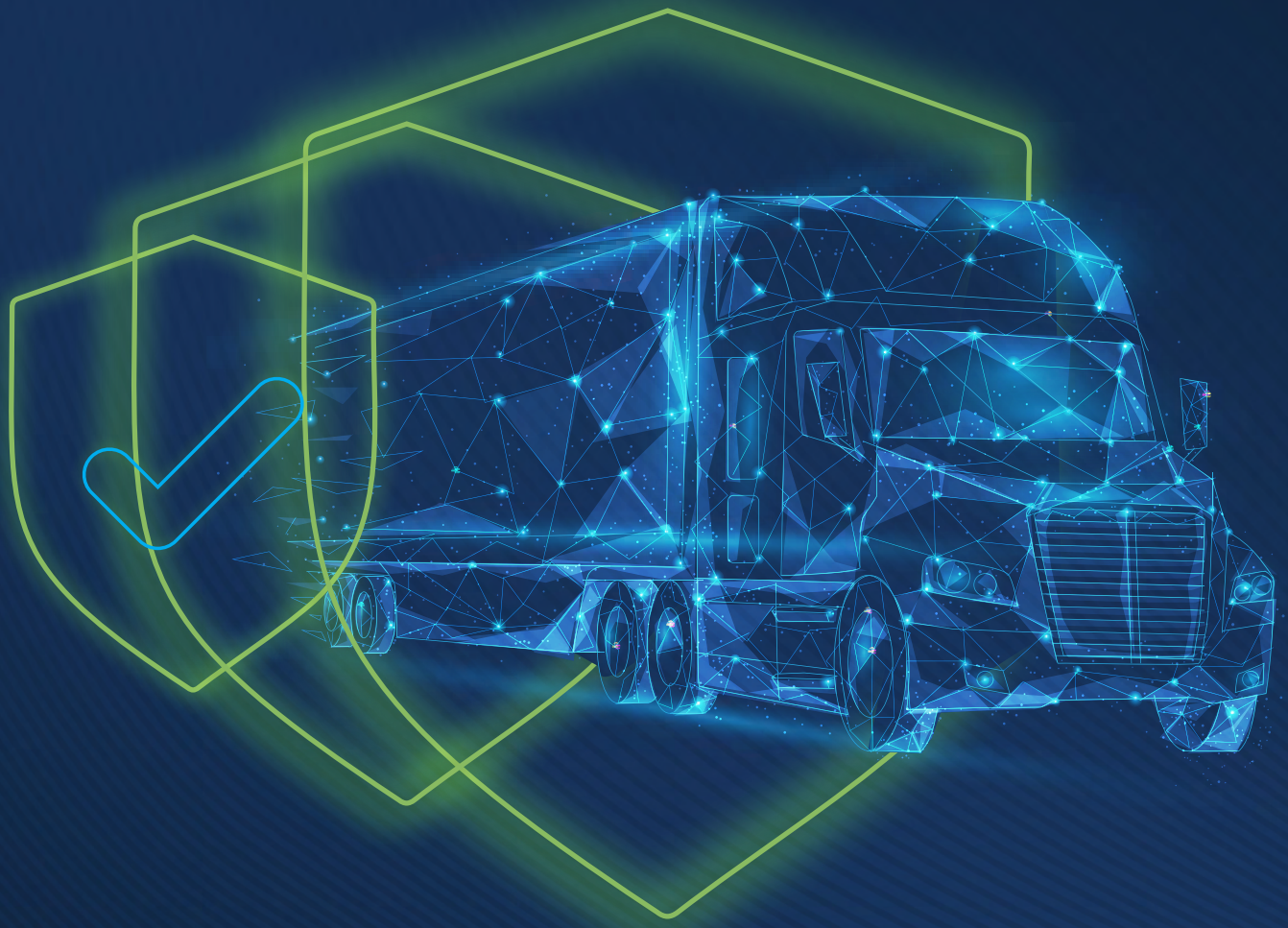
NMFTA CYBERSECURITY BEST PRACTICES GUIDEBOOK

Owner Operator & Small Fleet



As with any journey, your path to a hardened cybersecurity posture must start where you are today. No matter where that is, there are steps you can take now to protect yourself and the operation that you have built from cyberthreats.

NMFTA™
National Motor Freight Traffic Association, Inc.

CYBER

Table of Contents

Introduction

This guidebook contains an actionable list of cybersecurity control best practices, divided into four distinct maturity levels. These controls are based on a selection of industry standard cybersecurity frameworks, such as the National Institute for Standards & Technology's Cybersecurity Framework (NIST CSF 2.0) and the Center for Internet Security's 18 Critical Security Controls (CIS 18 v8.1) that have been tailored to the specific needs of the trucking industry as well as controls specifically designed for the requirements of trucking operations and their mobile assets.

While these controls represent the best-practice recommendations of the NMFTA cybersecurity team and provide a strong starting point for organizations to pursue their path to cybersecurity maturity, they are not designed to be an exhaustive list of all cybersecurity controls available to the trucking industry, nor do they provide any guarantee of complete or impenetrable defense from cyberattacks. For example, many systems and services within the modern enterprise come with several levels of optional security "out of the box" (e.g., SSL, TLS, and PKI security for transport layer protocols). The optimal configurations for these types of service options are not explicitly stated in this guide. The general rule should be to configure the most secure option that is practical in an organization's business environment. Cybersecurity programs and their individual requirements vary greatly from business to business, and depend largely on the specific operating infrastructure, business processes, staffing levels, and education, as well as the overall business risk tolerance of the business. Where applicable, this document contains references to additional resources and control frameworks that may be used to augment this best-practice guidebook, and to develop additional layers of controls for any business

This content and additional information can be found on the NMFTA cybersecurity website: www.nmfta.org/cybersecurity.

