IBSCO

Risk Assessment

17711 Telge Road
Cypress, TX 77429
(800) 231-6480

https://www.ibsco.com/



TESSERACT™
Compiled by Ardalyst
www.ardalyst.com

Disclaimers and Disclosures

This document is developed based on information provided by the Organization Seeking Certification (OSC) ("you", "your") regarding the classification and flow of CUI in your organization and the systems you use (or will use) in your end-state configuration. Their accuracy is dependent on the information you provided. The responsibility for identifying and designating CUI rests solely on you. Nothing in this document should be construed as legal advice. Ardalyst does not determine, interpret, or classify what constitutes Controlled Unclassified Information (CUI) or derivative CUI within your environment. For any determinations regarding CUI, derivative CUI, or related regulatory interpretations, you should consult qualified legal counsel.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Risk Assessment (RA) Approval

The policies contained herein are approved for immediate implementation and are authorized until replaced. This Cybersecurity Program is governed by DFARS 252.204-7012, 252.204-7019, 252.204-7020, and 252.204-7021, including the guidance provided in NIST SP 800-171, the Cybersecurity Maturity Model Level 2 Certification, the Cybersecurity Maturity Model Level 2 Scoping Guide, and the Cybersecurity Maturity Model Certification Level 2 Assessment Guides. Additional guidelines, if relevant, are noted in each policy.

Signed:

Richard Scroggins

Signature

Richard Scroggins

Printed Name

Technology Manager

Title

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Revision History

This document is updated annually at a minimum.

Version Number	Date Last Completed	Notes	Date Next Due
1.0	2023-10-01	Initial Document	2024-10-01
2.0	2026-01-14	Annual Update	2027-01-14
3.0	2026-08-27	Program Update	2027-08-27

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

IBSCO Risk Assessment

Introduction

The purpose of this Risk Assessment is to conduct the governance activities required to execute and mature the IBSCO Cybersecurity Program.

"Risk assessments are used to identify, estimate, and prioritize risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems." (NIST 800-30)

Conducting the Risk Assessment is required to meet RA.L2-3.11.1. We achieve this by identifying:
- organization value creation;
- key assets used to deliver that value, including personnel, systems and facilities;
- the risks involved in the use of those key assets, and;
- mitigation strategies for those risks.

Organization Overview

Mission Statement:	We maintain our position of leadership through a total commitment to our customer's complete satisfaction.
Value Propositions:	We offer custom solutions for advanced applications including miniature bearings, high performance bearings, and bearing related components. We have a state of the art Class 6 Cleanroom to handle your relubrication needs. As a factory-authorized distributor of standard, specialized, and custom bearings, we will meet and exceed your expectations. Excellent service and quality go hand-in-hand, and our bearing experts will not stop working after your order has been placed. Our best-in-service approach is part of our culture, and we will do everything needed to ensure complete satisfaction for all of your ball bearing needs, including miniature bearings and instrument bearings, needle bearings, roller bearings, or spherical plain bearings and rod end requirements. We support all High Precision Applications: Medical, Dental, Robotic, Motion Control and many more.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Customer Base:	We support commercial, military, and space applications as well as related ground support equipment, and we provide bearings for defense applications from missile programs to drone based camera turrets. Our ISO Class 6 cleanroom gives us a distinct advantage in the support of medical applications which often require specialized greases and/or specific lubrication fill rates; we can support dental hand-piece bearings as well as many other bio and life science platforms. If your bearing requirements are for motion control or factory automation we can support your needs; we provide bearings for motors, servos, encoders and actuators used in motion control and automation systems. We provide bearings for many "high tech" applications including but not limited to robotics, semiconductor production, laser applications and many more, and we support test and analytical equipment for high tech and other industries. We can also support your requirements in your industry with our experienced sales team assisting with specific industrial applications. We provide bearings in food service and agricultural applications, including the ability to re-lubricate bearings with food grade lubricants. We support bearing applications in components used in oil and gas production and processing as well as wind power and solar power systems. We provide bearings and parts for many hobby, amusement, or recreational applications including but not limited to 3D printers, game and pinball machines, RC cars and drones, spinners, and many more. We support automotive, racing, off-road and marine applications, with the ability to re-lubricate bearings with various high performance lubricants. We support bearing applications in components used in the outdoor industry including archery cam or pulley bearings, and various bearings used in fishing reels. [ibsco.com]
Services:	- Alternative Manufacturers - Relubrication - Product Customization - Scheduled Deliveries - Safety Stock - JIT – Just in Time Delivery - Inventory Management - Lead Time Elimination - Custom Solutions - Lubrication & Re-Lubrication Services (The Re-lubricating & Refreshing Authority for 40+ years; factory certified by NMB, NHBB & Myonic, RBC) - ISO Class 6 Cleanroom Lubrication & Packaging Services (Class 6 Cleanroom with Class 5 capabilities at the bench; MIL-DTL-197 capability) - Application Consulting (custom and unique applications and designs; ISO Class 6 factory certified cleanroom supporting hundreds of custom lubricants, closures, fill amounts, packaging and labeling) - Custom Labeling & Packaging (vial pack, strip pack, coin roll, individual box, kraft bag, kitting) - Basic failure evaluation services with access to in-depth failure analysis services from many of the leading ball bearing manufacturers
CUI Definition	We receive orders from government contractors that contain CUI. These documents are stored in our GCC-H cloud environment. Our inside sales team then uses the information in those orders to make a non-CUI workorder in our commercial system. Most work is using COTS products.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Performs Software Development?	No

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Understanding Your Cybersecurity Program

A robust cybersecurity program begins with a clear understanding of the risks your organization faces, allowing you to set priorities and direct your efforts effectively. Protecting sensitive information is essential, and this requires knowing where it resides and how it moves throughout your business. Physical security measures help ensure that only authorized individuals can access facilities and areas where critical data is stored. These foundational steps establish a strong base for safeguarding your organization's assets.

Controlling access to systems and data is a key part of the program. Regularly reviewing user permissions ensures that only those who need access have it, while privileged accounts with elevated permissions require careful oversight and monitoring. Security training programs keep all employees informed about best practices and emerging threats, helping to build a culture of awareness and responsibility. Together, these measures support a secure and well-prepared workforce.

Implementing a well-defined security architecture provides a structured approach to protecting systems and data. Establishing secure baselines for systems and endpoints ensures consistent configurations and helps detect unauthorized changes. Maintaining network boundaries limits exposure to external and internal threats, supporting the integrity of your organization's digital infrastructure. Verifying user identities through secure authentication mechanisms is crucial for preventing unauthorized access. Managing devices such as smartphones, laptops, and removable media helps prevent data loss and misuse, with clear policies and controls applied across all endpoints. These practices ensure that both access and devices are managed proactively to reduce risk.

Continuous monitoring and rapid response are essential for detecting and addressing threats. Managing vulnerabilities involves identifying weaknesses in systems and software and applying updates promptly to minimize exposure. Collecting and analyzing log data provides insight into system activity and helps spot anomalies. Monitoring endpoints and networks allows for early detection of suspicious behavior. Staying informed about threat intelligence and security advisories enables your organization to adapt quickly to new risks. Reviewing security events ensures that potential issues are investigated and addressed in a timely manner.

