CYVATAR.AI

CYVATAR BELIEVES CYBERSECURITY IS A FOUNDATIONAL BUSINESS INITIATIVE

Compliance Framework

When it comes to our members' regulatory mandates, we stand by a "security-first" approach, with compliance becoming a natural byproduct of a company that is properly cyber-secure.

Cybersecurity maturity is an important component of any security and/or Enterprise Risk Management (ERM) program. Our security/ERM maturity is continuous, all while keeping our member's compliant and aligning with their regulatory obligations as a baseline maturity, while facilitating a natural progression to proven security best-practice models, such as the CIS Top 20 and NIST.

The Cyvatar Platform a unified hub for all of your security solutions and natively mapped to NIST and CIS controls. Members can track their journey to cyber maturity that in turn, streamlines and fast-tracks becoming compliant. This approach is vital in keeping pace with the continuously evolving cyber threat landscape and maintaining compliant, which is especially useful for organizations in heavily regulated industries. The extensively long, bureaucratic, and slow pace of developing these regulations often results in organizations delaying in security, when in reality, a strong cybersecurity strategy naturally allows you to become compliant.

TABLE OF CONTENTS

CERT RMM

Essential organizational practices that are necessary to manage operational resilience.

CERT RMM	DESCRIPTION	DETAILS	CYVATAR EVIDENCE	MEMBER EVIDENCE	RESPONSIBILITY	SOLUTION	COMMENTS
OTA:SG1.SP1	General SAT	Ensure that managers, system administrators and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards and procedures related to the security of those systems.	Provide list of users and training completed	____	Cyvatar	**Security Awareness Training**	____
OTA:SG4.SP1	Role-base SAT	Ensure that personnel are trained to carry out their assigned information security- related duties and responsibilities.	Provide list of users and training completed	____	Cyvatar	**Security Awareness Training**	____
OTA:SG2.SP1	Insider Threat SAT	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Provide list of users and training completed	____	Cyvatar	**Security Awareness Training**	____
RISK:SG5.SP1	Vulnerability Plan of Action	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues.	____	Shared	**Threat & Vulnerability Management**	Cyvatar assits in identify gaps that are in need of POA&Ms
KIM:SG5.SP2	Baseline Configuration	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, fIncident Response Managementware and documentation) throughout the respective system development life cycles.	Asset Inventory and Review Dates AV Status Encryption Status Disk Encryption Device Inventory	Software Development Policy Baseline Configuration Standards	Shared	**IT Asset Management/ Threat & Vulnerability Management**	____
TM:SG2.SP2	Security Configuration	Establish and enforce security configuration settings for information technology products employed in organizational systems.	Technical: screen shot of groups and membership assignment Technical: screen shot of IT Asset Management console	Documentation showing the use and implimentation of RBAC	Shared	**IT Asset Management/ Threat & Vulnerability Management**	____
TM:SG4.SP1	Access Restrictions	Define, document, approve and enforce physical and logical access restrictions associated with changes to organizational systems.	Document showing the devices covered by the IT Asset Management soultion.	____	Shared	**IT Asset Management/ Threat & Vulnerability Management**	____
TM:SG5.SP2	Equipment Sanitization	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Screenshot of santization technology beng used	____	Cyvatar	**IT Asset Management/ Threat & Vulnerability Management**	____
VAR:SG2.SP2	Vulnerability Scan	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues.	____	Cyvatar	**Threat & Vulnerability Management**	Member uses Cyvatar's Threat Vulnerability Management(Threat & Vulnerability Management) services for continuous vulnerability assessment. For internal scanning, a dedicated scanner is installed in the network and scans the network at set intravals. For external scanning, continuous scanning is also performed. The member is alerted for any high or critical vulnerabilities identified by Cyvatar and remediation is performed. By doing continuous vulnerability scanning, the time-to-detect and time-to-remediate is greatly reduced.
VAR:SG3.SP1	Vulnerabilities Remediation Strategy	Remediate vulnerabilities in accordance with risk assessments.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues.	____	Cyvatar	**Threat & Vulnerability Management**	Member uses Cyvatar's Threat Vulnerability Management(Threat & Vulnerability Management) services for continuous vulnerability assessment. For internal scanning, a dedicated scanner is installed in the network and scans the network at set intravals. For external scanning, continuous scanning is also performed. The member is alerted for any high or critical vulnerabilities identified by Cyvatar and remediation is performed. By doing continuous vulnerability scanning, the time-to-detect and time-to-remediate is greatly reduced.
VAR:SG2.SP2	Information Systems Audit Controls	Identify, report and correct information and information system flaws in a timely manner.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues. Pen test results Patch management Process and Report	____	Cyvatar	**Threat & Vulnerability Management**	Member uses Cyvatar's Threat Vulnerability Management(Threat & Vulnerability Management) services for continuous vulnerability assessment. For internal scanning, a dedicated scanner is installed in the network and scans the network at set intravals. For external scanning, continuous scanning is also performed. The member is alerted for any high or critical vulnerabilities identified by Cyvatar and remediation is performed. By doing continuous vulnerability scanning, the time-to-detect and time-to-remediate is greatly reduced.
VAR:SG3.SP1	Malicious Code Protection	Provide protection from malicious code at appropriate locations within organizational information systems.	Screenshot of anti-malware configuration settings	____	Cyvatar	**Secure Endpoint Management**	____
VAR:SG3.SP1	AV Updates/Controls Against Malware	Update malicious code protection mechanisms when new releases are available/Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	Screenshot of anti-malware configuration settings. Evidence of Antivirus Software Configuration Evidence of updated AV	Evidence of firewall configurations	Shared	**Secure Endpoint Management**	____
ADM:SG1.SP1	Automated Discovery	Employ automated capability to discover and identify systems with specific component attributes (e.g., fIncident Response Managementware level, OS type) within your inventory.	____	____	____	**IT Asset Management**	____

Center for Internet Security®

CIS 18 CONTROLS

Best practices for prioritizing your organization’s security defenses.