Intended Audience

This document is intended for owner operators and small fleets consisting of a small number of assets (+/- 50). This audience shares many characteristics and constraints when considering their overall cybersecurity requirements and program limitations. Some fleets with more than fifty assets may find this guidebook is still applicable in whole or in part to their business. Similarly, complex operations with fifty or fewer assets may find that some elements of their operation are not addressed in this document, and so the fleet size listed here is intended as a point of reference only and not a hard limit. If this guidebook does not cover all aspects of their operation, the related *NMFTA Cybersecurity Best Practices Guidebook - Mid-Size Fleets* may be a better fit for their business.

Assumptions

Several assumptions were made in the creation of the included list of controls regarding this guidebook's intended audience. These assumptions are as follows:

Assumption 1: Limited Human Resources

This guidance assumes that an owner operator or small fleet owner either handles their own information technology (IT) and cybersecurity tasks, has a part-time team member that handles these responsibilities in addition to other duties, or contracts these responsibilities out to a third-party managed service provider (MSP) or managed security services provider (MSSP).

Assumption 2: Minimal Operational and Technical Complexity

This guidance assumes that an owner operator or small fleet will have limited network complexity in their operation, and will have a small number of computers, tablets, mobile phones, network hardware, cloud assets, vehicles, telematics units, and software as a service (SaaS) platforms to consider when building out their cybersecurity program.

Assumption 3: Limited Budget Available

This guidance assumes that there will be limited budget available for IT and cybersecurity expenses. Considering this, the recommendations in this guidebook focus on low cost and free cybersecurity controls that create maximal positive impact on the cybersecurity posture and resiliency of the operation.

Document Structure

This document is organized into four sections, each representing a distinct cybersecurity maturity level as owner operators or small fleets progress in developing their cybersecurity program. The top recommended controls for each maturity level are included in each section. For every control listed, there will be an identification number, followed by a brief description, and the intended purpose or benefit of each respective control. After defining the control, several example implementations are provided. These do not represent, nor are they intended to include all possible implementations for the given control, but are included with the intent of providing insight into the many ways in which the control could be implemented if applicable in the specific operating environment of the business following this best practice guide. The last item included in each control section will be a cross-reference to any related NIST CSF 2.0 controls or CIS 18 v8.1 safeguards for further information.

Prerequisites: Owner-Operator Controls - Tier One

As an owner operator, personal cybersecurity and online cyber hygiene go hand-in-hand with business cybersecurity. It is important to take steps to safeguard personal identity and credit to ensure continuity of operations and scalability of business. Freezing credit when not actively seeking new lines of credit, and enabling active credit monitoring with alerts for any new credit activity, are low-cost options with a significant impact on financial security. In addition, the top five cybersecurity controls in this section are those that owner operators and small fleets should implement immediately. These controls are representative of the minimum baseline requirements for fundamental cybersecurity controls, and are possible with little to no financial burden and limited internal technical resources.[1]

OOSF.01.1 - Keep Software and Operating Systems Updated

Keeping your operating systems and software updated is crucial for safety, reliability, and smooth functionality. Updates protect against potential security risks by fixing known issues that threat actors might try to exploit. They also improve performance, helping systems run better and avoid crashes, while often adding new features to keep tools current. By staying up to date, you reduce the chances of unexpected issues, stay in line with industry standards, and avoid many potential risks. In short, you can think of software and operating system updates like a preventative maintenance program for your computer assets.

Implementation Examples

Example 1: Turn on automatic updates for software and operating systems whenever it is an option.

Example 2: Apply all recommended patches released by software vendors, especially those related to new vulnerabilities and those designed to enhance security.

Example 3: Limit what software gets installed on work computers and mobile devices to work-related software. Uninstall and remove unauthorized software and services.

Example 4: Decide on, document, and follow through with an action plan to address software and operating systems that are reaching the end of manufacturer's support.

Example 5: Replace end-of-life software and service versions with supported, maintained versions.

Mappings to External Control Standards

- NIST PR.PS-02: Software is maintained, replaced, and removed commensurate with risk.
- CIS 18 v8.1: Safeguard 2.2: Ensure authorized software is currently supported.

1 This level of cybersecurity maturity maps to NIST maturity level: Partial

OOSF.01.2 – Back Up Important Files

Backing up important files is crucial to protect against data loss, and the "3-2-1" backup rule makes it easy to remember a smart approach: Keep **3 copies** of your data, store **2 copies on different types of media** (like an external drive and a cloud service), and keep **1 copy off-site** for added security. This strategy reduces the potential impact of hardware failure, accidental deletion, and cyberthreats. While backing up the files is a core component of a successful backup solution, testing those backups is an equally important and often overlooked requirement. It is imperative that all backups are regularly tested for validity and the restoration process is tested and rehearsed so that required data can be reliably restored in the event of an incident.

Implementation Examples

Example 1: Ensure that all important data is backed up regularly. Understand tolerance for data loss and set the backup schedule accordingly.

Example 2: Configure automated cloud backup solutions.

Example 3: Store an offline copy of the daily backup in a secure, offsite location such as a safety deposit box or cloud storage vault.

Example 4: Regularly test restoration of files from all backup solutions.