When incidents occur, a structured response process helps contain and resolve security breaches efficiently. Recovery planning ensures that operations can be restored quickly after disruptions, minimizing downtime and impact. Regular assessment and documentation of your cybersecurity program support transparency, readiness for audits, and ongoing improvement. By following these interconnected steps, your organization creates a continuous cycle of compliance, protection, and maturation.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Key Assets

The following personnel, locations and systems are included in the scope of the risk assessment

User Groups		
Group Name	**Group Type**	**Description**
IBSCO Authorized Privileged Users	Information Technology	IT personnel have access to administrative tools and resources via privileged accounts.
IBSCO CUI Authorized Users	Knowledge Workers (non-specialized)	Non-specialized knowledge workers access and view CUI documents within the Enclave using Microsoft SharePoint and/or Microsoft Teams. Microsoft Office applications are available within the Enclave to create, edit, and process CUI documents as required for authorized business purposes. Microsoft Outlook is available within the Enclave for email communication involving CUI when necessary and authorized. Microsoft Teams is also available within the Enclave for communication related to CUI, as required for official business.

Locations		
Location Name	**Location Type**	**Description**
Cloud CUI Enclave	Cloud Only without Mobile	Cloud only environments significantly mitigate risk by removing the presence of facilities storing sensitive data and media containing sensitive data. Users can access the enclave from anywhere; all access locations are considered out of scope as they do not have any physical CUI media contained within them. Physical endpoints used to access the cloud are Out of Scope Assets as defined in § 32 CFR 170.19 (c)(1) - Table 3 “CMMC Level 2 Asset Categories and Associated Requirements”, under the asset description “An endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of CUI beyond the Keyboard/Video/Mouse sent to the VDI client is considered an Out-of-Scope Asset.”

Systems		
System Name	**System Type**	**Purpose**
IBSCO - M365 GCC-H	M365 GCC-H	Microsoft 365 & Azure subsystems that are always present in a Tesseract enclave.
IBSCO - Qualys	Qualys	Patch management solution for managed endpoints
IBSCO - Win 10/11 AVD	Win 10/11 AVD	Virtual Windows endpoint with profile persistence using an AVD host pool to provide IaaS endpoints for users.
IBSCO - Win 10/11 Win365	Win 10/11 Win365	Provide a Cloud Desktop which gives users a desktop-based Windows experienced without the overhead of managing a virtual PC.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Outcome	Ardalyst CSF 2.0 Step
Understand Your Risk and Direct Your Program	Identify

A good cybersecurity program starts by figuring out what risks your organization faces and deciding how you'll address them. This helps you set priorities and make smart choices about protecting your systems and data.

Assess Risk: Review your risks at least once a year, and after major organizational changes, to make sure your security decisions still make sense.

Practices Affected	Tesseract Block	Risk	Mitigation
3.11.1 Risk Assessments	Perform Risk Assessments	Because the security landscape and organizational missions evolve frequently, organizations that fail to reassess risk on a regular basis may find their security postures outdated and misaligned with current needs or best practices, increasing the risk of vulnerabilities or gaps.	We routinely perform risk assessments to stay current with best practices and requirements, allowing us to tailor our program to organizational needs.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Outcome	Ardalyst CSF 2.0 Step
Control and Protect Your Sensitive Information	Protect

To keep important information safe, you need to map out how it moves through your organization and formally document those pathways. Understanding where sensitive data travels lets you put the right protections in place where they're needed most.

Document Data Flows: Write down how sensitive data moves through your systems and explain how you keep it safe.

Practices Affected	Tesseract Block	Risk	Mitigation
3.1.22 Control Public Information	Manage Publication Review - Self-Review Permitted	Posting data to public platforms, such as social media or organizational websites, exposes the organization to the risk of CUI data being inadvertently or intentionally disclosed. Insider threats may also deliberately post CUI data to these public systems, increasing the risk of compromise.	Authorized Publishers are named and must submit posts to a review authority before posting. Reviewers may review their own posts if the review is logged.
3.1.3 Control CUI Flow	Control CUI Flow	If an organization does not fully understand or control how data moves within its enclave, it cannot effectively protect or track that data. This lack of oversight increases the risk of data exposure, loss, or misuse, as sensitive information may go unaccounted for.	We map CUI data flows and identify all users and systems involved in transmitting, processing, or storing CUI, enabling us to implement targeted controls that reduce associated risks.
3.1.20 External Connections	Control External Connections	Any connection to external systems creates a possible entry point for attackers, raising the likelihood of unauthorized access, data spillage, or data loss. These connections expand the attack surface and can expose sensitive information to external threats.	We identify all external systems in use and establish controls and processes to prevent improper sharing of CUI with those systems.
3.10.6 Alternative Work Sites	Safeguard Alternative Work Sites - No Alternative Work Sites	Alternate worksites where CUI is present often lack the physical security measures of the primary worksite. This difference introduces unique risks, as each location may present vulnerabilities not present in the main organizational environment.	We reduce the risks associated with alternative work sites by not permitting them.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Manage Media: Set clear rules for how sensitive data is stored, labeled, accessed, and safely discarded across all types of media.			
Practices Affected	**Tesseract Block**	**Risk**	**Mitigation**
3.13.16 Data At Rest	Protect Data at Rest - Physical Endpoints with Data at Rest are Not Allowed	Storing CUI on any device introduces the risk that, if the device is present and accessible, unauthorized individuals could gain access to sensitive information, especially if proper controls are not in place.	We reduce the risk of data-at-rest compromise by not allowing devices that store data to connect to the tenant.
3.8.3 Media Disposal	Perform Media Sanitization - Cloud Only without Mobile	When media containing CUI is disposed of, the organization loses physical control over it, increasing the risk that sensitive information could be discovered, accessed, or compromised by unauthorized parties during or after disposal.	We rely on our Cloud Service Provider's FedRAMP authorization to ensure that they are properly sanitizing and destroying any physical media containing CUI.
3.8.1 Media Protection	Protect System Media - No Physical Media	Media that contains CUI, whether digital or physical, is at risk of compromise if it is lost, stolen, or accessed by unauthorized individuals. The loss of control over such media can lead to exposure or misuse of sensitive information.	We store all media in the cloud, eliminating physical compromise risk and inheriting the cloud provider's physical protections.
3.8.5 Media Accountability	Ensure Media Accountability - No Physical Media	Moving media with CUI outside the secure enclave increases the risk of loss or unauthorized access, as the media is no longer protected by the enclave's physical and procedural safeguards, making it more vulnerable to compromise.	We eliminate the risk of CUI loss or compromise during transport by not permitting any physical forms or storage of CUI.
3.7.3 Equipment Sanitization	Methods for Pre-Maintenance Equipment Sanitization - Physical Equipment Containing CUI Not Permitted	Maintenance activities on devices may expose controlled data to personnel who lack proper authorization, increasing the risk that sensitive information could be accessed, viewed, or compromised during routine or emergency maintenance.	We eliminate the risk of CUI loss or compromise during maintenance by not permitting any physical equipment that stores digital CUI.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

