plan has been reviewed and approved by ICS Operational Leadership
  - Response team are familiar with escalation procedure for OT incidents
  - Response teams are thoroughly familiar with the risks inherent to the ICS environment
  - Response team are thoroughly familiar with the mitigations to prevent secondary damage that may impact operational safety and protection of personnel, equipment, information, and a myriad of other dependent and interdependent factors.
  - Create incident scoring and prioritization schema based on known or potential impact
  - At least once a year, the business conducts cybersecurity incident tabletop exercises that include threats to ICS\_SCADA\_OT
  - These tabletop exercises also include ransomware as a potential threat to ICS\_SCADA\_OT
- OT.3.5 Who is authorized to respond to incidents? (select all that apply)
- MSSP
  - SOC
  - Other

### Incident Response Planning

---

OT.4.1 Does the organization use uninterruptable power supplies? If yes, for how many sites /facilities?  
[ Yes , No ]

### Internet of Things

OT.5.1 Does your organization utilize IoT devices? (If responding yes to this question please fill out questions 2-11)  
[ Yes , No ]

OT.5.2 Does your organization use any of the following techniques to control the use of Critical\_IoT administrative privileges? (Please select all that apply)

- Default passwords are changed to something unique
- Administrative accounts or accounts controlling a device use unique accounts with dedicated administrative passwords.
- Administrative accounts for management applications use unique passwords
- If possible, unsuccessful administrative account login attempts are logged and alerted.

OT.5.3 Does your organization maintain documented security configurations for Critical\_IoT?  
[ Yes , No ]

OT.5.4 Does your organization verify that updates are regularly applied to Critical\_IoT devices?  
[ Yes , No ]

OT.5.5 As related to Critical\_IoT, does your organization log inbound and outbound traffic for the discovery of malware infections?  
[ Yes , No ]

OT.5.6 Does your organization perform any of the following in regards to Critical\_IoT assets? (Please select all that apply.)

- Conduct at least monthly critical risk assessments to identify active ports, services, and protocols running on the critical assets
- After each risk assessment ensure that only expected and approved network ports, protocols, and services are running on each device
- Apply firewalls or port filtering tools on systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed
- Place firewalls in front of any critical systems to verify and validate the traffic going to the server and any unauthorized traffic is blocked and logged
- Prevent Critical\_IoT assets from being directly accessed via the internet

OT.5.7 Does your organization regularly back up Critical\_IoT data to approved backup locations?  
[ Yes , No ]

OT.5.8 Does your organization regularly perform tests of restoring Critical\_IoT from backed up data?  
[ Yes , No ]

OT.5.9 For your Critical\_IoT, does your organization require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication?  
[ Yes , No ]

OT.5.10 For your Critical\_IoT, does your organization scan all enterprise devices remotely logging into the organization's network prior to accessing the network?  
[ Yes , No ]

- OT.5.11 Does your organization have process for monitoring and disabling accounts in regards to your Critical\_IoT?  
(Please select all that apply)
- An automated process for revoking system access by disabling accounts immediately upon termination or employee changes responsibilities
  - Disable any account that is not associated with a business process or business owner
  - Automatically disable dormant accounts after a set period of inactivity
  - Ensure all accounts have an expiration date that is enforced
  - Monitor attempts to access deactivated accounts
  - Alert when users deviate from normal login behavior

#### Inventory / Asset Visibility

- OT.6.1 Does your organization use any of the following techniques to inventory and control ICS\_SCADA\_OT hardware assets ? (Please select all that apply.)
- Maintain an accurate and up-to-date inventory of new and old devices from multiple vendors, including up-to-date technical drawings
  - Ensure that all equipment acquisitions and system modifications follow an approval process and the technical drawings are updated
  - Immediate removal of unauthorized equipment

- OT.6.2 Does your organization use any of the following techniques to inventory and control ICS\_SCADA\_OT software assets? (Please select all that apply)
- Maintain an up-to-date list of recommended and supported software and versions, from the ICS manufacturers and vendors, that are required for each system.
  - Forecast operating systems and application lifecycle cost in alignment with typical COTS (commercial off the shelf software) End of Life and End of Support (EoL/EoS) Notifications.
  - Ensure cybersecurity requirements and secure development lifecycle are a consideration within procurement/sourcing processes.