CIS	DESCRIPTION	DETAILS	CYVATAR EVIDENCE	MEMBER EVIDENCE	RESPONSIBILITY	SOLUTION	COMMENTS
CRITICAL CONTROL 9 Security Skills Assessment and Appropriate Training to Fill Gaps	General SAT	Ensure that managers, system administrators and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards and procedures related to the security of those systems.	Provide list of users and training completed	____	Cyvatar	**Security Awareness Training**	____
CRITICAL CONTROL 9 Security Skills Assessment and Appropriate Training to Fill Gaps	Role-base SAT	Ensure that personnel are trained to carry out their assigned information security- related duties and responsibilities.	Provide list of users and training completed	____	Cyvatar	**Security Awareness Training**	____
CRITICAL CONTROL 9 Security Skills Assessment and Appropriate Training to Fill Gaps	Insider Threat SAT	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Provide list of users and training completed	____	Cyvatar	**Security Awareness Training**	____
CRITICAL CONTROL 2 Inventory of Authorized and Unauthorized Software. **CRITICAL CONTROL 3** Secure Configurations for Hardware and Software. **CRITICAL CONTROL 10** Secure Configurations for Network Devices such as Firewalls, Routers, and Switches.	Baseline Configuration	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, flncident Response Managementware and documentation) throughout the respective system development life cycles.	Asset Inventory and Review Dates AV Status Encryption Status Disk Encryption Device Inventory	Software Development Policy Baseline Configuration Standards	Shared	**IT Asset Management/ Threat & Vulnerability Management**	____
CRITICAL CONTROL 3 Secure Configurations for Hardware and Software. **CRITICAL CONTROL 10** Secure Configurations for Network Devices such as Firewalls, Routers, and Switches. **CRITICAL CONTROL 11** Limitation and Control of Network Ports, Protocols, and Services	Security Configuration	Establish and enforce security configuration settings for information technology products employed in organizational systems.	Technical: screenshot of groups and membership assignment Technical: screenshot of IT Asset Management console	Documentation showing the use and implimentation of RBAC	Shared	**IT Asset Management/ Threat & Vulnerability Management**	____
CRITICAL CONTROL 2 Inventory of Authorized and Unauthorized Software **CRITICAL CONTROL 3** Secure Configurations for Hardware and Software **CRITICAL CONTROL 10** Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Access Restrictions	Define, document, approve and enforce physical and logical access restrictions associated with changes to organizational systems.	Document showing the devices covered by the IT Asset Management soultion.	____	Shared	**IT Asset Management/ Threat & Vulnerability Management**	____
CRITICAL CONTROL 7 Continuous Vulnerability Management	Vulnerability Scan	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues.	____	Cyvatar	**Threat & Vulnerability Management/SEM**	Member uses Cyvatar's Threat Vulnerability Management(Threat & Vulnerability Management) services for continuous vulnerability assessment. For internal scanning, a dedicated scanner is installed in the network and scans the network at set intravals. For external scanning, continuous scanning is also performed. The member is alerted for any high or critical vulnerabilities identified by Cyvatar and remediation is performed. By doing continuous vulnerability scanning, the time-to-detect and time-to-remediate is greatly reduced.
CRITICAL CONTROL 7 Continuous Vulnerability Management	Vulnerabilities Remediation Strategy	Remediate vulnerabilities in accordance with risk assessments.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues.	____	Cyvatar	**Threat & Vulnerability Management**	Member uses Cyvatar's Threat Vulnerability Management(Threat & Vulnerability Management) services for continuous vulnerability assessment. For internal scanning, a dedicated scanner is installed in the network and scans the network at set intravals. For external scanning, continuous scanning is also performed. The member is alerted for any high or critical vulnerabilities identified by Cyvatar and remediation is performed. By doing continuous vulnerability scanning, the time-to-detect and time-to-remediate is greatly reduced.
CRITICAL CONTROL 7 Continuous Vulnerability Management **CRITICAL CONTROL 8** Audit Log Management **CRITICAL CONTROL 10** Malware Defenses **CRITICAL CONTROL 17** Incident Response Management	Information Systems Audit Controls	Identify, report and correct information and information system flaws in a timely manner.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues. Pen test results Patch management Process and Report	____	Cyvatar	**IT Asset Management**	Member uses Cyvatar's Threat Vulnerability Management(Threat & Vulnerability Management) services for continuous vulnerability assessment. For internal scanning, a dedicated scanner is installed in the network and scans the network at set intravals. For external scanning, continuous scanning is also performed. The member is alerted for any high or critical vulnerabilities identified by Cyvatar and remediation is performed. By doing continuous vulnerability scanning, the time-to-detect and time-to-remediate is greatly reduced.
CRITICAL CONTROL 7 Continuous Vulnerability Management **CRITICAL CONTROL 8** Audit Log Management **CRITICAL CONTROL 10** Malware Defenses **CRITICAL CONTROL 17** Incident Response Management	Malicious Code Protection	Provide protection from malicious code at appropriate locations within organizational information systems.	Screenshot of anti-malware configuration settings	____	Cyvatar	**Secure Endpoint Management**	____

CMMC 2.0

Protect federal contract information and controlled unclassified information.

CMMC 2.0	DESCRIPTION	DETAILS	CYVATAR EVIDENCE	MEMBER EVIDENCE	RESPONSIBILITY	SOLUTION	COMMENTS
AT.L2-3.2.1	General SAT	Ensure that managers, system administrators and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards and procedures related to the security of those systems.	Provide list of users and training completed	____	Cyvatar	**Security Awareness Training**	____
AT.L2-3.2.2	Role-base SAT	Ensure that personnel are trained to carry out their assigned information security- related duties and responsibilities.	Provide list of users and training completed	____	Cyvatar	**Security Awareness Training**	____
AT.L2-3.2.3	Insider Threat SAT	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Provide list of users and training completed	____	Cyvatar	**Security Awareness Training**	____
CA.L2-3.12.2	Vulnerability Plan of Action	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues.	____	Shared	**Threat & Vulnerability Management**	____
CM.L2-3.4.1	Baseline Configuration	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, flncident Response Managementware and documentation) throughout the respective system development life cycles.	Asset Inventory and Review Dates AV Status Encryption Status Disk Encryption Device Inventory	Software Development Policy Baseline Configuration Standards	Shared	**IT Asset Management/ Threat & Vulnerability Management**	____
CM.L2-3.4.2	Security Configuration	Establish and enforce security configuration settings for information technology products employed in organizational systems.	Technical: screenshot of groups and membership assignment Technical: screenshot of IT Asset Management console	Documentation showing the use and implimentation of RBAC	Shared	**IT Asset Management/ Threat & Vulnerability Management**	____
CM.L2-3.4.5	Access Restrictions	Define, document, approve and enforce physical and logical access restrictions associated with changes to organizational systems.	Document showing the devices covered by the IT Asset Management soultion.	____	Shared	**IT Asset Management/ Threat & Vulnerability Management**	____
MA.L2-3.7.3	Equipment Sanitization	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Screenshot of santization technology beng used	____	Cyvatar	**IT Asset Management/ Threat & Vulnerability Management**	____
MA.L2-3.7.5	Multi-factor Authentication	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	Screenshot showing Multi-factor Authentication settings	____	Cyvatar	**Identity Access Management**	____
RM.L2-3.11.2	Vulnerability Scan	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues.	____	Cyvatar	**Threat & Vulnerability Management**	____
RM.L2-3.11.3	Vulnerabilities Remediation Strategy	Remediate vulnerabilities in accordance with risk assessments.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues.	____	Cyvatar	**Threat & Vulnerability Management**	____
SC.L2-3.13.12	Remote Activation	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Screenshot of IT Asset Management configuration	____	Cyvatar	**Threat & Vulnerability Management/IT Asset Management/Secure Endpoint Management**	____
SI.L1-3.14.1	Information Systems Audit Controls	Identify, report and correct information and information system flaws in a timely manner.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues. Pen test results Patch management Process and Report	____	Cyvatar	**Threat & Vulnerability Management**	____
SI.L1-3.14.2	Malicious Code Protection	Provide protection from malicious code at appropriate locations within organizational information systems.	Screenshot of anti-malware configuration settings	____	Cyvatar	**Secure Endpoint Management**	____

HIPAA

Protecting sensitive patient health information from being disclosed without the patient’s consent or knowledge.