Mappings to External Control Standards

- NIST PR.DS-11: Backups of data are created, protected, maintained, and tested.
- CIS 18 v8.1 Safeguard 11.2: Perform Automated Backups.
- CIS 18 v8.1 Safeguard 11.3: Protect Recovery Data.
- CIS 18 v8.1 Safeguard 11.4: Establish and Maintain an Isolated Instance of Recovery Data.
- CIS 18 v8.1 Safeguard 11.5: Test Data Recovery.

OOSF.01.3 – Use Strong, Unique Passwords

Using strong, unique passwords and changing all default credentials is essential for securing your accounts and devices. Aim to create passwords that are at least 12 characters long and include a mix of letters, numbers, and symbols—this complexity makes them much harder for threat actors to guess or crack using brute-force attacks. Default passwords, often set by manufacturers, are well-known and easily exploitable, so replacing them with secure, personalized passwords is critical. Longer and more complex passwords (particularly when used in combination with multi-factor authentication (MFA)[2] add an extra add an extra layer of security, significantly reducing the risk of a successful account compromise.

Implementation Examples

Example 1: Change default credentials on all devices and hardware before using them.

Example 2: Do not use names, important dates, favorite teams, brands, or any other personal information in passwords. This type of information is commonly used by threat actors to seed brute-force attacks.

Example 3: Use a password management app to automatically generate and securely store all passwords.

Example 4: Do not share passwords between employees. Use a unique password for every user.

Mappings to External Control Standards

- NIST PR.AA-03: Users, services, and hardware are authenticated.
- CIS 18 v8.1 Safeguard 5.2: Use Unique Passwords.

2 See Also IO.01.5 Require Multifactor Authentication (MFA)

OOSF.01.4 – Require Passwords on All Devices

Requiring a password on all devices—like computers, tablets, mobile phones, and network hardware —is a simple, effective step toward keeping your data and accounts secure. Password protection acts as the first line of defense, preventing unauthorized access if a device is lost, stolen, or left unattended. Passwords help protect sensitive information and prevent unauthorized changes to security settings. This safeguard reduces the risk of breaches, identity theft, unauthorized access to personal or work networks, helping to ensure that only trusted users can access your device's data and settings.

Implementation Examples

Example 1: Require pin (minimum) or biometric (preferred) authentication for mobile devices.

Example 2: Enforce minimum complexity and/or length requirements for pins and passwords.

Example 3: Disable guest access and require password protected accounts on all computers.

Mappings to External Control Standards

- NIST PR.AA-03: Users, services and hardware are authenticated.
- CIS 18 v8.1 Safeguard 5.2: Use Unique Passwords.

OOSF.01.5 – Require Multi-Factor Authentication

Implementing multi-factor authentication (MFA) is a highly effective way to add an extra layer of security to your accounts and devices. MFA requires users to verify their identity in two or more ways, typically combining something you know (like a password) with something you have (like a phone or security token) or something you are (like a fingerprint or facial scan). This makes it much harder for threat actors to gain access, even if they compromise your username and password. By enabling MFA, you significantly reduce the risk of unauthorized access, helping to protect your company data and accounts from cyberthreats.

Implementation Examples

Example 1: Set up an authenticator app for use as an MFA token for online accounts.

Example 2: Configure SMS or Text alerts for account access verification. While not the most secure MFA method available, even SMS codes transmitted to a mobile number to verify access provide a significant increase in the difficulty of compromising an account.

Example 3: Configure facial ID or fingerprint authentication for access to mobile devices.

Example 4: Require MFA for all administrative accounts.

Mappings to External Control Standards

- NIST PR.AA-03: Users, services and hardware are authenticated.
- CIS 18 v8.1 Safeguard 6.3: Require MFA for Externally Exposed Applications.
- CIS 18 v8.1 Safeguard 6.4: Require MFA for Remote Network Access.
- CIS 18 v8.1 Safeguard 6.5: Require MFA for Administrative Access.

Additional Reading

For more information on the core cybersecurity controls that make up the foundation of a solid cybersecurity program please consult the following sites:

www.nmfta.org/cybersecurity
https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe

Initial: Owner Operator Controls - Tier Two

Tier two contains the next set of controls that owner operators and small fleets should implement after cybersecurity fundamentals are addressed. These controls will begin to turn a business into a hardened target, further decreasing the likelihood that the business will become the victim of a cybersecurity crime of opportunity due to poor cybersecurity practices. There are additional controls in this tier and further study of the NIST CSF and CIS 18 v8.1 standards is recommended. The controls in this section represent the most cost effective, highest impact controls at this maturity level.[3]

OOSF.02.1 – Basic Cybersecurity User Awareness Training Program

Implementing a basic cybersecurity user awareness training program is an affordable and effective way to empower users to recognize and avoid common security threats. This type of program educates employees on key topics like phishing scams, safe internet usage practices, secure password management, and how to identify suspicious emails or attachments. It can also cover policies on handling sensitive data and guidelines for reporting potential security incidents. By providing this training, businesses can help to ensure that every employee understands the role that they play in protecting sensitive information. This will reduce the likelihood of human errors that could lead to breaches or successful attacks.

Implementation Examples

Example 1: Provide mandatory basic cybersecurity user awareness training to all employees and any other third parties that interact with internal company systems or assets.

Example 2: Provide training to personnel to help them recognize phishing and other social engineering attempts. Include information on how to properly report suspicious activity and basic cyber hygiene requirements.

Example 3: Ensure that all employees and contractors understand the immediate and potential consequences of cybersecurity policy violations to both the individual and the business.