3.8.4 Media Markings	Perform Media Marking	If media containing CUI is not clearly marked, personnel may not recognize its sensitivity, which can result in improper handling, storage, or disposal, increasing the risk of accidental exposure or loss of controlled information.	We follow federal standards for marking CUI, reducing the risk of it being unrecognized or mishandled.
3.8.6 Portable Storage Encryption	Enforce Cryptography on Portable Storage Devices - Portable Storage Not Permitted	Storing data on portable media, such as USB drives or external disks, raises the risk of data spillage due to the potential for theft, loss, or misplacement, which can result in unauthorized access to sensitive information.	We eliminate data spillage and insider threat risks by banning the use of portable storage devices.
3.8.9 Protect Backups	Enforce Cryptography for Backups - No Physical Backups Present	Backup devices can be a weak point in data protection if not properly managed, as they may be overlooked during security planning, making them a potential source of data compromise if accessed by unauthorized individuals.	By not allowing physical backups, we reduce this potential weak point for data compromise.
3.8.2 Media Access	Control Media Access - No Physical Media	Allowing unrestricted access to media containing CUI, whether digital or physical, raises the chances of unauthorized individuals accessing, misusing, or exposing sensitive data, increasing the risk of compromise or loss.	We store all media in the cloud, eliminating the risk of physical compromise and benefiting from the cloud provider's physical security measures.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Outcome	Ardalyst CSF 2.0 Step
Control and Monitor Your Facilities	Protect

Keeping an eye on your buildings and workspaces helps make sure only the right people can get to sensitive information. Secure spaces—like locked server rooms, badge-access offices, or dedicated storage areas—give your team a safe place to work with and store important data.

Manage Physical Access: Establish and maintain controls that restrict, manage, and monitor access to physical spaces where sensitive data is stored or processed.

Practices Affected	Tesseract Block	Risk	Mitigation
3.10.2 Monitor Facility	Monitor Facilities - No Physical Facility Containing CUI	Trusted enclave spaces are designed to securely store, process, and transmit CUI. If a malicious actor or unauthorized, untrained person gains access, they can introduce vulnerabilities or compromise both the data and the devices within the enclave.	We eliminate risks associated with physical spaces by running our enclave in the cloud and not allowing any physical spaces containing CUI.
3.10.1 Limit Physical Access	Limit Physical Access - No Physical Facility Containing CUI	Trusted enclave spaces are designed to securely store, process, and transmit CUI. If a malicious actor or unauthorized, untrained person gains access, they can introduce vulnerabilities or compromise both the data and the devices within the enclave.	We eliminate risks associated with physical spaces by running our enclave in the cloud and not allowing any physical spaces containing CUI.
3.10.5 Manage Physical Access	Manage Physical Access - No Physical Facilities Containing CUI	Trusted enclave spaces are designed to securely store, process, and transmit CUI. If a malicious actor or unauthorized, untrained person gains access, they can introduce vulnerabilities or compromise both the data and the devices within the enclave.	We eliminate risks associated with physical spaces by running our enclave in the cloud and not allowing any physical spaces containing CUI.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Manage Visitors: Implement procedures to authorize, identify, and monitor visitors in areas where sensitive data is present.			
Practices Affected	**Tesseract Block**	**Risk**	**Mitigation**
3.10.3 Escort Visitors	Methods for Escorting Visitors - No Physical Facility Containing CUI	Visitors to facilities containing CUI may not have the necessary training or authorization, making them a potential insider threat. Their access can increase the risk of accidental or intentional exposure or compromise of sensitive information.	We eliminate risks associated with physical spaces by running our enclave in the cloud and not allowing any physical spaces containing CUI.

Log Access: Keep records of who enters sensitive areas and when, so you can spot issues and support investigations if needed.			
Practices Affected	**Tesseract Block**	**Risk**	**Mitigation**
3.10.4 Physical Access Logs	Log Physical Access - No Physical Facility Containing CUI	If access to physical facilities is not tracked, it becomes difficult to trace policy violations or malicious actions back to specific individuals, reducing accountability and increasing the risk of undetected or unresolved security incidents.	We eliminate risks associated with physical spaces by running our enclave in the cloud and not allowing any physical spaces containing CUI.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Outcome	Ardalyst CSF 2.0 Step
Monitor and Manage Your User Access	Protect

Monitoring and managing user access helps ensure that only authorized individuals can reach your systems and data. This means regularly reviewing who has access, updating permissions when people change roles or leave the organization, and making sure users only have the access they need to do their jobs. Good access management helps protect sensitive information and reduces the risk of accidental or intentional misuse.

Manage Personnel: Screen new hires and promptly adjust access when people leave or change roles to keep systems secure.

Practices Affected	Tesseract Block	Risk	Mitigation
3.9.1 Screen Individuals	Methods for Background Screening - Background + US Persons	Personnel who are not trustworthy pose a risk to both the integrity and confidentiality of data. If granted access to systems, they may intentionally or unintentionally cause harm, compromise sensitive information, or disrupt operations.	We assess potential employees' trustworthiness through background checks and confirm US Person status to ensure CUI eligibility.
3.9.2 Personnel Actions	Manage Personnel Actions	When personnel are transferred or terminated, their access needs change. If access is not promptly updated, individuals may retain or gain access to data they no longer qualify for, creating a potential insider threat and increasing the risk of data misuse.	We manage personnel actions to ensure transferred staff surrender unneeded access and terminated staff surrender all access devices and media. Involuntarily terminated personnel have access revoked before or during termination to minimize insider threats.

Manage User Accounts: Keep a complete list of user accounts and make sure only approved users can access your data.

Practices Affected	Tesseract Block	Risk	Mitigation
3.1.1 Authorized Access Control	Control Authorized Access	Systems lacking access controls are vulnerable to compromise by malicious actors. While user access is a primary concern, risks also arise from other entities like service principals and computing devices that may interact with the system.	Access is granted only after approval from HR and the Technical Lead, ensuring all users, service principals, and assets follow a controlled authorization process.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Manage User Sessions: Make sure users are identified, shown their responsibilities, and only allowed to use the functions they need—then end their sessions automatically when they're no longer active.			
Practices Affected	**Tesseract Block**	**Risk**	**Mitigation**
3.1.11 Session Termination	Enforce Session Termination	Unattended sessions provide an opportunity for attackers to gain unauthorized access to systems or data, as there is no active user monitoring the session. This increases the risk of malicious activity or data compromise during periods of inactivity.	We automatically terminate unused sessions after a set period to reduce the risk of unauthorized access.
3.1.2 Transaction and Function Control	Control Transactions and Functions	Vendor-supplied systems often include numerous features and functions, some of which may be exploited accidentally or maliciously. This variety increases the risk of misuse, as not all capabilities may be necessary or properly secured.	Our system baselines disable all functions not required for user responsibilities, reducing unnecessary risk and limiting potential attack vectors.
3.1.9 Privacy and Security Notices	Display Privacy and Security Notices	Users may forget the sensitivity of the systems they access, claim ignorance of security requirements, or object to established security policies, increasing the risk of accidental or intentional policy violations and potential data compromise.	Systems accessed by non-privileged users display privacy and security notices at login and periodically require acceptance of terms of use.
3.13.9 Connections Termination	Enforce Connection Termination	Open network connections can be exploited by attackers to access systems or intercept data. Without proper controls, these connections increase the risk of unauthorized entry, data breaches, or other malicious activities targeting the organization.	We automatically disconnect unused sessions after a set period to reduce the risk of unauthorized access.
3.5.1 Identification	Inventory Unique Identifiers	Systems lacking access controls are vulnerable to compromise by malicious actors. While user access is a primary concern, risks also arise from other entities like service principals and computing devices that may interact with the system.	We inventory users, service principals, and assets, documenting their unique identifiers to recognize authorized access and quickly identify unauthorized accounts.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

3.5.2 Authentication	Enforce Authentication	Systems lacking access controls are vulnerable to compromise by malicious actors. While user access is a primary concern, risks also arise from other entities like service principals and computing devices that may interact with the system.	All systems require authentication using at least an identifier and a password to ensure secure access.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Outcome	Ardalyst CSF 2.0 Step
Monitor and Manage Your Privileged User Access	Protect

Privileged users have extra permissions to control and manage your systems, which means they can access sensitive information and perform important administrative tasks. It's important to carefully manage who gets these privileges and regularly review their activities. Monitoring privileged user actions helps prevent mistakes, intentional misuse, and ensures only trusted individuals have access to critical parts of your organization's systems.