HIPAA	DESCRIPTION	DETAILS	CYVATAR EVIDENCE	MEMBER EVIDENCE	RESPONSIBILITY	SOLUTION	COMMENTS
HIPAA Security Section - 45 CFR 164.308(a)(5)(i)	General SAT	Ensure that managers, system administrators and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards and procedures related to the security of those systems.	Provide list of users and training completed	____	Cyvatar	**Security Awareness Training**	____
HIPAA Security Section - 45 CFR 164.308(a)(5)(i)	Role-base SAT	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Provide list of users and training completed	____	Cyvatar	**Security Awareness Training**	____
HIPAA Security Section - 45 CFR 164.308(a)(5)(ii)(B)	AV Updates/Controls Against Malware	Update malicious code protection mechanisms when new releases are available/Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	Screen shot of anti-malware configuration settings. Evidence of Antivirus Software Configuration Evidence of updated AV	Evidence of firewall configurations	Shared	**Secure Endpoint Management**	____
HIPAA Security Section - 45 CFR 164.308(a)(5)(ii)(c)	Train Workforce Members on Authentication Best Practices	Train workforce members on authentication best practices. Example topics include Multi-factor Authentication, password composition, and credential management.	Provide list of users and training completed any subject of training	____	Cyvatar	**Security Awareness Training**	____
HIPAA Security Section - 45 CFR 164.308(a)(5)(ii)(d)	Train Workforce Members on Recognizing and Reporting Security Incidents	Train workforce members to be able to recognize a potential incident and be able to report such an incident.	Provide list of users and training completed any subject of training	____	Cyvatar	**Security Awareness Training**	____

ISO27002

Implement, maintain, and improve your organization’s information security management.

ISO27002	DESCRIPTION	DETAILS	CYVATAR EVIDENCE	MEMBER EVIDENCE	RESPONSIBILITY	SOLUTION	COMMENTS
7.2.2 12.2.1	General SAT	Ensure that managers, system administrators and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards and procedures related to the security of those systems.	Provide list of users and training completed	____	Cyvatar	**Security Awareness Training**	____
7.2.2 12.2.1	Role-base SAT	Ensure that personnel are trained to carry out their assigned information security- related duties and responsibilities.	Provide list of users and training completed	____	Cyvatar	**Security Awareness Training**	____
6.1.2 14.2.8 18.2.2 18.2.3	Vulnerability Plan of Action	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues.	____	Shared	**Threat & Vulnerability Management**	Cyvatar assists in identify gaps that are in need of POA&Ms
8.1.1 8.1.2	Baseline Congifuration	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, flncident Response Managementware and documentation) throughout the respective system development life cycles.	Asset Inventory and Review Dates AV Status Encryption Status Disk Encryption Device Inventory	Software Development Policy Baseline Configuration Standards	Shared	**IT Asset Management**	____
8.1.1 8.1.2	Security Configuration	Establish and enforce security configuration settings for information technology products employed in organizational systems.	Technical: screenshot of groups and membership assignment Technical: screenshot of IT Asset Management console	Documentation showing the use and implimentation of RBAC	Shared	**IT Asset Management**	____
9.2.3 9.4.5 12.1.2 12.1.4 12.5.1	Access Restrictions	Define, document, approve and enforce physical and logical access restrictions associated with changes to organizational systems.	Document showing the devices covered by the IT Asset Management soultion.	____	Shared	**IT Asset Management**	____
11.2.4 11.2.5	Equipment Sanitization	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Screenshot of santization technology beng used	____	Cyvatar	**IT Asset Management**	____
12.6.1	Vulnerability Scan	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues.	____	Cyvatar	**Threat & Vulnerability Management**	Member uses Cyvatar's Threat Vulnerability Management(Threat & Vulnerability Management) services for continuous vulnerability assessment. For internal scanning, a dedicated scanner is installed in the network and scans the network at set intravals. For external scanning, continuous scanning is also performed. The member is alerted for any high or critical vulnerabilities identified by Cyvatar and remediation is performed. By doing continuous vulnerability scanning, the time-to-detect and time-to-remediate is greatly reduced.
12.6.1	Vulnerabilities Remediation Strategy	Remediate vulnerabilities in accordance with risk assessments.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues.	____	Cyvatar	**Threat & Vulnerability Management**	Member uses Cyvatar's Threat Vulnerability Management(Threat & Vulnerability Management) services for continuous vulnerability assessment. For internal scanning, a dedicated scanner is installed in the network and scans the network at set intravals. For external scanning, continuous scanning is also performed. The member is alerted for any high or critical vulnerabilities identified by Cyvatar and remediation is performed. By doing continuous vulnerability scanning, the time-to-detect and time-to-remediate is greatly reduced.
13.2.1	Remote Activation	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Screenshot of IT Asset Management configuration	____	Cyvatar	**IT Asset Management**	____
6.1.4 12.2.1 12.6.1 14.2.2 14.2.3 16.1.3	Information Systems Audit Controls	Identify, report and correct information and information system flaws in a timely manner.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues. Pen test results Patch management Process and Report	____	Cyvatar	**Threat & Vulnerability Management**	Member uses Cyvatar's Threat Vulnerability Management(Threat & Vulnerability Management) services for continuous vulnerability assessment. For internal scanning, a dedicated scanner is installed in the network and scans the network at set intravals. For external scanning, continuous scanning is also performed. The member is alerted for any high or critical vulnerabilities identified by Cyvatar and remediation is performed. By doing continuous vulnerability scanning, the time-to-detect and time-to-remediate is greatly reduced.
6.1.4 12.2.1 12.6.1 14.2.2 14.2.3 16.1.3	Malicious Code Protection	Provide protection from malicious code at appropriate locations within organizational information systems.	Screenshot of anti-malware configuration settings	____	Cyvatar	**Threat & Vulnerability Management**	____

NERC
CIP

NERC CIP

Standards aimed at regulating, enforcing, monitoring and managing the security of the Bulk Electric System (BES) in North America.