Example 4: Periodically test employees on their cybersecurity awareness and compliance with required cybersecurity policies.

Mappings to External Control Standards

- NIST PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind.
- CIS 18 v8.1 Safeguard 14.1: Establish and Maintain a Security Awareness Program.

3 This level of cybersecurity maturity maps to NIST maturity level: Risk Informed

OOSF.02.2 – Deploy Endpoint Detection and Response Software

Deploying endpoint detection and response (EDR) software is a crucial step in enhancing cybersecurity by providing continuous monitoring and real-time analysis of potential threats across all devices in a network. EDR software helps detect, investigate, and respond to suspicious activities across computers, mobile devices, and servers. It offers advanced features like threat hunting, automated responses to block malicious actions, and detailed reporting to help security teams understand and mitigate risks. By implementing EDR, businesses can quickly identify and address potential threats before they lead to data breaches, strengthening overall security and improving incident response times.

Implementation Examples

Example 1: Monitor failed authentication attempts. These can be a sign of unauthorized credential use or a brute-force attack.

Example 2: Monitor endpoints for configuration changes that deviate from security baselines.

Example 3: Monitor both hardware and software for signs of tampering or unauthorized access.

Example 4: Proactively monitor endpoints for general cybersecurity health (e.g., missing patches, malware, unauthorized installations), and automate responses to prevent incidents and breaches.

Mappings to External Control Standards

- NIST DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events.
- CIS 18 v8.1 Safeguard 10.1: Deploy and Maintain Anti-Malware Software.
- CIS 18 v8.1 Safeguard 10.5: Enable Anti-Exploitation Features.
- CIS 18 v8.1 Safeguard 10.6: Centrally Manage Anti-Malware Software.

OOSF.02.3 – Have an Incident Response Plan

Having an incident response plan (IRP) is essential for preparing businesses to quickly and effectively address security incidents when they occur. An IRP outlines the steps to take during and after a cyberattack or data breach, including identifying the scope of the incident, containing the threat, eradicating the cause, and recovering affected systems. It also details roles and responsibilities, ensuring that everyone knows their part in the response process. By having a well-structured plan in place, businesses can minimize the impact of an incident, reduce downtime, and prevent further damage, while ensuring compliance with regulatory requirements and improving their overall resilience to future attacks. In trucking, a well-defined IRP should also include contact lists for drivers and customers to ensure continuity of communication during any potential incident. IRPs should be stored both digitally[4] and in hard copy to ensure availability during any type of incident.

Implementation Examples

Example 1: Establish contingency plans for incident response[5], business continuity[6], and disaster recovery[7]. Include guidelines for responding to and recovering from adverse events that can interfere with operations or endanger the organization's core mission.

Example 2: Confirm that all IRP documentation includes contact details and communication channels for all key personnel. Include details on standard incident handling, incident escalation procedures, and contingency planning in case of key personnel availability issues.

Example 3: Clearly communicate cybersecurity response plans (including any subsequent updates) to all responsible parties.

Mappings to External Control Standards

- NIST ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved.
- CIS 18 v8.1 Safeguard 17.1: Designate Personnel to Manage Incident Handling.
- CIS 18 v8.1 Safeguard 17.4: Establish and Maintain and Incident Response Process.
- CIS 18 v8.1 Safeguard 17.5: Assign Key Roles and Responsibilities.
- CIS 18 v8.1 Safeguard 17.6: Define Mechanisms for Communicating During Incident Response.

4 See also IO.01.2 Backup Important Files
5 Incident Response Plan (IRP)
6 Business Continuity Plan (BCP)
7 Disaster Recovery Plan (DRP)

OOSF.02.4 – Secure Wireless Networks

Encrypting all wireless networks with WPA2 or greater is crucial for protecting the confidentiality and integrity of data transmitted over Wi-Fi. WPA2 encryption helps prevent unauthorized access by ensuring that only authorized users can connect to the network. Securing wireless routers is equally important – by changing default login credentials[8] and disabling remote management, you reduce the risk of outsiders gaining control over your network settings. These steps protect against cyberthreats like eavesdropping and unauthorized network changes, safeguarding your data from attackers who might exploit weak or unsecured networks.

Implementation Examples

Example 1: Ensure that all wireless networks are configured with WPA2 encryption or stronger.

Example 2: Disable Wi-Fi Protected Setup and all other insecure or automated authentication methods for wireless networks.

Example 3: Configure strong, unique passwords for wireless network access.

Mappings to External Control Standards

- NIST PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected.
- NIST PR.PS-01: Configuration management practices are established and applied.
- CIS 18 v8.1 Safeguard 3.10: Encrypt Sensitive Data in Transit.
- CIS 18 v8.1 Safeguard 4.1: Establish and Maintain a Secure Configuration Process.
- CIS 18 v8.1 Safeguard 4.2: Establish and Maintain a Secure Configuration for Network Infrastructure.
- CIS 18 v8.1 Safeguard 12.6: Use of Secure Network Management and Communication Protocols.

8 See also IO.01.3 Use Strong, Unique Passwords

OOSF.02.5 – Implement a Least Privilege Account Access Policy

Implementing a least privilege account access policy is a fundamental security practice that limits user access to only the information and resources necessary for their job functions. By granting the minimum required permissions, businesses reduce the risk of accidental or intentional misuse of access to sensitive data and systems. This approach helps prevent unauthorized access to critical files, reduces the attack surface in the event of a potential breach, and limits the damage that could occur if an account is compromised. A least privilege policy also ensures better control over access management, making it easier to audit, monitor, and enforce security protocols, ultimately strengthening overall organizational security.