Manage Privileged Roles: Define privileged roles carefully to separate duties and limit access, so no single user can control or hide critical system actions.

Practices Affected	Tesseract Block	Risk	Mitigation
3.1.4 Separation Of Duties	Enforce Separation of Duties	Privileged users with both configuration and monitoring rights can modify systems or access data and then conceal their actions by altering monitoring records. This dual access increases the risk of undetected unauthorized changes or data compromise.	We separate privileged monitoring and configuration roles, limit dual-role accounts, and log privileged access to enhance oversight and reduce risk.
3.13.3 Role Separation	Enforce Role Separation	When privileged and non-privileged functions are combined in a single role, it increases the risk that the role could be misused to gain unauthorized control over systems or sensitive data, making it harder to enforce separation of duties and limit access.	We provide separate accounts for privileged and non-privileged activities, ensuring privileged access is only used when necessary.

Manage Privileged Access: Limit privileged access to essential tasks, authorize it carefully—especially for remote activities—and make sure all actions are logged and reviewed.

Practices Affected	Tesseract Block	Risk	Mitigation
3.1.6 Non-Privileged Account Use	Enforce Non-Privileged Account Use	Privileged accounts have elevated access that can be exploited by malicious actors to gain control over systems or sensitive data. If these accounts are compromised, the attacker can perform actions that may go undetected and cause significant harm.	Privileged accounts are restricted from productivity software licenses and may only be used for privileged functions, reducing misuse risk.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

3.1.7 Privileged Functions	Restrict Privileged Functions	When access to privileged functions is widely distributed, it becomes harder to control and monitor who can make critical changes, increasing the risk that systems or data could be compromised by unauthorized or unintentional actions.	We configure systems so that only privileged accounts can execute privileged functions, reducing the risk of unauthorized actions.
3.3.9 Audit Management	Limit Audit Management	Audit logs are essential for detecting and investigating malicious activity. If responsibility for managing logs is spread across many individuals or teams, it increases the risk that logging processes could be compromised or manipulated without detection.	Privileged access to auditing tools is limited to a few roles, and all privileged access is logged to track who manages auditing functionality.
3.1.5 Least Privilege	Employ Least Privilege	Granting broad privileges to privileged accounts may simplify management, but it also increases the risk that these accounts could be misused, either intentionally or accidentally, to cause harm or compromise sensitive systems and data.	We use vendor-supplied roles to assign privileged accounts only the minimum access needed, enforcing least privilege principles.
3.1.15 Privileged Remote Access	Authorize Privileged Remote Access - Authorize All	Remote access bypasses the physical security controls present on-site, exposing systems and data to additional risks. Without the organization's physical protections, remote sessions are more vulnerable to interception, unauthorized access, or compromise.	We enable remote administration of our systems and maintain detailed access logs to monitor all remote administrative actions, enhancing oversight and reducing the risk associated with remote management.

Manage Maintenance Access: Establish clear rules to control and monitor maintenance access to prevent misuse and protect sensitive systems.

Practices Affected	Tesseract Block	Risk	Mitigation
3.7.2 System Maintenance Control	Perform System Maintenance Control - Self Approval	System maintainers need privileged access for their work, which makes them a potential insider threat or a target for malicious actors seeking to exploit their elevated permissions to compromise systems or data.	We use privileged identity management to monitor and manage remote privileged access, requiring a documented request for privileged account use.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

3.7.6 Maintenance Personnel	Supervise Maintenance Personnel	On-site system maintenance often requires granting access to secure areas, which increases the risk of data loss or compromise if maintainers are not properly supervised or if their access is not tightly controlled.	IT staff supervise maintenance personnel to reduce risk during maintenance activities.
3.7.5 Nonlocal Maintenance	Control Nonlocal Maintenance	When system maintainers connect remotely to the enclave, it reduces the organization's ability to monitor and control their activities, increasing the risk of unauthorized actions or providing new opportunities for attackers to exploit remote access.	We require multifactor authentication for all nonlocal maintenance and ensure maintenance sessions are terminated immediately after activities are completed.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Outcome	Ardalyst CSF 2.0 Step
Manage Your Security Training Program	Protect

Everyone—including users with special access—should understand the basics of cybersecurity and know how to spot risks from inside the organization. It's also important for all users to follow good habits for handling sensitive information.

Train Users: Provide regular training to help users understand cybersecurity risks and recognize behaviors that could signal insider threats.

Practices Affected	Tesseract Block	Risk	Mitigation
3.2.1 Role-Based Risk Awareness	Ensure Role-Based Risk Awareness	If privileged users lack a clear understanding of their responsibilities, they may misuse their elevated access, either carelessly or without authorization, increasing the risk of accidental or intentional harm to systems or data.	We provide role-based training to ensure personnel understand their security responsibilities.
3.2.3 Insider Threat Awareness	Conduct Insider Threat Awareness Training	Insider threats are especially dangerous since insiders already have trusted access to sensitive systems and data, making it easier for them to bypass security controls and cause significant damage or data breaches.	We deliver insider threat training to personnel, equipping them to recognize, report, and counter potential insider threats.

Train Privileged Users: Provide specialized training to privileged users so they understand how to use their elevated access responsibly and securely.

Practices Affected	Tesseract Block	Risk	Mitigation
3.2.2 Role-Based Training	Conduct Role-Based Training	If privileged users lack a clear understanding of their responsibilities, they may misuse their elevated access, either carelessly or without authorization, increasing the risk of accidental or intentional harm to systems or data.	We conduct role-based security training to ensure all personnel understand their specific security responsibilities.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Outcome	Ardalyst CSF 2.0 Step
Employ the Tesseract Security Architecture	Protect

A solid security architecture gives you a clear plan for setting up your systems with the right protections, like firewalls, access controls, and encryption. These controls help keep your organization's data and operations secure.

Design an Architecture: Create a security-focused system architecture that includes secure design principles and ensures protections are built in from the start.

Practices Affected	Tesseract Block	Risk	Mitigation
3.13.2 Security Engineering	Employ Security Engineering - Org Does Not Develop Software	Implementing security measures after a system has been designed and built is challenging and often less effective. Retrofitting controls can leave gaps or vulnerabilities that are harder to address than if security was integrated from the start.	We design systems using secure products and best practices, integrating security at the outset to ensure protection is embedded from the beginning.