NERC CIP	DESCRIPTION	DETAILS	CYVATAR EVIDENCE	MEMBER EVIDENCE	RESPONSIBILITY	SOLUTION	COMMENTS
NERC-CIP-004 Personnel & Training R3	General SAT	Ensure that managers, system administrators and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards and procedures related to the security of those systems.	Provide list of users and training completed	____	Cyvatar	**Security Awareness Training**	____
NERC CIP-004 Personnel &Training R1, R2	Role-base SAT	Ensure that personnel are trained to carry out their assigned information security- related duties and responsibilities.	Provide list of users and training completed	____	Cyvatar	**Security Awareness Training**	____
NERC CIP-004 Personnel &Training R1, R2	Insider Threat SAT	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Provide list of users and training completed	____	Cyvatar	**Security Awareness Training**	____
NERC CIIP-010 Baseline Configuration Mgmt and vulnerabilty Assessments	Baseline Congifuration	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, fIncident Response Managementware and documentation) throughout the respective system development life cycles.	Asset Inventory and Review Dates AV Status Encryption Status Disk Encryption Device Inventory	Software Development Policy Baseline Configuration Standards	Shared	**IT Asset Management**	____
NERC CIIP-010 Baseline Configuration Mgmt and vulnerabilty Assessments	Security Configuration	Establish and enforce security configuration settings for information technology products employed in organizational systems.	Technical: screenshot of groups and membership assignment Technical: screenshot of IT Asset Management console	Documentation showing the use and implimentation of RBAC	Shared	**IT Asset Management**	____
NERC CIIP-010 Baseline Configuration Mgmt and vulnerabilty Assessments	Access Restrictions	Define, document, approve and enforce physical and logical access restrictions associated with changes to organizational systems.	Document showing the devices covered by the IT Asset Management soultion.	____	Shared	**IT Asset Management**	____
NERC CIIP-010 Baseline Configuration Mgmt and vulnerabilty Assessments **NERC CIP-007** Systems Security Mgmt	Vulnerability Scan	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues.	____	Cyvatar	**Threat & Vulnerability Management**	Member uses Cyvatar's Threat Vulnerability Management(Threat & Vulnerability Management) services for continuous vulnerability assessment. For internal scanning, a dedicated scanner is installed in the network and scans the network at set intravals. For external scanning, continuous scanning is also performed. The member is alerted for any high or critical vulnerabilities identified by Cyvatar and remediation is performed. By doing continuous vulnerability scanning, the time-to-detect and time-to-remediate is greatly reduced.
NERC CIP-005 Electronic Security Perimeters **NERC CIP-007** Systems Security Mgmt	Vulnerabilities Remediation Strategy	Remediate vulnerabilities in accordance with risk assessments.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues.	____	Cyvatar	**Threat & Vulnerability Management**	Member uses Cyvatar's Threat Vulnerability Management(Threat & Vulnerability Management) services for continuous vulnerability assessment. For internal scanning, a dedicated scanner is installed in the network and scans the network at set intravals. For external scanning, continuous scanning is also performed. The member is alerted for any high or critical vulnerabilities identified by Cyvatar and remediation is performed. By doing continuous vulnerability scanning, the time-to-detect and time-to-remediate is greatly reduced.
NERC CIP-005 Electronic Security Perimeters **NERC CIP-007** Systems Security Mgmt	Remote Activation	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Screenshot of IT Asset Management configuration	____	Cyvatar	**IT Asset Management**	____
NERC CIP-005 Electronic Security Perimeters **NERC CIP-007** Systems Security Mgmt	Infomation Systems Audit Controls	Identify, report and correct information and information system flaws in a timely manner.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues. Pen test results Patch management Process and Report	____	Cyvatar	**Threat & Vulnerability Management**	Member uses Cyvatar's Threat Vulnerability Management(Threat & Vulnerability Management) services for continuous vulnerability assessment. For internal scanning, a dedicated scanner is installed in the network and scans the network at set intravals. For external scanning, continuous scanning is also performed. The member is alerted for any high or critical vulnerabilities identified by Cyvatar and remediation is performed. By doing continuous vulnerability scanning, the time-to-detect and time-to-remediate is greatly reduced.
NERC CIP-005 Electronic Security Perimeters **NERC CIP-007** Systems Security Mgmt	Malicious Code Protection	Provide protection from malicious code at appropriate locations within organizational information systems.	Screenshot of anti-malware configuration settings	____	Cyvatar	**Threat & Vulnerability Management**	____
NERC CIP-005 Electronic Security Perimeters **NERC CIP-007** Systems Security Mgmt	AV Updates/Controls Against Malware	Update malicious code protection mechanisms when new releases are available/Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	Screenshot of anti-malware configuration settings. Evidence of Antivirus Software Configuration Evidence of updated AV	Evidence of firewall configurations	Shared	**Secure Endpoint Management**	____
NERC CIP-005 Electronic Security Perimeters **NERC CIP-007** Systems Security Mgmt	Automated Discovery	Employ automated capability to discover and identify systems with specific component attributes (e.g., fIncident Response Managementware level, OS type) within your inventory.	____	____	____	**IT Asset Management**	____

NIST 800-53 R4

Evolving technology and threat space, issues particular to mobile and cloud computing; insider threats; applications security; supply chain risks; advanced persistent threat; and trustworthiness, assurance, and resilience of information systems