Implementation Examples

Example 1: Ensure that employees only have access to the systems and data required for their assigned job duties.

Example 2: Take all attributes of the requested resource into account during each authorization decision: Location, time and day of the week, and cyber health of the requesting endpoint.

Example 3: Revoke access rights immediately when employees change roles or leave the business.

Example 4: Do not grant access to any systems or data beyond the minimal access needed for the role.

Mappings to External Control Standards

- NIST PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties.
- CIS 18 v8.1 Safeguard 5.1: Establish and Maintain an Inventory of Accounts.
- CIS 18 v8.1 Safeguard 6.8: Define and Maintain Role-Based Access Control.

Additional Reading

Once you have implemented the controls outlined in this section, you will be well on the way to creating a well-designed and effective cybersecurity program. For more information on the controls that make up this tier of cybersecurity maturity, consult the following sites:

https://www.nmfta.org/cybersecurity
https://www.nist.gov/cyberframework
https://www.cisecurity.org/controls/v8
https://www.cisa.gov/cyber-guidance-small-businesses

Intermediate: Owner Operator Controls - Tier Three

Once the core controls are in place, it's time to focus on more advanced hardening techniques that will elevate the level of skill, sophistication, and resources required of a threat actor to compromise the operation. These controls will begin to move the business out of the range of a typical target of opportunity for threat actors.[9] Additional resources for the following two sections may be found at the end of this guidebook. Intermediate and advanced cybersecurity programs require extensive tailoring and scoping of a wide range of controls in order to effectively address the specific security concerns of the business. Please refer to the additional resources appendix for a list of documents and sites that will provide insights into these additional controls.

OOSF.03.1 – Inventory and Classify All Business Data

Inventorying and classifying all business data is a critical step in ensuring data security and compliance with applicable privacy regulations and security standards. Once you define and categorize all data based on its sensitivity and value to your business, you can apply the appropriate security controls and prioritize protection efforts. This process helps ensure that sensitive data, such as personally identifiable information (PII) or financial records, are protected with stricter controls, while less critical data is managed accordingly. Completing this important step will help you to better control access to data, assist in detection of threats and inappropriate use of data, and more effectively protect your data.

Implementation Examples

Example 1: Maintain a list of the designated data types of interest (e.g., personally identifiable information, protected health information, financial account numbers, business intellectual property, operational technology data).

Example 2: Monitor all new data to identify new instances of designated data types.

Example 3: Assign data classifications to designated data types through tags or labels.

Example 4: Track the provenance, data owner, and geolocation of each instance of designated data types.

Mappings to External Control Standards

- NIST ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained.
- CIS 18 v8.1 Safeguard 3.2: Establish and Maintain a Data Inventory.

9 This level of cybersecurity maturity maps to NIST maturity level: Repeatable

OOSF.03.2 – Designate Cybersecurity Roles and Responsibilities

Designating clear cybersecurity roles and responsibilities is essential for creating an accountable and structured security environment. By assigning specific duties to team members—such as monitoring threats, managing incident response, or overseeing compliance— businesses ensure that every aspect of cybersecurity is covered. This practice helps streamline communication, prevent gaps in security coverage, and clarifies who should take action in various scenarios, such as responding to incidents or conducting audits. Defining roles and responsibilities, as emphasized in NIST CSF and CIS 18 standards, not only strengthens the business's overall security posture but also enhances coordination, accountability, and responsiveness to evolving threats.

Implementation Examples

Example 1: Identify a security point person. Choose someone within the company to work with the service provider (or internal IT if applicable), ensuring that cybersecurity questions and tasks are addressed.

Example 2: Create a basic incident response plan (IRP) and assign primary incident responder duties to someone on the team. Outline who to call and what steps to take if a security issue arises, such as a hacked email account or suspicious activity.

Example 3: Assign someone to oversee sensitive data. Have a trusted person monitor access to critical data like payroll and customer records, ensuring that only authorized people can access, or modify this data.

Example 4: Designate a security awareness advocate. Pick a team member to promote safe practices, like using strong passwords, recognizing phishing emails, and to help organize regular security reminders or cybersecurity awareness training.

Mappings to External Control Standards

- NIST GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving.

OOSF.03.3 – Layered Network Access Controls

Implementing layered network access controls is a key strategy for protecting your business network by limiting access based on user roles and security levels. This approach creates multiple checkpoints, such as firewalls, virtual private networks (VPNs), and segmented networks, that control who can access specific areas and systems. By layering these controls, you make it harder for unauthorized users to move through your network and reach sensitive information, even if they breach one layer. This practice reduces the risk of data breaches, supports regulatory compliance, and aligns with cybersecurity frameworks like NIST CSF and CIS 18, creating stronger, more resilient network defenses.

Implementation Examples

Example 1: Use a secure Wi-Fi network with a strong password. Set up a secure, password protected Wi-Fi network for business use and avoid sharing it with non-employees or using it for personal devices.

Example 2: Enable a firewall on the router. Ensure that the firewall feature on the router is active to block unwanted access to the network and monitor for unusual activity.

Example 3: Implement device-based access controls. Only allow approved devices, like company laptops or tablets, to connect to the main business network. This limits network access to known devices, adding another layer of security.

Mappings to External Control Standards

- NIST PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.
- CIS 18 v8.1 Safeguard 3.12: Segment Data Processing and Storage Based on Sensitivity.