Employ Cryptography: Use strong encryption to protect sensitive data during storage and transmission, and manage cryptographic keys securely

Practices Affected	Tesseract Block	Risk	Mitigation
3.13.11 CUI Encryption	Employ FIPS-Validated Cryptography	Poorly implemented cryptography systems can be vulnerable to attack, allowing malicious actors to bypass encryption and gain access to sensitive data that should have been protected.	We ensure all encryption within our environment uses FIPS-validated protocols for maximum security.
3.13.8 Data In Transit	Protect Data in Transit - No Physical Facility Present	Data being transmitted between systems can be intercepted by malicious or unauthorized actors, increasing the risk of data breaches or exposure of sensitive information during transfer.	We encrypt all data in transit using FIPS-validated encryption protocols.
3.13.10 Key Management	Perform Key Management	Cryptographic keys are used to decrypt sensitive data. If a malicious actor obtains these keys, they can access and compromise protected information, undermining the effectiveness of encryption.	Our systems automatically manage cryptographic keys.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

3.1.13 Remote Access Confidentiality	Encrypt Remote Access Sessions	Remote access sessions often travel across the internet and other networks outside the organization's control, making them vulnerable to interception, interference, or eavesdropping by unauthorized parties.	We encrypt all remote access sessions to protect confidentiality and prevent third parties from accessing intercepted data.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Outcome	Ardalyst CSF 2.0 Step
Establish and Maintain Secure Baselines	Protect

Setting a baseline for your systems means you know how things should look when they're properly configured. This helps you make sure security protections are in place and spot any unexpected changes that could signal a problem.

Design Baselines: Define secure system configurations, enforce them consistently, and limit functionality to only what's needed.

Practices Affected	Tesseract Block	Risk	Mitigation
3.4.6 Least Functionality	Employ Least Functionality	Every system function may introduce vulnerabilities that attackers can exploit. Systems with extensive functionality present a larger attack surface, increasing the likelihood that some features may contain exploitable weaknesses.	Our baselines deactivate unnecessary system functions, reducing exposure to vulnerabilities and potential attack vectors.
3.4.1 System Baselining	Employ System Baselining	Detecting unauthorized or malicious activity often relies on monitoring system changes. If security controls are not consistently and effectively implemented across all systems, or if configurations vary widely, it becomes harder to detect issues and ensure proper protection.	We design and document system baselines that specify the security configurations applied to each system, ensuring consistent and secure setups.
3.4.2 Security Configuration Enforcement	Enforce Security Configurations	Enforcing security configurations as part of a system baseline is essential to ensure the necessary restrictions and protections are in place. Without consistent enforcement, systems are more vulnerable to risks and potential compromise.	We enforce system baselines using configuration and conditional access policies to ensure proper and consistent installation.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Manage Baseline Changes: Use a formal process to review and approve system changes, and analyze their security impact before making updates.			
Practices Affected	**Tesseract Block**	**Risk**	**Mitigation**
3.4.3 System Change Management	Perform Change Management	Monitoring for unauthorized or malicious activity often depends on detecting system changes. If changes are not managed, it becomes harder to spot unauthorized actions and increases the risk that security configurations will be compromised.	We use a change management process to ensure all changes are planned and evaluated for security concerns.
3.4.4 Security Impact Analysis	Perform Security Impact Analyses	Any change to a system can introduce new vulnerabilities or risks, potentially weakening security controls and increasing the likelihood of exploitation or compromise.	We use a change management process to ensure all changes are planned and evaluated for security concerns.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Outcome	Ardalyst CSF 2.0 Step
Establish and Maintain Secure Endpoints	Protect

For endpoints—like laptops, desktops, and mobile devices—baselines are especially important because these devices are used directly by people and can be exposed to more risks. Endpoint baselines should be tailored to the specific tasks users perform, making sure each device has the right protections for its role.

Manage Endpoint Configurations: Design and enforce rules for the application of endpoint configuration options			
Practices Affected	**Tesseract Block**	**Risk**	**Mitigation**
3.4.8 Application Execution Policy	Limit Optional Software - Employ a denylist	Software installation not only introduces new attack vectors but also adds functionality that may contain vulnerabilities. Users may inadvertently increase system risk by installing software that is unapproved or insecure.	We use a denylist to block installation of known malicious software.
3.4.5 Access Restrictions For Change	Restrict Access for Change - No Physical CUI Systems	Changes to systems can intentionally or accidentally weaken an organization's security posture. If changes are not properly controlled or documented, the risk of introducing vulnerabilities or degrading security increases significantly.	Digital systems use logical restrictions, particularly for privileged accounts and functions, to control and monitor changes.
3.4.9 User-Installed Software	Restrict Software Installation - User Installation Allowed with Denylist	Installing software can introduce new vulnerabilities or serve as an attack vector. Users may unknowingly expose systems to additional risks by installing unapproved or insecure software, increasing the likelihood of compromise.	Employees who must install software are trained to complete a security impact analysis before installation, reducing associated risks.
3.13.4 Shared Resource Control	Control Shared Resources - Shared Resources Present	Shared resources can lead to accidental or intentional data compromise, as not all users may be authorized to access the sensitive data stored there. This lack of segregation increases the risk of unauthorized disclosure.	We limit data transfer risks on shared systems by using inherited controls and restricting administrator access, minimizing the chance of unauthorized data access.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

3.13.13 Mobile Code	Control Mobile Code	Mobile code embedded in websites or emails is a common and easily exploited attack vector. Such code can execute automatically, potentially compromising systems or data without the user's knowledge.	We use malicious code protection tools within our enclave to control and mitigate the risks associated with mobile code.

Manage VPN/SWG Access: Design and enforce rules regarding endpoint remote connection technology			
Practices Affected	**Tesseract Block**	**Risk**	**Mitigation**
3.13.7 Split Tunneling	Prevent Split Tunneling - VPN or SWG Not Present	Split tunneling allows a system to access both local network resources and those protected by a secure tunnel, creating a potential attack vector. This dual access can expose sensitive data to threats from less secure networks.	We eliminate split tunneling risks by not using tunneling devices.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Outcome	Ardalyst CSF 2.0 Step
Establish and Maintain Secure Boundaries	Protect

External boundaries, such as firewalls and secure gateways, protect your organization's network from outside threats by controlling how data enters and leaves your systems. For larger or more complex networks, internal boundaries—like network segmentation and access controls—can help limit access within your organization and reduce the risk of unauthorized activity.