### Network Architecture

- OT.7.1 Does your organization physically or logically segregate ICS, SCADA, and OT assets from the rest of the organization?  
[ Yes , No ]
- OT.7.2 Are there any dual homed computers in the ICS architecture ( ie. Dual homed means having infrastructure such as servers in both IT and OT environments)?  
[ Yes , No ]
- OT.7.3 Are emergency shutdown systems segregated from control systems and sensing functions?  
[ Yes , No ]

### Network Security

- OT.8.1 For your critical ICS\_SCADA\_OT assets does your organization enable anti-exploitation features, deploy appropriate toolkits that offer additional malware protection, and/or use ICS\_SCADA\_OT firewalls to block malicious activity?  
[ Yes , No ]



- 
- OT.8.2 Does your organization leverage the use of wireless networks and technology within the ICS\_SCADA\_OT environment? (if yes, then please answering the Wireless Access Control questions below.)  
[ Yes , No ]
- OT.8.3 Does your organization use any of the following techniques to track, control, prevent, and correct the security use of wireless local area networks (WLANS), access points, and wireless client systems within your ICS\_SCADA\_OT environment?
- Perform regular risk assessments to understand how a wireless incident may impact personal and functional safety, lead to ICS disruption, damage, or destruction of digital and physical products and services
  - Ensure wireless ICS system utilizing Public Key Infrastructure (PKI), enforce expiration dates, non-repudiation and certificate chains validation, and revocation
  - Ensure wireless (including cellular, sat, etc.) based ICS systems do not fail open when jammed
  - Ensure wireless (including cellular, sat, etc.) based ICS networks are controlled/private networks
  - Ensure software security patches and product upgrades are applied throughout the wireless infrastructure and products are kept current throughout their lifecycle
  - If wired connection is more appropriate, then use that connection in place of wireless
  - Where possible, limit wireless signal strength and range to what is necessary for the application in order to reduce the potential for remote accessibility of the connection from outside a security perimeter
  - Ensure that rogue wireless discovery tools are set to alert only
  - Ensure that all wireless connections are persistent, encrypted, defined point-to-point or point-to-multipoint wireless configuration
  - Ad hoc or guest connections are not permitted

- 
- OT.8.4 Does your organization prevent ICS\_SCADA\_OT assets from being directly accessed via the internet?  
[ Yes , No ]
- OT.8.5 Does your organization apply host-based firewalls or port filtering tools on systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed?  
[ Yes , No ]
- OT.8.6 Does your organization place application firewalls in front of any critical systems to verify and validate the traffic going to the server and any unauthorized traffic is blocked and logged?  
[ Yes , No ]
- OT.8.7 Does your organization ensure that network firewalls, within the ICS\_SCADA\_OT environment, are configured to deny by default?  
[ Yes , No ]
- OT.8.8 Does your organization use any of the following techniques to track, control, prevent, and correct secure access to critical ICS\_SCADA\_OT assets according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification. (select all that apply)
- ICS systems are physically and logically network segmented
  - Enable firewall filtering between ICS and non-ICS networks to ensure that only authorized systems are able to communicate with ICS systems necessary to fulfill their specific responsibilities
  - Encrypt all sensitive information in transit between ICS and non-ICS networks
  - Enforce detailed audit logging for access to sensitive ICS data or changes to sensitive ICS data
  - Enable access control lists to restrict data and system access to only authorized individuals and systems

- 
- OT.8.9 For your ICS\_SCADA\_OT, does your organization deploy web application firewalls (WAFs) or application firewalls that inspect traffic flowing to the ICS\_SCADA\_OT web application?  
[ Yes , No ]
- OT.8.10 Does your organization configure the ICS, SCADA, and OT servers to automatically conduct an anti-malware scan of removable media when inserted or connected?  
[ Yes , No ]
- OT.8.11 Does your organization configure the assets hosting ICS, SCADA, and OT assets to not auto-run content from removable media?  
[ Yes , No ]
- OT.8.12 Does your organization configure systems not to write data to external removable media, if there is no business need for supporting such devices.  
[ Yes , No ]

### Patch Management

- OT.9.1 How does your organization patch OT systems ?  
[ Manual , Automated , N/A ]
- OT.9.2 What is the frequency for installation patches?
- OT.9.3 For your ICS\_SCADA\_OT, does your organization maintain separate environments for production and non-production systems? Developers should not have unmonitored access to production environments.  
[ Yes , No ]