OOSF.03.4 – Internal Network Segmentation

Implementing internal network segmentation involves dividing your business's network into separate segments or sections, each with its own access controls. This practice prevents users from moving freely across the network, so if one part of the network is compromised, the threat remains contained to that segment. Network segmentation can help protect sensitive information, limit the impact of cyberattacks, and make it easier to monitor network activity for potential issues. For small companies, this approach strengthens security by ensuring that access to critical areas, such as financial records or fleet data, is limited to authorized users only.

Implementation Examples

Example 1: Separate financial systems from general operations. Isolate accounting and payroll systems from other parts of the network to protect sensitive financial data.

Example 2: Create a dedicated network segment for fleet management. Keep fleet management and maintenance systems on a separate network segment so that access is limited and closely monitored.

Example 3: Restrict internet access for certain segments. For sensitive areas like employee data, limit or block internet access to reduce direct exposure to online threats and browser-based attacks.

Example 4: Implement user-based access controls for each segment. Only allow access to specific segments for employees who need it, ensuring that data and systems are accessible only to relevant team members or departments.

Mappings to External Control Standards

- NIST PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.
- CIS 18 v8.1 Safeguard 3.12: Segment Data Processing and Storage Based on Sensitivity.

OOSF.03.5 – Virtual Private Network Required for all Remote Access

Requiring a virtual private network (VPN) for all remote access is essential for keeping your data secure when employees access the network from outside locations. A VPN creates an encrypted connection between the remote user and your internal network, preventing unauthorized access and lowering the risk of interception of data in transit. This is particularly important as more and more companies shift toward remote and hybrid workforces and the need for access to critical data and systems on the go increases. By using a VPN, you add a secure layer to protect your information, ensuring that only trusted individuals can connect to your network remotely.

Implementation Examples

Example 1: Set up a VPN service for all remote employees. Choose a reliable VPN provider and ensure that all remote employees have VPN access clients installed on their devices.

Example 2: Require VPN usage for accessing sensitive systems. Make it mandatory to use the VPN when accessing critical business systems like payroll, fleet management, or customer data.

Example 3: Train staff on VPN use and benefits. Educate employees on how to connect to the VPN and explain its importance in protecting company data during remote work.

Example 4: Monitor and enforce VPN usage. Regularly check remote access logs to ensure that employees are using the VPN and to identify any unusual login attempts.

Mappings to External Control Standards

- NIST PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.
- CIS 18 v8.1 Safeguard 3.12: Segment Data Processing and Storage Based on Sensitivity.

OOSF.03.6 – Documented Hardware and Software Inventory Management

Maintaining a documented hardware and software inventory is vital for managing and securing your business's technology assets. By keeping a detailed record of all devices, applications, and systems in use, you gain better visibility over your network, making it easier to identify outdated or unauthorized items. A well-organized inventory helps track software licenses, monitor hardware for updates, and quickly identify devices that may need security patches. This practice also supports efficient troubleshooting and compliance with industry standards, ensuring that your technology environment is secure, up-to-date, and aligned with cybersecurity best practices.

Implementation Examples

Example 1: Create a centralized inventory document. Use a spreadsheet or inventory management tool to track all hardware devices and software applications in use, noting details like serial numbers, model, and license information.

Example 2: Assign responsibility for inventory updates. Designate someone to regularly update the inventory list, adding new devices and removing retired or decommissioned items.[10]

Example 3: Perform routine inventory audits. Schedule periodic checks to verify that the inventory matches what's currently in use and to identify any unauthorized or unapproved devices or software.

Example 4: Monitor software license expirations. Track software license renewal dates in inventory to prevent lapses that could lead to compliance issues or security vulnerabilities.

Mappings to External Control Standards

- NIST ID.AM-01: Inventories of hardware managed by the organization are maintained.
- NIST ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained.
- CIS 18 v8.1 Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory.
- CIS 18 v8.2 Safeguard 2.1: Establish and Maintain a Software Inventory.

10 See also IO.03.2 – Designate Cybersecurity Roles and Responsibilities

OOSF.03.7 – Configure Email Security

Configuring Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting, and Conformance (DMARC) policies, along with a Secure Email Gateway (SEG), is essential for protecting your business from email-based threats like phishing and spoofing. SPF helps verify that email claiming to be from your domain are sent from authorized servers, while DMARC builds on this by allowing you to set policies on how to handle unauthenticated messages. A SEG further enhances protection by filtering incoming emails for malicious content. When used together, these tools help to prevent unauthorized email use, protect against spam and phishing, and safeguard sensitive communication.

Implementation Examples

Example 1: Set up SPF Records. Configure SPF by adding a Domain Name Service (DNS) record that specifies which mail servers are authorized to send emails on behalf of the domain.

Example 2: Implement DMARC policies. Configure DMARC policies in the DNS settings to dictate how to handle messages that fail SPF and DomainKeys Identified Mail (DKIM) checks, such as marking them as spam or rejecting them completely.

Example 3: Use a SEG. Deploy an SEG to filter out phishing attempts, malware, and spam before emails reach anyone's inbox, ensuring an added layer of email protection.

Example 4: Monitor DMARC reports regularly. Enable DMARC reporting to receive feedback on email authentication results, helping identify unauthorized email activity and adjust policies as needed.

Mappings to External Control Standards

- NIST DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events.
- CIS 18 v8.1 Safeguard 10.1: Deploy and Maintain Anti-Malware Software.