Manage Network Devices: Design and enforce configurations for network devices and supported ports and protocols

Practices Affected	Tesseract Block	Risk	Mitigation
3.1.16 Wireless Access Authorization	Authorize Wireless Access - No Managed WAPs, No Managed Devices Capable of Connecting to Unmanaged WAPs.	Wireless networks can extend beyond physical boundaries, making them accessible from outside secure areas. Traffic on these networks, especially public ones, is susceptible to interception and unauthorized monitoring.	We eliminate wireless network risks by not using any in scope CUI devices capable of connecting to wireless access points.
3.1.17 Wireless Access Protection	Protect Wireless Access - No Managed WAPs, Connection to Unmanaged WAPs Not Permitted.	Wireless access increases organizational risk because it is easier to access than wired networks and can sometimes be reached from outside the physical security perimeter, making it more vulnerable to unauthorized use.	We eliminate wireless network risks by prohibiting all wireless access within our environment.
3.4.7 Nonessential Functionality	Limit Nonessential Functionality	Enabling non-essential system functions expands the attack surface and raises the likelihood of unauthorized use or exploitation, as unnecessary features may introduce vulnerabilities or be misused.	We reduce risk by limiting nonessential system functionality, preventing its use in risky or unauthorized ways.
3.13.6 Network Communication By Exception	Deny Network Communication by Default	Allowing broad network traffic to ensure functionality during configuration or troubleshooting can expose the network to multiple attack methods, increasing the risk of unauthorized access or exploitation.	We configure boundary protection devices to deny network access by default, permitting only essential traffic to enhance security.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Manage VOIP: Design and enforce configuration options for VOIP systems			
Practices Affected	**Tesseract Block**	**Risk**	**Mitigation**
3.13.14 Voice Over Internet Protocol	Control VOIP	VOIP systems can create new risks by serving as a vector for attacks or eavesdropping. These systems may be targeted to intercept communications or gain unauthorized access to the network.	We restrict VOIP system use to authorized users and monitor Microsoft Teams activity, reducing the risk of unauthorized access to restricted data.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Outcome	Ardalyst CSF 2.0 Step
Employ Secure Authentication Mechanisms	Protect

Authentication is how you confirm someone's identity when they try to access your systems. Because attackers often target these methods, using strong and modern authentication helps lower the risk of unauthorized access to your organization's resources.

Manage Authentication: Design and enforce rules to control authentication processes and allowable authentication methods			
Practices Affected	**Tesseract Block**	**Risk**	**Mitigation**
3.5.3 Multifactor Authentication	Employ Multifactor Authentication	Malicious actors use a variety of techniques to compromise account passwords, including phishing, brute-force attacks, and exploiting weak or reused passwords, increasing the risk of unauthorized access.	We require multi-factor authentication to reduce risks associated with password-only or single-factor authentication methods.
3.1.10 Session Lock	Threshold for Session Lock	Leaving sessions unattended creates an opportunity for malicious actors to access systems or data without authorization, increasing the risk of compromise during periods when no user is present.	We lock sessions after a defined period of inactivity to prevent unauthorized access.
3.1.8 Unsuccessful Logon Attempts	Threshold for Account Lockout	Multiple consecutive login attempts can signal malicious activity, such as brute-force attacks, where an attacker tries to gain unauthorized access by repeatedly guessing credentials.	We lock accounts after a set number of consecutive failed login attempts to prevent unauthorized access.
3.13.15 Communications Authenticity	Protect Communications Authenticity	Malicious actors can hijack, spoof, or otherwise compromise communication sessions, allowing them to intercept, alter, or impersonate legitimate communications and gain unauthorized access.	Our systems automatically verify the authenticity of communications.
3.5.4 Replay-Resistant Authentication	Employ Replay-Resistant Authentication	Attackers can target authentication systems using replay attacks, where they intercept and reuse valid authentication data to gain unauthorized access to systems or data.	We require replay-resistant authentication methods to protect against replay attacks.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Manage Identities: Design and enforce rules for the issuance and maintenance of identities			
Practices Affected	Tesseract Block	Risk	Mitigation
3.5.6 Identifier Handling	Disable Inactive Identifiers	Identifiers that are not actively used or monitored can be exploited by malicious actors to gain unauthorized access to systems and data, increasing the risk of compromise.	We automatically disable inactive identifiers after a set period, reducing the risk of unauthorized access through dormant accounts.
3.5.5 Identifier Reuse	Prevent Identifier Reuse	Authentication systems use identifiers to assign access permissions. If an identifier is deactivated but reused, a malicious actor could exploit it to impersonate a user or compromise the account, leading to unauthorized access.	Our systems automatically prevent the reuse of identifiers.

Manage Passwords: Design and enforce rules for the generation and maintenance of passwords			
Practices Affected	Tesseract Block	Risk	Mitigation
3.5.7 Password Complexity	Enforce Password Complexity	Simple passwords are vulnerable to compromise, as they can be easily guessed or cracked by attackers using automated tools or common password lists.	Our systems enforce password complexity requirements and require multi-factor authentication to strengthen account security.
3.5.8 Password Reuse	Limit Password Reuse	Changing passwords helps prevent attackers from maintaining access if a password is compromised. If systems allow consecutive reuse of the same password, this defense is weakened, making it easier for attackers to retain access.	We configure systems to prevent password reuse, and where not possible, enforce this requirement through policy.
3.5.9 Temporary Passwords	Enforce Temporary Password Change	Temporary passwords issued during account creation are often known by multiple people and may be transmitted insecurely, increasing the risk that unauthorized individuals could use them to gain access before the password is changed.	We require temporary passwords to be changed at first login, enforcing this through system configuration or policy as needed.
3.5.10 Cryptographically -Protected Passwords	Use Cryptographically -Protected Passwords	Storing or transmitting passwords without encryption exposes them to interception or theft, significantly increasing the risk that attackers could compromise accounts and gain unauthorized access.	Administrators are required to use encrypted transmission methods when communicating password information.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

3.5.11 Obscure Feedback	Obscure Feedback	Authentication systems often provide feedback, such as displaying passwords as they are typed, to help users enter credentials correctly. However, this feedback can be observed by unauthorized parties, increasing the risk of password compromise.	Our systems automatically obscure password and authentication feedback to prevent observation by unauthorized parties.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Outcome	Ardalyst CSF 2.0 Step
Control and Secure Your Devices	Protect

Devices like USB drives and smartphones need extra attention because they're easy to lose, can be used to move data in and out of your organization, and are common targets for malware or unauthorized access.

Manage Mobile Devices: Design and enforce rules for the use of mobile devices such as laptops and smartphones

Practices Affected	Tesseract Block	Risk	Mitigation
3.1.18 Mobile Device Connection	Control Mobile Device Connections - Mobile Devices Not Permitted	Mobile computing platforms and devices, like laptops and smartphones, enhance workforce flexibility but also expand the attack surface. As these devices leave the enclave's physical boundary and use wireless connectivity, they increase the risk of data loss and exposure to internet-based threats.	We eliminate mobile device risks by prohibiting their connection to the enclave.
3.1.19 Encrypt CUI On Mobile	Encrypt Mobile Devices and Mobile Computing Platforms - Mobile Computing Platforms and Mobile Devices Not Permitted	Mobile computing platforms and devices, such as laptops and smartphones, increase the risk of data loss or compromise because they can carry sensitive data outside the enclave's physical boundaries, making it harder to control and protect the information.	We eliminate the risk of CUI compromise on laptops or mobile devices by not allowing any mobile computing platforms or devices to contain CUI.

Manage Portable Storage Devices: Design and enforce rules for the use of portable storage devices such as USB drives

Practices Affected	Tesseract Block	Risk	Mitigation
3.1.21 Portable Storage Use	Control Portable Storage Use in External Systems - Portable Storage Not Permitted	Connecting portable storage devices to external or unmanaged systems can introduce malware or lead to data loss, as these devices may transfer malicious software or expose sensitive data to unauthorized environments.	We eliminate all risks associated with portable storage devices by banning their use entirely.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

3.8.7 Removeable Media	Control Removable Media - Removable Media Not Permitted	Removable media like USB drives, due to their small size and portability, are especially vulnerable to loss or theft, increasing the risk that sensitive data stored on them could be compromised.	We eliminate risks associated with removable media by prohibiting their use entirely.
3.8.8 Shared Media	Prevent Shared Portable Storage Use - Portable Storage Not Permitted	Sharing portable storage devices among users increases the risk of loss and reduces accountability for their protection. Additionally, not all users may be authorized to access the data, raising the risk of unauthorized disclosure.	We eliminate the risk of data loss from shared portable storage devices by prohibiting their use.