### Penetration Testing

- OT.10.1 Does your organization use any of the following techniques for ICS\_SCADA\_OT penetration testing? (select all that apply)
- Leveraging both the internal OT team and specialized third parties to conduct regular security assessments to identify a greater diversity of vulnerabilities and attack vectors that can be used to breach security of ICS systems
  - Ensuring that personnel conducting vulnerability assessments are skilled in working within ICS environments to reduce the possibility of inadvertent negative impact to operations
  - Including tests for the presence of unprotected system information, data leakage, and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, documents containing passwords, or other information critical to system operation
  - Using results from vulnerability scans and security assessments in concert
  - Ensuring personal and functional safety, as well as protecting digital and physical assets throughout the testing process
- OT.10.2 Ensuring personal and functional safety, as well as protecting availability of operations, the organization conducts intrusive penetration testing on: (select all that apply)
- The whole OT environment
  - Specific systems only
  - Specific vulnerabilities only
  - Red team/blue team exercise
- OT.10.3 Has your organization created a test bed that mimics a production environment for specific ICS, SCADA, and OT penetration tests and Red Team exercises to prevent from adversely impacting the production environment?  
[ Yes , No ]

- OT.10.4 Does your organization deploy automated software update tools in order to ensure that your ICS, SCADA, and OT are running the most recent security updates provided by the software vendor, and/or does your organization retroactively remediate all high severity vulnerabilities (and OWASP-ICS /SCADA top 10 vulnerabilities) after each vulnerability scan?  
[ Yes , No ]

### Physical Security

- OT.11.1 How is physical access controlled to critical devices?

### Policies, Standards and Procedures

- OT.12.1 Does your organization have an ICS\_SCADA\_OT specific cybersecurity policy?  
[ Yes , No ]
- OT.12.2 Does your organization employ dedicated personnel whose primary responsibility is ICS\_SCADA\_OT cybersecurity?  
[ Yes , No ]
- OT.12.3 If yes to #2, are the dedicated ICS\_SCADA\_OT personnel part of the IT Security organization?  
[ Yes , No , N/A ]
- OT.12.4 If yes to #2, are they part of the Engineering /Operational Support organization?  
[ Yes , No , N/A ]
- OT.12.5 Is there a dedicated budget for ICS\_SCADA\_OT cybersecurity?  
[ Yes , No ]
- OT.12.6 Who is authorized to approve the budget for SCADA OT Cybersecurity every year?
- OT.12.7 Does your organization maintain documented, standard security configuration standards for all authorized ICS\_SCADA\_OT systems?  
[ Yes , No ]

- 
- OT.12.8 Does your organization keep inventory of secure images as related to ICS\_SCADA\_OT? (Please select all that apply)
- Maintain secure images or templates for all systems in the enterprise
  - Store and monitor master images and templates on secure servers
- OT.12.9 Does your organization implement any of the following security awareness and training programs for employees and contractors that interface with the ICS\_SCADA\_OT environment? (Please select all that apply)
- A completion of a security awareness program is for all visitors (Including 3rd parties: contractors, subcontractors, vendors, etc.).
  - Baseline physical and cybersecurity security education is provided to standardize knowledge, skills, and abilities (KSAs) for ICS personnel, as well as others that interface with and support ICS (e.g. IT personnel, ITOT Hybrid personnel, third-party contractors, service/support personnel, and others as appropriate).
  - Advanced immersive cybersecurity security education and training is provided to personnel expected to perform higher-risk, more advanced processes, or those who are making decisions relating to design, build, operation, and maintenance factors.
  - Standardizing on baseline and periodic measures of security KSAs including personnel capabilities assessments, required industry security certifications, security skills building roadmaps to grow personnel capabilities over time to better safeguard systems, reinforce best practices, and evolve as new risks are identified and new threats emerge.
- OT.12.10 Are the facilities under the scope of coverage designed with mechanical safety protection devices in accordance with relevant regulations and standards ( API,ISO, IEC etc.)  
[ Yes , No ]
- OT.12.11 Are the facilities under the scope of coverage compliant with international safety and security standards such as NERC?  
[ Yes , No ]
-

OT.12.12 How do you evaluate and manage the spare part requirements to resume business operations within defined time period in case of system failure.

### Vendor Management

OT.13.1 List Control systems and the Vendor which supports the systems

OT.13.2 Does your organization have in place the following?

- A maintenance and support contract with all vendors for the systems which is reviewed annually.
- The contract with vendors captures the escalation matrix of vendors which is reviewed annually.
- A documented Third party security policy to ensure the implementation security controls with respect to the services provided by the Third Party.
- Monitoring the service provided by the third party for ICS, SCADA and OT peripherals and review the services on periodic basis.
- Document the changes in the services provided by the third party in the maintenance and support contract.
- Perform risk assessment whenever there is change in the service provided by the third party and appropriate actions are taken for the closure of identified risks.
- Enforced appropriate risk-based multifactor authentication (MFA).
- Engagement with the internal security operations center to develop specific use cases for monitoring third party accesses.
- Code of Conduct
- Access management (provision/modification /revocation).
- Training