NIST 800-53 R4	DESCRIPTION	DETAILS	CYVATAR EVIDENCE	MEMBER EVIDENCE	RESPONSIBILITY	SOLUTION	COMMENTS
AT-2	General SAT	Ensure that managers, system administrators and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards and procedures related to the security of those systems.	Provide list of users and training completed	____	Cyvatar	**Security Awareness Training**	____
AT-3	Role-base SAT	Ensure that personnel are trained to carry out their assigned information security- related duties and responsibilities.	Provide list of users and training completed	____	Cyvatar	**Security Awareness Training**	____
AT-2 (2)	Insider Threat SAT	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Provide list of users and training completed	____	Cyvatar	**Security Awareness Training**	____
CA-2 CA-5 CA-7 PL-2	Vulnerability Plan of Action	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues.	____	Shared	**Threat & Vulnerability Management**	Cyvatar assists in identify gaps that are in need of POA&Ms
CM-2(1)(3)(7)	Baseline Configuration	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, fIncident Response Managementware and documentation) throughout the respective system development life cycles.	Asset Inventory and Review Dates AV Status Encryption Status Disk Encryption Device Inventory	Software Development Policy Baseline Configuration Standards	Shared	**IT Asset Management/ Threat & Vulnerability Management**	____
CM-6(3)	Security Configuration	Establish and enforce security configuration settings for information technology products employed in organizational systems.	Technical: screenshot of groups and membership assignment Technical: screenshot of IT Asset Management console	Documentation showing the use and implimentation of RBAC	Shared	**IT Asset Management/ Threat & Vulnerability Management**	____
CM-5	Access Restrictions	Define, document, approve and enforce physical and logical access restrictions associated with changes to organizational systems.	Document showing the devices covered by the IT Asset Management soultion.	____	Shared	**IT Asset Management/ Threat & Vulnerability Management**	____
MA-2	Equipment Sanitization	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Screenshot of santization technology beng used	____	Cyvatar	**IT Asset Management/ Threat & Vulnerability Management**	____
RA-5 RA-5(5)	Vulnerability Scan	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues.	____	Cyvatar	**Threat & Vulnerability Management**	Member uses Cyvatar's Threat Vulnerability Management(Threat & Vulnerability Management) services for continuous vulnerability assessment. For internal scanning, a dedicated scanner is installed in the network and scans the network at set intravals. For external scanning, continuous scanning is also performed. The member is alerted for any high or critical vulnerabilities identified by Cyvatar and remediation is performed. By doing continuous vulnerability scanning, the time-to-detect and time-to-remediate is greatly reduced.
RA-5	Vulnerabilities Remediation Strategy	Remediate vulnerabilities in accordance with risk assessments.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues.	____	Cyvatar	**Threat & Vulnerability Management**	Member uses Cyvatar's Threat Vulnerability Management(Threat & Vulnerability Management) services for continuous vulnerability assessment. For internal scanning, a dedicated scanner is installed in the network and scans the network at set intravals. For external scanning, continuous scanning is also performed. The member is alerted for any high or critical vulnerabilities identified by Cyvatar and remediation is performed. By doing continuous vulnerability scanning, the time-to-detect and time-to-remediate is greatly reduced.
SC-15	Remote Activation	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Screenshot of IT Asset Management configuration	____	Cyvatar	**Threat & Vulnerability Management/IT Asset Management/Secure Endpoint Management**	____
SI-2 SI-3 SI-5	Information Systems Audit Controls	Identify, report and correct information and information system flaws in a timely manner.	Provide the vulnerability scan results for a sample quarter, along with status and action items for the identified issues. Pen test results Patch management Process and Report	____	Cyvatar	**Threat & Vulnerability Management**	Member uses Cyvatar's Threat Vulnerability Management(Threat & Vulnerability Management) services for continuous vulnerability assessment. For internal scanning, a dedicated scanner is installed in the network and scans the network at set intravals. For external scanning, continuous scanning is also performed. The member is alerted for any high or critical vulnerabilities identified by Cyvatar and remediation is performed. By doing continuous vulnerability scanning, the time-to-detect and time-to-remediate is greatly reduced.
SI-2 SI-3 SI-5	Malicious Code Protection	Provide protection from malicious code at appropriate locations within organizational information systems.	Screenshot of anti-malware configuration settings	____	Cyvatar	**Secure Endpoint Management**	____
SI-3	AV Updates/Controls Against Malware	Update malicious code protection mechanisms when new releases are available/Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	Screenshot of anti-malware configuration settings. Evidence of Antivirus Software Configuration Evidence of updated AV	Evidence of firewall configurations	Shared	**Secure Endpoint Management**	____
CM-8(2)	Automated Discovery	Employ automated capability to discover and identify systems with specific component attributes (e.g., fIncident Response Managementware level, OS type) within your inventory.	____	____	____	**IT Asset Management**	____

PCI

Ensuring the compliance and security of credit card transactions for payments.

PCI	DESCRIPTION	DETAILS	CYVATAR EVIDENCE	MEMBER EVIDENCE	RESPONSIBILITY	SOLUTION	COMMENTS
Build and Maintain a Secure Network and Systems	1. Install and Maintain Network Security Controls.	Network security controls (NSCs), such as firewalls and other network security technologies, are network policy enforcement points that typically control network traffic between two or more logical or physical network segments (or subnets) based on pre-defined policies or rules.	Cyvatar provides a security policy framework. For vulnerability management Cyvatar installs, configures, assesses, remediates, and maintains a secure state of network from a vulnerability management perspective. Includes internal, external, cloud and remote networks.	Additional Hardening of Network & Firewalls	Shared	**Threat & Vulnerability Management**	——
Build and Maintain a Secure Network and Systems	2. Apply Secure Configurations to All System Components.	Malicious individuals, both external and internal to an entity, often use default passwords and other vendor default settings to compromise systems. These passwords and settings are well known and are easily determined via public information. Applying secure configurations to system components reduces the means available to an attacker to compromise the system. Changing default passwords, removing unnecessary software, functions, and accounts, and disabling or removing unnecessary services all help to reduce the potential attack surface.	Cyvatar provides a security policy framework. For vulnerability management and multi-factor authentication Cyvatar installs, configures, assesses, remediates, and maintains a secure state of systems from a vulnerability management perspective. Includes internal, external, cloud and remote systems	Additional Hardening of Systems	Shared	**Threat & Vulnerability Management, Multi-factor Authentication**	——
Protect Account Data	3. Protect Stored Account Data.	Protection methods such as encryption, truncation, masking, and hashing are critical components of account data protection. If an intruder circumvents other security controls and gains access to encrypted account data, the data is unreadable without the proper cryptographic keys and is unusable to that intruder. Other effective methods of protecting stored data should also be considered as potential risk-mitigation opportunities.	N/A	N/A	Member	**Member**	——
Protect Account Data	4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.	The use of strong cryptography provides greater assurance in preserving data confidentiality, integrity, and non-repudiation.	N/A	N/A	Member	**Member**	——
Maintain a Vulnerability Management Program	5. Protect All Systems and Networks from Malicious Software.	Malicious software (malware) is software or flncident Response Managementware designed to infiltrate or damage a computer system without the owner's knowledge or consent, with the intent of compromising the confidentiality, integrity, or availability of the owner's data, applications, or operating system.	Cyvatar provides a security policy framework. For malicious software and security awareness training Cyvatar installs, configures, assesses, remediates, and maintains a secure endpoint in blocking and does not employ a detect and respond approach allowing malicious software to execute.	——	Cyvatar	**Secure Endpoint Management, Security Awareness Training**	——
Maintain a Vulnerability Management Program	6. Develop and Maintain Secure Systems and Software.	Actors with bad intentions can use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor provided security patches, which must be installed by the entities that manage the systems. All system components must have all appropriate software patches to protect against the exploitation and compromise of account data by malicious individuals and malicious software.	Cyvatar provides a security policy framework. For vulnerability management Cyvatar installs, configures, assesses, remediates, and maintains a secure endpoint in blocking and does not employ a detect and respond approach allowing malicious software to execute.	——	Shared	**Threat & Vulnerability Management**	——
Implement Strong Access Control Measures	7. Restrict Access to System Components and Cardholder Data by Business Need to Know.	Unauthorized individuals may gain access to critical data or systems due to ineffective access control rules and definitions. To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.	Cyvatar provides a security policy framework. For multi-factor authentication Cyvatar installs, configures, assesses, remediates, and maintains a secure endpoint in blocking and does not employ a detect and respond approach allowing malicious software to execute.	——	Shared	**Multi-factor Authentication**	——
Implement Strong Access Control Measures	8. Identify Users and Authenticate Access to System Components.	Two fundamental principles of identifying and authenticating users are to 1) establish the identity of an individual or process on a computer system, and 2) prove or verify the user associated with the identity is who the user claims to be.	Cyvatar provides a security policy framework. For multi-factor authentication Cyvatar installs, configures, assesses, remediates, and maintains a secure endpoint in blocking and does not employ a detect and respond approach allowing malicious software to execute.	——	Cyvatar	**Multi-factor Authentication**	——
Implement Strong Access Control Measures	9. Restrict Physical Access to Cardholder Data.	Any physical access to cardholder data or systems that store, process, or transmit cardholder data provides the opportunity for individuals to access and/or remove systems or hardcopies containing cardholder data; therefore, physical access should be appropriately restricted.	N/A	N/A	Member	**Member**	——
Regularly Monitor and Test Networks	10. Log and Monitor All Access to System Components and Cardholder Data.	Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs on all system components and in the cardholder data environment (CDE) allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is difficult, if not impossible, without system activity logs.	Cyvatar provides a security policy framework. For logging and monitoring Cyvatar installs, configures, assesses, remediates, and maintains a secure endpoint in blocking and does not employ a detect and respond approach allowing malicious software to execute.	——	Shared	**Managed Security Orchestration and Response**	Member uses Cyvatar's Threat Vulnerability Management(Threat & Vulnerability Management) services for continuous vulnerability assessment. For internal scanning, a dedicated scanner is installed in the network and scans the network at set intervals. For external scanning, continuous scanning is also performed. The member is alerted for any high or critical vulnerabilities identified by Cyvatar and remediation is performed. By doing continuous vulnerability scanning, the time-to-detect and time-to-remediate is greatly reduced.
Regularly Monitor and Test Networks	11. Test Security of Systems and Networks Regularly.	Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and bespoke and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.	Cyvatar provides a security policy framework. For vulnerability management Cyvatar installs, configures, assesses, remediates, and maintains a secure endpoint in blocking and does not employ a detect and respond approach allowing malicious software to execute. Penetration testing is offered.	——	Shared	**Threat & Vulnerability Management**	Member uses Cyvatar's Threat Vulnerability Management(Threat & Vulnerability Management) services for continuous vulnerability assessment. For internal scanning, a dedicated scanner is installed in the network and scans the network at set intervals. For external scanning, continuous scanning is also performed. The member is alerted for any high or critical vulnerabilities identified by Cyvatar and remediation is performed. By doing continuous vulnerability scanning, the time-to-detect and time-to-remediate is greatly reduced.
Maintain an Information Security Policy	12. Support Information Security with Organizational Policies and Programs.	The organization's overall information security policy sets the tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of cardholder data and their responsibilities for protecting it.	Cyvatar provides a security policy framework.	——	Shared	**Free Policies**	——