Manage Collaborative Computing Devices: Design and enforce rules for the use of collaborative computing devices such as conference room cameras and microphones

Practices Affected	Tesseract Block	Risk	Mitigation
3.13.12 Collaborative Device Control	Control Collaborative Devices - No Collaborative Devices In Scope	Collaborative devices, such as conference room equipment and smart whiteboards, often transmit audio and video. If activated remotely by a malicious actor or left on unintentionally, they can cause loss of control over CUI data.	We eliminate risks associated with collaborative computing devices by prohibiting their use.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Outcome	Ardalyst CSF 2.0 Step
Manage Your Vulnerabilities	Protect

New security weaknesses, called vulnerabilities, are discovered all the time. These can exist in software, hardware, or even in how systems are set up. It's important for your organization to stay informed about the latest risks, regularly update systems, and apply patches or fixes as soon as possible. Managing vulnerabilities also means knowing which ones matter most to your organization and making sure they're addressed quickly to reduce the chance of a security incident.

Manage Maintenance Activities: Design and implement a process for routine system maintenance

Practices Affected	Tesseract Block	Risk	Mitigation
3.7.4 Media Inspection	Methods for Diagnostic Removable Media Inspection - Any Removable Media Not Permitted	Diagnostic tools and their media, used during maintenance or troubleshooting, can serve as attack vectors if they are compromised or introduce malware, increasing the risk to systems and data.	We do not permit the use of any removable media, including diagnostic and test program media, eliminating associated risks.
3.7.1 Perform Maintenance	Perform Maintenance	Systems that are not regularly maintained may miss critical patches and security updates, making them more vulnerable to exploitation and compromise by attackers.	We use various technologies to ensure all systems receive timely patches and updates.

Manage and Remediate Vulnerabilities: Design and implement a process for vulnerability detection and remediation

Practices Affected	Tesseract Block	Risk	Mitigation
3.11.3 Vulnerability Remediation	Perform Vulnerability Remediation	All systems contain vulnerabilities that are regularly discovered by both security professionals and attackers. Failing to patch these vulnerabilities increases the organization's attack surface and the risk of exploitation.	We routinely scan systems for vulnerabilities and use a vulnerability management process to remediate identified issues.
3.14.1 Flaw Remediation	Flaw Remediation	Configuration or operational flaws exist in all systems. If these flaws are not addressed, they can expand the organization's attack surface and increase the risk of compromise.	We routinely scan systems for vulnerabilities and use a vulnerability management process to remediate identified issues.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

3.11.2 Vulnerability Scan	Perform Vulnerability Scanning	All systems contain vulnerabilities that are regularly discovered by both security professionals and attackers. Failing to patch these vulnerabilities increases the organization's attack surface and the risk of exploitation.	We routinely scan systems for vulnerabilities and use a vulnerability management process to remediate identified issues.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Outcome	Ardalyst CSF 2.0 Step
Collect, Curate and Analyze Your Log Data	Detect

Setting up good logs means you'll have lots of helpful information to spot mistakes or suspicious activity. You need to collect, organize, monitor, and analyze this data so your organization can understand what's happening and respond to issues.

Collect Logs: Design and implement a process for the collection, maintenance and review of logs.			
Practices Affected	**Tesseract Block**	**Risk**	**Mitigation**
3.3.1 System Auditing	Duration of Log Retention	As log data accumulates, storage costs can rise. If events or incidents are discovered late, necessary log data may have already been deleted, hindering investigations and response efforts.	We retain audit logs for ninety (90) days to support monitoring and compliance.
3.3.2 User Accountability	Ensure User Accountability	If audit logs do not link actions to specific users, it becomes difficult to identify and address unauthorized or malicious activity, complicating investigations and remediation efforts.	All audit logs record the user identity associated with each logged activity, supporting accountability and traceability.
3.3.3 Event Review	Perform Event Review	Extensive audit logs can generate large data sets, leading to higher costs, delayed detection of malicious activity, and false positives that consume organizational resources and complicate security monitoring.	We routinely review logged events and adjust event collection based on findings.
3.3.7 Authoritative Time Source	Provide Authoritative Time Source	Audit logs lacking correlation with an authoritative time source make it difficult to determine the sequence of events, complicating efforts to identify and remediate unauthorized or malicious activity.	All audit functionality is synchronized with an authoritative time source to ensure consistent and accurate event logging.

Protect Logs: Implement techniques to protect logs from accidental or malicious interference			
Practices Affected	**Tesseract Block**	**Risk**	**Mitigation**
3.3.4 Audit Failure Alerting	Monitor Audit Logging Failure	Failures in audit log collection can create gaps, making it harder to identify and remediate unauthorized or malicious activity due to missing or incomplete records.	Our auditing systems alert security administrators if previously collected logs are no longer received, indicating a logging failure.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

3.3.8 Audit Protection	Employ Audit Protection	If audit logs are modified or deleted by malicious or careless actors, it can hinder or prevent the identification and remediation of unauthorized or malicious activity.	Access to audit logs and logging functions is restricted to security administrators, reducing the risk of unauthorized log manipulation.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Outcome	Ardalyst CSF 2.0 Step
Monitor and Protect Your Endpoints	Detect

Since devices like laptops and phones connect users to your systems, it's important to monitor how they're used. Special monitoring can help you spot the difference between normal activity and anything suspicious or unauthorized. This includes tracking login attempts, unusual data transfers, and other behaviors that might signal a security issue.

Employ Malicious Code Protection: Design and implement a process for implementing and maintaining malicious code protection

Practices Affected	Tesseract Block	Risk	Mitigation
3.14.4 Update Malicious Code Protection	Update Malicious Code Protection	Malicious actors frequently update and release new malicious code. Organizations that do not keep their code protection systems current are more susceptible to these evolving threats.	We update malicious code protection in real time to ensure defenses remain current and effective.
3.14.2 Malicious Code Protection	Protect from Malicious Code	Malicious code can bypass protective controls and be delivered through various methods. Systems lacking detection and response capabilities are especially vulnerable to compromise from such attacks.	We deploy malicious code protection on endpoints to intercept and neutralize threats before compromise, and to alert us if malicious code is executed.
3.14.5 System and File Scanning	Perform System & File Scanning	Malicious code may execute on a timer or when files are downloaded, opened, or run. Organizations that lack both periodic and real-time scanning are especially vulnerable to these types of attacks.	Our malicious code protection system performs routine and on-access scans to minimize the risk of undetected or unmitigated malicious code execution.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Outcome	Ardalyst CSF 2.0 Step
Monitor and Protect Your Networks and Boundaries	Detect

Monitoring activity on your network and at its boundaries provides important information about who is using your systems and whether their actions are authorized. By keeping an eye on things like data transfers, connection attempts, and traffic patterns, you can quickly spot unusual or unauthorized activity and respond before it becomes a bigger issue.