### Vulnerability Assessment

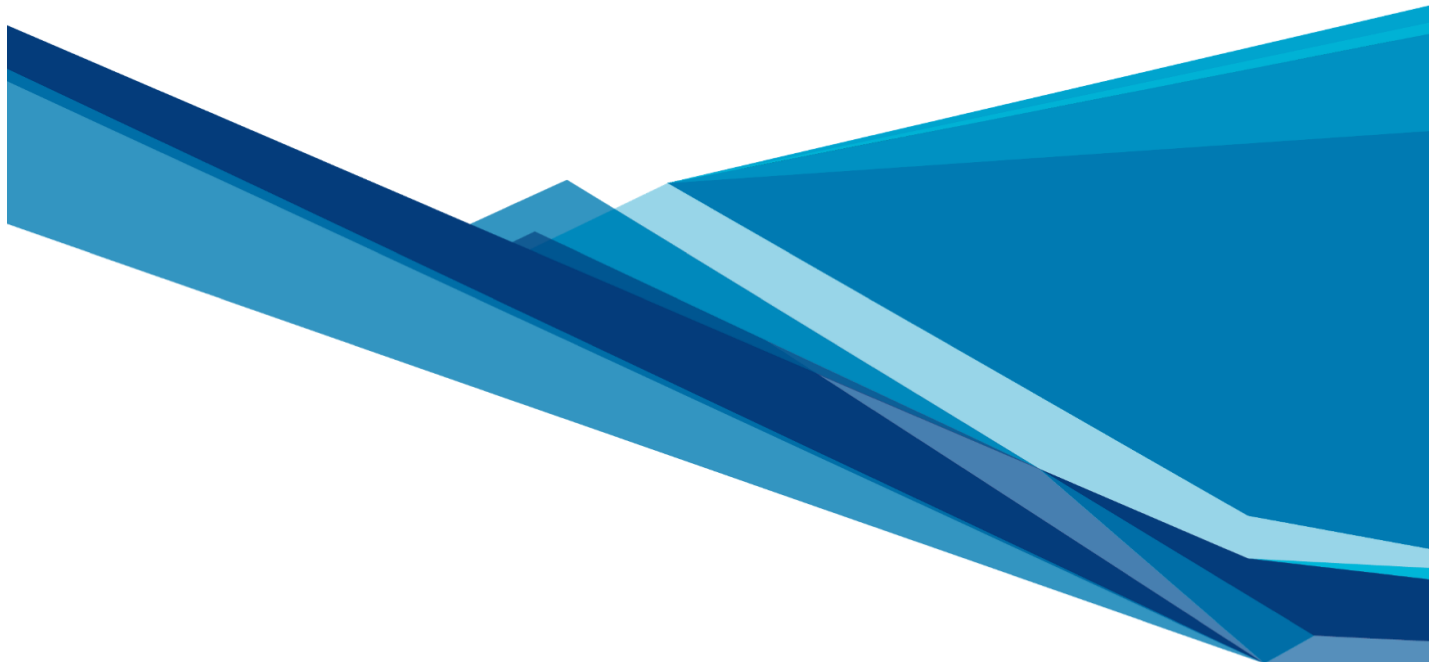
- 
- OT.14.1 Does your ICS\_SCADA\_OT environment contain legacy systems that the original manufacturer considers 'end of life' or that are no longer supported with security patches and updates?  
[ Yes , No ]
- OT.14.2 How often does your organization conduct ICS, SCADA, and OT vulnerability assessments?
- OT.14.3 Does the organization have a defined process for identifying ICS\_SCADA\_OT devices with critical vulnerabilities?  
[ Yes , No ]
- OT.14.4 Does your organization use any of the following techniques for ICS\_SCADA\_OT continuous vulnerability management? (Please select all that apply)
- Before use in production, ensure that any vulnerability scanning tool does not cause adverse conditions that could alter the integrity of the system
  - Ensure that tools do not automatically deploy software into the production environment, but only report and identify where security updates are needed
  - Utilize an OEM vulnerability reporting service to identify all known vulnerabilities on the organization's ICS
  - Utilize passive monitoring tools which identify a specific device and software version and correlate that to known vulnerabilities
  - Operating system and application updates, security patches, and service packs need to be properly regression tested to ensure availability and reliability of the system will not be adversely affected
  - Create a test bed that mimics a production environment for specific patch regression testing prior to implementing in production OT environments
- OT.14.5 Is there a defined patch management process in place for these devices?  
[ Yes , No ]





This document and any recommendations, analysis, or advice provided by Marsh (collectively, the Marsh Analysis) are intended solely for the entity identified as the recipient herein (you). This document contains proprietary, confidential information of Marsh and may not be shared with any third party, including other insurance producers, without Marsh's prior written consent. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, accounting, tax, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party with regard to the Marsh Analysis or to any services provided by a third party to you or Marsh. Marsh makes no representation or warranty concerning the application of policy wordings or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. All decisions regarding the amount, type or terms of coverage shall be your ultimate responsibility. While Marsh may provide advice and recommendations, you must decide on the specific coverage that is appropriate for your particular circumstances and financial position. By accepting this report, you acknowledge and agree to the terms, conditions and disclaimers set forth above.