SOC 2 TYPE 2

Managing the highest standards to protect customer data correctly, consisting of the five Trust Services Categories: security, availability, processing integrity, confidentiality, and privacy.

SOC 2 TYPE 2	DESCRIPTION	DETAILS	CYVATAR EVIDENCE	MEMBER EVIDENCE	RESPONSIBILITY	SOLUTION	COMMENTS
Risk Assessment	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Considers Tolerances for Risk—Management considers the acceptable levels of variation relative to the achievement of operations objectives.	Cyvatar FREE - Risk Manager: Build your risk register, assign risk ownership and track remediation tasks. Cyvatar FREE - Assessment: Conduct an assessment of your Cybersecurity controls.	Complete Risk Assessment questionnaire & use Risk Manager	Shared	**Freemium**	——
Risk Assessment	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Establishes Sub-objectives to Support Objectives—Management identifies sub-objectives related to security, availability, processing integrity, confidentiality, and privacy to support the achievement of the entity's objectives related to reporting, operations, and compliance.	Cyvatar FREE - Risk Manager: Build your risk register, assign risk ownership and track remediation tasks. Cyvatar FREE - Assessment: Conduct an assessment of your Cybersecurity controls.	Complete Risk Assessment questionnaire & use Risk Manager	Shared	**Freemium**	——
Risk Assessment	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels—The entity identifies and assesses risk at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives.	Cyvatar FREE - Risk Manager: Build your risk register, assign risk ownership and track remediation tasks. Cyvatar FREE - Assessment: Conduct an assessment of your Cybersecurity controls.	Complete Risk Assessment questionnaire & use Risk Manager	Shared	**Freemium**	——
Risk Assessment	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Analyzes Internal and External Factors—Risk identification considers both internal and external factors and their impact on the achievement of objectives.	Cyvatar FREE - Risk Manager: Build your risk register, assign risk ownership and track remediation tasks. Cyvatar FREE - Assessment: Conduct an assessment of your Cybersecurity controls. Cyvatar implements a complete vulnerability management program.	Complete Risk Assessment questionnaire & use Risk Manager	Shared	**Freemium, Threat & Vulnerability Management**	——
Risk Assessment	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Estimates Significance of Risks Identified—Identified risks are analyzed through a process that includes estimating the potential significance of the risk.	Cyvatar FREE - Risk Manager: Build your risk register, assign risk ownership and track remediation tasks. Cyvatar FREE - Assessment: Conduct an assessment of your Cybersecurity controls. Cyvatar implements a complete vulnerability management program.	Complete Risk Assessment questionnaire & use Risk Manager	Shared	**Freemium, Threat & Vulnerability Management**	——
Risk Assessment	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Determines How to Respond to Risks—Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.	Cyvatar FREE - Risk Manager: Build your risk register, assign risk ownership and track remediation tasks. Cyvatar FREE - Assessment: Conduct an assessment of your Cybersecurity controls. Cyvatar implements a complete vulnerability management program.	Complete Risk Assessment questionnaire & use Risk Manager	Shared	**Freemium, Threat & Vulnerability Management**	——
Risk Assessment	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Identifies and Assesses Criticality of Information Assets and Identifies Threats and Vulnerabilities—The entity's risk identification and assessment process includes (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets.	Cyvatar FREE - Risk Manager: Build your risk register, assign risk ownership and track remediation tasks. Cyvatar FREE - Assessment: Conduct an assessment of your Cybersecurity controls. Cyvatar implements a complete vulnerability management program. Cyvatar implements an IT Asset Management Solution.	Complete Risk Assessment questionnaire & use Risk Manager	Shared	**Freemium, Threat & Vulnerability Management, IT Asset Management**	——
Risk Assessment	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Considers the Significance of the Risk—The entity's consideration of the potential significance of the identified risks includes (1) determining the criticality of identified assets in meeting objectives; (2) assessing the impact of identified threats and vulnerabilities in meeting objectives; (3) assessing the likelihood of identified threats; and (4) determining the risk associated with assets based on asset criticality, threat impact, and likelihood.	Cyvatar FREE - Risk Manager: Build your risk register, assign risk ownership and track remediation tasks. Cyvatar FREE - Assessment: Conduct an assessment of your Cybersecurity controls. Cyvatar implements a complete vulnerability management program. Cyvatar implements an IT Asset Management Solution.	Complete Risk Assessment questionnaire & use Risk Manager	Shared	**Freemium, Threat & Vulnerability Management, IT Asset Management**	——
Risk Assessment	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Assess Changes in Systems and Technology—The risk identification process considers changes arising from changes in the entity's systems and changes in the technology environment.	Cyvatar FREE - Risk Manager: Build your risk register, assign risk ownership and track remediation tasks. Cyvatar FREE - Assessment: Conduct an assessment of your Cybersecurity controls. Cyvatar implements a complete vulnerability management program. Cyvatar implements an IT Asset Management Solution.	Complete Risk Assessment questionnaire & use Risk Manager	Shared	**Freemium, Threat & Vulnerability Management, IT Asset Management**	——