Protect System Boundaries: Design and implement methods for protecting system boundaries

Practices Affected	Tesseract Block	Risk	Mitigation
3.13.1 Boundary Protection	Employ Boundary Protection	Most attacks originate from remote locations via the internet. Systems exposed to the internet are at higher risk and can be compromised rapidly if not properly secured.	Systems exposed to the internet are configured to block access from untrusted sources.
3.13.5 Public-Access System Separation	Separate Publicly Accessible Systems - No Publicly Accessible System Components	Hosting publicly accessible systems increases the risk of compromise due to their exposure. These systems are more likely to be targeted by attackers seeking vulnerabilities.	We eliminate risks from publicly accessible systems by not allowing them in our controlled enclave.

Manage Remote Access: Design and implement methods for providing secure remote access

Practices Affected	Tesseract Block	Risk	Mitigation
3.1.12 Control Remote Access	Control Remote Access - ND	Remote systems, including those in the cloud, are outside the organization's physical protection controls. While cloud providers offer some safeguards, remote access can still be exploited by unauthorized parties.	We reduce unauthorized remote access risk by specifying permitted access types and configuring systems to reject connections from unauthorized devices, untrusted locations, or non-compliant systems.
3.1.14 Remote Access Routing	Control Remote Access Routing - No VPN or SWG Present	Using unmanaged remote access methods expands the organization's attack surface, making it more vulnerable to unauthorized access and potential security breaches.	We do not allow Virtual Private Networks (VPNs) or Secure Web Gateways (SWGs). The only managed access control point present is the cloud service provider.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Outcome	Ardalyst CSF 2.0 Step
Monitor and Respond to Advisories and Threat Intel	Detect

Cybersecurity is always evolving, with new threats and vulnerabilities being discovered all the time. Staying informed means regularly following trusted sources like security advisories, industry news, and updates from software vendors. These activities help your organization respond quickly to new risks and keep your systems protected against the latest threats.

News Review: Design and implement a process of reviewing and responding to news and intelligence sources

Practices Affected	Tesseract Block	Risk	Mitigation
3.14.3 Security Alerts and Advisories	Monitor Security Alerts & Advisories	The security landscape evolves as new threats emerge and targets shift. Organizations that do not monitor alerts and advisories risk having outdated security postures that do not align with the current threat environment.	We monitor intelligence and news sources, producing weekly overviews and emerging threat notifications to address issues requiring immediate action.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Outcome	Ardalyst CSF 2.0 Step
Monitor and Manage Your Security Events	Detect

Security events are activities or changes in your systems or network that could indicate a potential risk. Not every event is a problem, but it's important to review and investigate them to decide if action is needed. Some events may reveal vulnerabilities or lead to incidents that require a formal response.

Manage Logs: Design and implement a process to correlate, reduce, and report on events			
Practices Affected	**Tesseract Block**	**Risk**	**Mitigation**
3.3.5 Audit Correlation	Perform Audit Correlation	Audit logs generated from multiple sources can produce overwhelming volumes of events, making it challenging to identify unlawful, unauthorized, suspicious, or unusual activities.	We configure systems for automatic audit reduction, correlation, and reporting to better identify unlawful, unauthorized, suspicious, or unusual activity.
3.3.6 Reduction and Reporting	Provide Audit Reduction and Reporting Capabilities	Audit logs generated from multiple sources can produce overwhelming volumes of events, making it challenging to identify unlawful, unauthorized, suspicious, or unusual activities.	We configure systems for automatic audit reduction, correlation, and reporting to better identify unlawful, unauthorized, suspicious, or unusual activity.

Monitor Logs: Design and implement a process to monitor and alert on security events			
Practices Affected	**Tesseract Block**	**Risk**	**Mitigation**
3.14.6 Monitor Communications For Attacks	Monitor Security Logs	Audit logs generated from multiple sources can produce overwhelming volumes of events, making it challenging to identify unlawful, unauthorized, suspicious, or unusual activities.	We configure systems for automatic audit reduction, correlation, and reporting to better identify unlawful, unauthorized, suspicious, or unusual activity.
3.14.7 Identify Unauthorized Use	Identify Unauthorized Use	When users do not follow established policies and procedures, they expose the organization to risks that vary depending on the specific policy or procedure violated, potentially leading to security incidents or compliance issues.	We require users to sign an Acceptable Use Policy, identify authorized use, and monitor for policy violations, enabling retraining or corrective action as needed to reduce system-wide risks.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Outcome	Ardalyst CSF 2.0 Step
Conduct Your Incident Response	Respond

Some security problems, called incidents, need special attention. These can include things like unauthorized access, data loss, or other events that may require you to notify affected individuals or meet legal and regulatory reporting requirements.

Respond to Incidents: Design and use an incident response plan			
Practices Affected	**Tesseract Block**	**Risk**	**Mitigation**
3.6.1 Incident Handling	Perform Incident Handling	No system is completely secure, and the severity of incidents depends on how quickly they are detected and addressed. Organizations lacking incident response capabilities face a higher risk of loss when incidents occur.	We maintain an incident response plan, practiced annually through tabletop simulations, which includes proper reporting procedures.
3.6.2 Incident Reporting	Perform Incident Reporting	Failure to report incidents can result in legal or contractual violations and associated penalties. Organizations without effective incident reporting mechanisms are at greater risk of non-compliance and potential sanctions.	We maintain an incident response plan, practiced annually through tabletop simulations, which includes proper reporting procedures.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Outcome	Ardalyst CSF 2.0 Step
Assess, Mature and Document Your Program	Evolve

Keeping good records helps you get ready for audits and reviews, and makes it easier to check your own work. Regular self-checks and outside reviews help your cybersecurity program get better over time.

Document the Program: Develop documentation and track planned improvements			
Practices Affected	Tesseract Block	Risk	Mitigation
3.12.2 Operational Plan of Action	Employ an Operational Plan of Action	Effective security programs identify deficiencies and vulnerabilities. Organizations that fail to create remediation plans are at greater risk of experiencing security incidents due to unresolved issues.	We use an operational plan of action to track deficiencies and document remediation plans, ensuring continuous improvement in our security posture.
3.12.4 System Security Plan	Employ a System Security Plan	Security is most effective when implemented as a coordinated, comprehensive plan. Applying security measures in a piecemeal or inconsistent manner increases the risk of gaps and weaknesses in the organization's defenses.	We maintain a system security plan that documents processes, configurations, and responsible parties, ensuring all team members understand their roles in maintaining security.

Assess the Program: Test the plan's capabilities and routinely assess compliance and effectiveness			
Practices Affected	Tesseract Block	Risk	Mitigation
3.6.3 Incident Response Testing	Perform Incident Response Testing	Incident response is challenging and stressful. Organizations that do not regularly practice their response procedures may perform poorly during actual incidents, increasing the likelihood and severity of negative outcomes.	We maintain an incident response plan, practiced annually through tabletop simulations, which includes proper reporting procedures.
3.12.1 Security Control Assessment	Perform Security Control Assessment	Security controls can become ineffective or misconfigured as time passes, raising the risk that the organization's security posture will deteriorate and vulnerabilities will go unaddressed.	We conduct annual self-assessments (or third-party assessments) to evaluate our security controls for compliance and effectiveness.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

3.12.3 Security Control Monitoring	Monitor Security Control Effectiveness	Over time, security controls can lose effectiveness, increasing the risk that the organization's overall security posture will degrade and become more susceptible to threats.	We routinely monitor security controls to ensure their ongoing effectiveness.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.