Copyright © 2024 Marsh LLC. All rights reserved.



## INFORMAZIONI AGGIUNTIVE QUESTIONARIO CYBER RISKS SOGEI SPA

- **Sezione 1 -MFA:** non si richiede la multi factor authentication per tutti gli accessi da remoto (molti mercati utilizzano questo step all'entrata per la valutazione di qualunque rischio); **E' un errore visto che per tutti gli accessi c'è la MFA.**
- **Sezione 2 - EDR:** bassa la percentuale di device mobili su cui vi sono gli antimalware e che siano regolarmente patchati; possiamo a tal proposito fornire dettagli in merito a qualche remediation alternativa? Vi è in progetto un maggior controllo dei device stessi? **C'è un progetto di utilizzo del MAM entro luglio 2024.**
- **Sezione 4 - PAM:** mancanza di un PAM. Inoltre nella sezione opzionale "External partner accompaniments" non sono quantificati il numero di service account e i loro privilegi amministrativi. Inseriamo in allegato una definizione per meglio chiarire il tema. È possibile avere un approfondimento in tal senso? Sarebbe ottimale il completamento della tabella excel che inseriamo in allegato per dare un quadro completo del tema ai mercati. **Il PAM è una soluzione standard utilizzata su 11.000 server. Ulteriori informazione nella tabella Excel "Service account".**
- **Sezione 8- Cyber security awareness:** non vi è obbligatorietà nei corsi di formazione per i dipendenti; questo sarà sicuramente un punto critico nell'interrogazione dei mercati. Avete in pipeline un cambiamento in tal senso? **Abbiamo in programma di erogare un corso di cyber security awareness nei prossimi mesi (anche se non abbiamo ancora un contratto ma materiale sì), però l'obbligatorietà non deriva da una scelta nostra ma da un mandato di HR. Essendo ora la stessa direzione generale potremmo impegnarci in tal senso. In ambito sicurezza e continuità operativa nel corso del 2022 sono state erogate complessivamente 989 gg di formazione mentre nel 2023 le giornate sono state 1137. Al momento non è previsto un obbligo ma di sicuro la sicurezza è un tema all'attenzione e credo i numeri indicati ne siano una evidenza incontrovertibile.**
- **Sezione 11 - Sistemi End of life:** la mancata segregazione dei sistemi end of life è un altro tema rilevante. Anche in questo caso sarebbe necessario argomentare maggiormente in merito. **Per i sistemi in EOL abbiamo creato due nuovi ambienti denominati blue e green in cui spostiamo le applicazioni sanando le obsolescenze: nell'area blu ci vanno le applicazioni su sistemi non obsolete il cui porting non necessita di re-engineering, nell'area green ci vanno le nuove applicazioni o quelle ingegnerizzate ex-novo.**

Appendice "Account di servizio" "Privilegiato"
Nome dell'account
SOLO A TITOLO DI ESEMPIO <i>svc_cyberark</i>
oper1/oper2/oper3
cybuser
root
cybadm
Administrator
cybadm_win

Privilegi che ha
SOLO A TITOLO DI ESEMPIO: <i>Amministratore di dominio</i>
Nessun privilegio amministrativo
Nessun privilegio amministrativo
amministratore host Linux
amministratore host
amministratore sistema Windows
amministratore di dominio

[illegible]

Su quale HOST si Autentica
<i>SOLO A TITOLO DI ESEMPIO Esclusivamente controller di dominio</i>
circa 11.000 host Linux
circa 11.000 host Linux
circa 11.000 host Linux
circa 11.000 host Linux
circa 3.700 server Windows
uno per domain controller

Perché questi diritti sono richiesti
SOLO A TITOLO DI ESEMPIO
<i>DA richiesto per modificare le password degli account sensibili</i>
lettura log sui sistemi
per fare login alla macchina prima di switch root user
attività di gestione dell'host
per riconciliare l'utenza di root
attività di gestione del sistema
per riconciliare l'utenza Administrator