SOC 2 TYPE 2	DESCRIPTION	DETAILS	CYVATAR EVIDENCE	MEMBER EVIDENCE	RESPONSIBILITY	SOLUTION	COMMENTS
Risk Assessment	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Assess Changes in Systems and Technology—The risk identification process considers changes arising from changes in the entity's systems and changes in the technology environment.	Cyvatar FREE - Risk Manager: Build your risk register, assign risk ownership and track remediation tasks. Cyvatar FREE - Assessment: Conduct an assessment of your Cybersecurity controls. Cyvatar implements a complete vulnerability management program. Cyvatar implements an IT Asset Management Solution.	Complete Risk Assessment questionnaire & use Risk Manager	Shared	**Freemium, Threat & Vulnerability Management, IT Asset Management**	——
Control Activities	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Integrates With Risk Assessment—Control activities help ensure that risk responses that address and mitigate risks are carried out.	Cyvatar FREE - Risk Manager: Build your risk register, assign risk ownership and track remediation tasks. Cyvatar FREE - Assessment: Conduct an assessment of your Cybersecurity controls. Cyvatar implements a complete vulnerability management program. Cyvatar implements an IT Asset Management Solution.	Complete Risk Assessment questionnaire & use Risk Manager	Shared	**Freemium, Threat & Vulnerability Management, IT Asset Management**	——
Control Activities	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Evaluates a Mix of Control Activity Types—Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.	Cyvatar FREE - Risk Manager: Build your risk register, assign risk ownership and track remediation tasks. Cyvatar FREE - Assessment: Conduct an assessment of your Cybersecurity controls. Cyvatar implements a complete vulnerability management program. Cyvatar implements an IT Asset Management Solution.	Complete Risk Assessment questionnaire & use Risk Manager	Shared	**Freemium, Threat & Vulnerability Management, IT Asset Management**	——
Control Activities	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Establishes Relevant Technology Infrastructure Control Activities—Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.	Cyvatar FREE - Risk Manager: Build your risk register, assign risk ownership and track remediation tasks. Cyvatar FREE - Assessment: Conduct an assessment of your Cybersecurity controls.	Complete Risk Assessment questionnaire & use Risk Manager	Shared	**Freemium**	——
Control Activities	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities—Management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives.	Cyvatar FREE - Risk Manager: Build your risk register, assign risk ownership and track remediation tasks. Cyvatar FREE - Assessment: Conduct an assessment of your Cybersecurity controls.	Complete Risk Assessment questionnaire & use Risk Manager	Shared	**Freemium**	——
Logical and Physical Access Controls	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Identifies and Manages the Inventory of Information Assets—The entity identifies, inventories, classifies, and manages information assets.	"Cyvatar implements a complete vulnerability management program. Cyvatar implements an IT Asset Management Solution.		Shared	**IT Asset Management**	——
Logical and Physical Access Controls	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Restricts Logical Access—Logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted through the use of access control software and rule sets.	Cyvatar implements an IT Asset Management Solution.		Shared	**IT Asset Management**	——
Logical and Physical Access Controls	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Identifies and Authenticates Users—Persons, infrastructure and software are identified and authenticated prior to accessing information assets, whether locally or remotely.	Cyvatar implements a Multi-Factor Authentication program.		Shared	**Multi-factor Authentication**	——
Logical and Physical Access Controls	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Manages Credentials for Infrastructure and Software—New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required or the infrastructure and software are no longer in use.	Cyvatar implements a Multi-Factor Authentication program.		Shared	**Multi-factor Authentication**	——

SOC 2 TYPE 2	DESCRIPTION	DETAILS	CYVATAR EVIDENCE	MEMBER EVIDENCE	RESPONSIBILITY	SOLUTION	COMMENTS
Logical and Physical Access Controls	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Requires Additional Authentication or Credentials—Additional authentication information or credentials are required when accessing the system from outside its boundaries.	Cyvatar implements a Multi-Factor Authentication program.		Shared	**Freemium**	____
Logical and Physical Access Controls	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Scans Information Assets from Outside the Entity for Malware and Other Unauthorized Software—Procedures are in place to scan information assets that have been transferred or returned to the entity's custody for malware and other unauthorized software and to remove any items detected prior to its implementation on the network.	Cyvatar implements a complete vulnerability management program that includes remediation of the vulnerabilities. Cyvatar implements an IT Asset Management Solution.		Shared	**Freemium**	____
System Operations	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Monitors Infrastructure and Software—The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.	Cyvatar implements a complete vulnerability management program that includes remediation of the vulnerabilities. IT Asset Program, secure endpoint program with 24/7 monitoring and cloud SaaS monitoring and logging of changes.		Shared	**Freemium**	____
System Operations	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Implements Change-Detection Mechanisms—The IT system includes a change-detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files.	Cyvatar implements a complete vulnerability management program, IT Asset Program, secure endpoint program with 24/7 monitoring and cloud SaaS monitoring and logging of changes.		Shared	**Freemium, Threat & Vulnerability Management**	____
System Operations	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Conducts Vulnerability Scans—The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis.	Cyvatar implements a complete vulnerability management program that includes remediation of the vulnerabilities.		Shared	**Freemium, Threat & Vulnerability Management**	____
System Operations	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Implements Detection Policies, Procedures, and Tools—Detection policies and procedures are defined and implemented, and detection tools are implemented on Infrastructure and software to identify anomalies in the operation or unusual activity on systems. Procedures may include (1) a defined governance process for security event detection and management that includes provision of resources; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; and (3) logging of unusual system activities.	Cyvatar implements several monitoring solutions: 1. Endpoint protect configured to block first and then with 24/7 detection monitoring. 2. Cloud SaaS monitoring to monitor SaaS application in the cloud. 3. Cloud and on premises 24/7 detection and response monitoring of assets.		Shared	**Freemium, Threat & Vulnerability Management**	____
System Operations	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Designs Detection Measures—Detection measures are designed to identify anomalies that could result from actual or attempted (1) compromise of physical barriers; (2) unauthorized actions of authorized personnel; (3) use of compromised identification and authentication credentials; (4) unauthorized access from outside the system boundaries; (5) compromise of authorized external parties; and (6) implementation or connection of unauthorized hardware and software.	Cyvatar implements several monitoring solutions: 1. Endpoint protect configured to block first and then with 24/7 detection monitoring. 2. Cloud SaaS monitoring to monitor SaaS application in the cloud. 3. Cloud and on premises 24/7 detection and response monitoring of assets.		Shared	**Freemium, Threat & Vulnerability Management, IT Asset Management**	____
System Operations	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Implements Filters to Analyze Anomalies—Management has implemented procedures to filter, summarize, and analyze anomalies to identify security events.	Cyvatar implements several monitoring solutions: 1. Endpoint protect configured to block first and then with 24/7 detection monitoring. 2. Cloud SaaS monitoring to monitor SaaS application in the cloud. 3. Cloud and on premises 24/7 detection and response monitoring of assets.		Shared	**Freemium, Threat & Vulnerability Management, IT Asset Management**	____