OOSF.03.8 – Encrypt all Devices

Encrypting all devices is a critical security measure that ensures data remains protected even if a device is lost or stolen. Encryption converts data into unreadable code that can only be unlocked with a decryption key, preventing unauthorized access to sensitive information. Encrypting devices, such as laptops, mobile phones, tablets, and storage devices help to secure customer information, financial data, and other sensitive records.

Implementation Examples

Example 1: Enable full disk encryption. Activate full disk encryption on all company laptops, desktops, and tablets (e.g., BitLocker for Windows, FileVault for macOS) to protect data stored on the device.

Example 2: Use mobile device encryption. For mobile phones and tablets, enable device encryption through the settings menu to secure data, especially for devices used for business communication.

Example 3: Encrypt removeable storage media. Encrypt all external drives, USBs, and other portable storage devices used for business purposes to protect data when transferring files or backing up information.

Example 4: Require strong passwords for encrypted devices. Ensure that all encrypted devices are protected with strong, unique passwords or PINs to prevent unauthorized access to the encrypted data.[11]

Mappings to External Control Standards

- NIST PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected.
- CIS 18 v8.1 Safeguard 3.9: Encrypt Data on Removeable Media.
- CIS 18 v8.1 Safeguard 3.11: Encrypt Sensitive Data at Rest.

11 See also IO.01.3 – Use Strong, Unique Passwords

OOSF.03.9 – Enable Detailed Security Logging

Enabling detailed security logging is essential for tracking and understanding activity across your network, systems, and devices. Security logs provide valuable insights into who accessed systems, what actions were taken, and any unusual behavior that may indicate a potential security threat. Detailed logging helps you detect and investigate incidents quickly, supports regulatory compliance, and provides critical evidence in the event of a security breach. By maintaining comprehensive logs, you strengthen your business's ability to monitor security and respond effectively to any suspicious activity.

Implementation Examples

Example 1: Enable logging on all key systems. Ensure that logging is activated for all essential systems, such as servers, network devices, and applications to capture critical security events.

Example 2: Configure centralized log storage. Use a centralized logging solution to collect and store logs in one location, making it easier to review and analyze events across multiple systems.

Example 3: Set up alerts for unusual activity. Configure alerts for specific security events, such as failed login attempts or unusual network activity.

Example 4: Retain and regularly review logs. Schedule routine log reviews to identify patterns or anomalies and retain logs for a designated period to comply with legal or regulatory requirements.

Mappings to External Control Standards

- NIST PR.PS-04: Log records are generated and made available for continuous monitoring.
- CIS 18 v8.1 Safeguard 8.2: Collect Audit Logs.

OOSF.03.10 – Software Version Control and End of Life Management

Managing software version control and end of life (EOL) is vital for maintaining a secure and functional technology environment. Version control ensures that software is kept up to date, providing access to the latest features, improvements, and security patches. EOL management consists of tracking software that is no longer supported by the vendor which means that the software no longer receives updates or security patched, leaving systems vulnerable to attack.

Implementation Examples

Example 1: Establish a software inventory. Keep a detailed list of all software, including version numbers, and EOL dates. This allows tracking of which applications need to be updated or replaced.[12]

Example 2: Automate updates where possible. Use tools to automatically apply updates or notify when new versions are available. Ensure that critical patches are applied as soon as they are available.[13]

Example 3: Monitor EOL dates for all software. Regularly review EOL dates in inventory and plan to replace or upgrade software well before support ends.

Example 4: Develop a replacement plan for EOL software. Identify alternative solutions for software nearing EOL to avoid disruption and maintain security when older versions are phased out.

Mappings to External Control Standards

- NIST PR.PS-04: Log records are generated and made available for continuous monitoring.
- CIS 18 v8.1 - Safeguard 2.2: Ensure Authorized Software is Currently Supported.

12 See also IO.03.6 - Documented Hardware and Software Inventory Management
13 See also IO.01.1 - Keep Software and OS Updated

Advanced: Owner Operator Controls - Tier Four

Advanced cybersecurity controls require additional investment both in time and resources. However, they will pay dividends when it comes to the security and resiliency of the operation. One of the best ways to avoid being a victim of cybercrime is to be the least appealing target.[14]

OOSF.04.1 – Security Incident and Event Management Solution

A Security Incident and Event Management (SIEM) solution is a powerful tool that can help your business monitor, detect, and respond to security threats in real time. SIEM systems collect and analyze security data from across your IT infrastructure, including network devices, servers, and applications. By aggregating logs and correlating events, SIEM solutions can identify suspicious activities and provide alerts. This enables quicker responses to potential incidents. SIEMs also offer centralized visibility and reporting, which can help a business meet regulatory compliance requirements and improve their overall security posture.

Implementation Examples

Example 1: Choose a scalable SIEM tool. Select a SIEM that can grow with the business, ensuring that it can handle increasing data volume and complexity as needs expand.

Example 2: Integrate all critical data sources. Connect key systems, like firewalls, endpoints, and cloud services to the SIEM to ensure a comprehensive view of the security landscape of the entire business.

Example 3: Customize alert settings. Set up specific alerts for high-risk activities relevant to the business to reduce noise and false positives. This will allow the security team to focus on critical security incidents.

Example 4: Establish regular log reviews. Develop a process for routinely analyzing SIEM logs and reports, allowing for early detection of anomalies and a proactive approach to security management.

Mappings to External Control Standards

- NIST DE.AE-02: Potentially adverse events are analyzed to better understand associated activities.
- CIS 18 v8.1 Safeguard 8.9: Centralize Audit Logs.