SOC 2 TYPE 2	DESCRIPTION	DETAILS	CYVATAR EVIDENCE	MEMBER EVIDENCE	RESPONSIBILITY	SOLUTION	COMMENTS
System Operations	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Responds to Security Incidents—Procedures are in place for responding to security incidents and evaluating the effectiveness of those policies and procedures on a periodic basis.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	____
System Operations	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Communicates and Reviews Detected Security Events—Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	____
System Operations	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Develops and Implements Procedures to Analyze Security Incidents—Procedures are in place to analyze security incidents and determine system impact.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	____
System Operations	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Assesses the Impact on Personal Information—Detected security events are evaluated to determine whether they could or did result in the unauthorized disclosure or use of personal information and whether there has been a failure to comply with applicable laws or regulations.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	____
System Operations	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Determines Personal Information Used or Disclosed—When an unauthorized use or disclosure of personal information has occurred, the affected information is identified.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	____
System Operations	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Assigns Roles and Responsibilities—Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are assigned, including the use of external resources when necessary.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	____
System Operations	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Contains Security Incidents—Procedures are in place to contain security incidents that actively threaten entity objectives.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	____

SOC 2 TYPE 2	DESCRIPTION	DETAILS	CYVATAR EVIDENCE	MEMBER EVIDENCE	RESPONSIBILITY	SOLUTION	COMMENTS
System Operations	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Mitigates Ongoing Security Incidents—Procedures are in place to mitigate the effects of ongoing security incidents.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	——
System Operations	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Ends Threats Posed by Security Incidents—Procedures are in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	——
System Operations	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Restores Operations—Procedures are in place to restore data and business operations to an interim state that permits the achievement of entity objectives.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	——
System Operations	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Develops and Implements Communication Protocols for Security Incidents—Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	——
System Operations	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Obtains Understanding of Nature of Incident and Determines Containment Strategy—An understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate containment strategy, including (1) a determination of the appropriate response time frame, and (2) the determination and execution of the containment approach.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	——
System Operations	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Remediates Identified Vulnerabilities—Identified vulnerabilities are remediated through the development and execution of remediation activities.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	——
System Operations	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Communicates Remediation Activities—Remediation activities are documented and communicated in accordance with the incident response program.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	——

SOC 2 TYPE 2	DESCRIPTION	DETAILS	CYVATAR EVIDENCE	MEMBER EVIDENCE	RESPONSIBILITY	SOLUTION	COMMENTS
System Operations	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Evaluates the Effectiveness of Incident Response—The design of incident response activities is evaluated for effectiveness on a periodic basis.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	____
System Operations	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Periodically Evaluates Incidents—Periodically, management reviews incidents related to security, availability, processing integrity, confidentiality, and privacy and identifies the need for system changes based on incident patterns and root causes.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	____
System Operations	The entity identifies, develops, and implements activities to recover from identified security incidents.	Restores the Affected Environment—The activities restore the affected environment to functional operation by rebuilding systems, updating software, installing patches, and changing configurations, as needed.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	____
System Operations	The entity identifies, develops, and implements activities to recover from identified security incidents.	Communicates Information About the Event—Communications about the nature of the incident, recovery actions taken, and activities required for the prevention of future security events are made to management and others as appropriate (internal and external).	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	____
System Operations	The entity identifies, develops, and implements activities to recover from identified security incidents.	Determines Root Cause of the Event—The root cause of the event is determined.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	____
System Operations	The entity identifies, develops, and implements activities to recover from identified security incidents.	Implements Changes to Prevent and Detect Recurrences—Additional architecture or changes to preventive and detective controls, or both, are implemented to prevent and detect recurrences on a timely basis.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	____
System Operations	The entity identifies, develops, and implements activities to recover from identified security incidents.	Improves Response and Recovery Procedures—Lessons learned are analyzed, and the incident response plan and recovery procedures are improved.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	____

SOC 2 TYPE 2	DESCRIPTION	DETAILS	CYVATAR EVIDENCE	MEMBER EVIDENCE	RESPONSIBILITY	SOLUTION	COMMENTS
System Operations	The entity identifies, develops, and implements activities to recover from identified security incidents.	Implements Incident Recovery Plan Testing—Incident recovery plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of relevant system components from across the entity that can impair availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.	Cyvatar implements several incident response solutions as needed: 1. Incident Response Retainer 2. Incident Response Maturity Assessment 3. Incident Response Plan, Program, or Policy Development 4. Incident Response Playbook Development 5. Incident Response Tabletop Exercise 6. Response Advisory Services		Shared	**Incident Response Management**	——
Risk Mitigation	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Considers Mitigation of Risks of Business Disruption—Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet the entity's objectives during response, mitigation, and recovery efforts.	Cyvatar FREE - Risk Manager: Build your risk register, assign risk ownership and track remediation tasks. Cyvatar FREE - Assessment: Conduct an assessment of your Cybersecurity controls.	Complete Risk Assessment questionnaire & use Risk Manager	Shared	**Freemium**	——
Risk Mitigation	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Considers the Use of Insurance to Mitigate Financial Impact Risks—The risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives.	Cyvatar FREE - Risk Manager: Build your risk register, assign risk ownership and track remediation tasks. Cyvatar FREE - Assessment: Conduct an assessment of your Cybersecurity controls.	Complete Risk Assessment questionnaire & use Risk Manager	Shared	**Freemium, Cyber Insurance Partnerships**	——
ADDITIONAL CRITERIA FOR PRIVACY			Cyvatar partners with several privacy flncident Response Managements to assist in filing privacy needs.			**Cyvatar Privacy Partnerships**	——

THANK YOU

Let Cyvatar Streamline and drive faster compliance with effortless cybersecurity-as-a-service.

VISIT **CYVATAR.AI** TO LEARN MORE & CREATE A FREE ACCOUNT.