14 This level of cybersecurity maturity maps to NIST maturity level: Adaptive

OOSF.04.2 – Secure Baseline Configurations or Device Images

Establishing secure baselines for devices is an essential practice to ensure that all devices meet minimum security standards. A secure baseline includes configurations and settings that will harden a device against common vulnerabilities, such as disabling unnecessary services, enforcing strong password policies, and applying security patches. By creating these baselines for each type of device—whether computer, mobile phone, or network hardware—and using standardized device images, businesses can maintain consistent security measures across their environment, reducing the risk of attacks and simplifying compliance with cybersecurity standards.

Implementation Examples

Example 1: Define baseline configurations and create device images. Develop standardized security configurations and create device images for each type of device, ensuring that secure settings are consistently applied when new devices are deployed.

Example 2: Use automated tools for baselines and images. Implement tools that automate the application of baseline configurations or device images to ensure that all devices have the exact same security settings across the business without relying on manual action.

Example 3: Regularly review and update baseline images. Schedule routine reviews to update baselines and recreate device images as new threats emerge or as compliance requirements change, keeping configurations current.

Example 4: Monitor for baseline deviations. Set up monitoring to detect when a device falls out of compliance with its baseline, allowing IT or cybersecurity personnel to quickly address the potential vulnerabilities and restore the device to its secure state.

Mappings to External Control Standards

- NIST PR.PS-01: Configuration management practices are established and applied.
- CIS 18 v8.1 Safeguard 4.1: Establish and Maintain a Secure Configuration Process.
- CIS 18 v8.1 Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure.

OOSF.04.3 – Network Intrusion Detection System

A network intrusion detection system (NIDS) is a critical security tool that monitors network traffic for suspicious activities or potential threats. By analyzing data packets moving though the network, a NIDS can identify patterns that may indicate unauthorized access, malware, or other security issues. When a threat is detected, the system generates alerts, allowing security teams to respond quickly to prevent further damage. NIDS solutions provide valuable visibility into network activity, helping businesses protect sensitive data, maintain compliance with security standards, and reduce the risk of a successful breach.

Implementation Examples

Example 1: Deploy NIDS at key network entry points. Position the NIDS at critical points within the network, such as near the firewall or in high traffic areas (network trunk links) to monitor all incoming and outgoing data effectively.

Example 2: Configure NIDS to detect specific threats. Tailor the NIDS settings to detect threats relevant to the environment, such as unauthorized logins, known indicators of compromise (IOCs) related to specific threats, malware activity, or abnormal bandwidth usage.

Example 3: Integrate NIDS with SIEM solutions. Connect the NIDS to a SIEM system to correlate alerts with other security events, providing a comprehensive view of potential incidents.[15]

Example 4: Regularly update NIDS signatures and rules. Keep the NIDS up to date with the latest threat signatures and detection rules to ensure that it can identify new attack patterns and signs of activity around new vulnerabilities.

Mappings to External Control Standards

- NIST DE.CM-01: Networks and network services are monitored to find potentially adverse events.
- CIS 18 v8.1 Safeguard 13.1: Centralize Security Event Alerting.
- CIS 18 v8.1 Safeguard 13.3: Deploy a Network Intrusion Detection Solution.

15 See also IO.04.1 – Security Incident and Event Management (SIEM) Solution

OOSF.04.4 – Formalized, Documented Cybersecurity Policies

Formalized, documented cybersecurity policies are essential for setting clear guidelines on how a business protects information, manages risks, and maintains regulatory compliance. These policies establish the foundation for acceptable behavior, defining standards for everything from password management and data handling to device usage and incident response. Well-defined policies help employees understand their responsibilities, support a unified approach to security, and demonstrate a commitment to cybersecurity. Documented policies also make it easier to manage and enforce security practices, minimizing the potential for vulnerabilities due to inconsistent or unclear expectations.

Implementation Examples

Example 1: Develop comprehensive policy documents. Create clear, accessible policies that cover key areas like data protection, access control, acceptable use, and incident response. Ensure that these policies are tailored to the specific needs of the business and/or small fleet.

Example 2: Store policies in a secure, accessible location and format. Keep cybersecurity policies in a secure, easily accessible location, such as a protected share drive or internal website so that all employees can reference them as needed but only authorized parties can modify the policy documents.

Example 3: Schedule regular policy reviews. Set up regular review intervals to update policies as new risks, technologies and compliance requirements arise, ensuring that policies remain current and relevant.

Example 4: Incorporate policies into employee training and employee manuals. Make cybersecurity policies a part of regular employee training to reinforce their importance and ensure that all employees understand that adhering to business standards for cybersecurity is their responsibility.

Mappings to External Control Standards

- NIST GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced.

OOSF.04.5 – Regular Assessments and Exercises

Conducting regular risk assessments, vulnerability assessments, penetration tests, and tabletop exercises is crucial for proactively identifying and mitigating cybersecurity risk within a business. **Risk assessments** evaluate potential threats, vulnerabilities, and impacts on key assets, providing insights into areas needing improved security. **Vulnerability assessments** involve scanning systems and networks for known vulnerabilities, allowing for proactive patching and updates to reduce the risk of exploitation. **Penetration tests** simulate real-world attacks to identify weak points in defenses, offering a practical view of where systems may be vulnerable. The Cybersecurity & Infrastructure Security Agency (CISA) offers free network testing for critical infrastructure organizations[16] point for trucking operations seeking to harden their public-facing digital assets. **Tabletop exercises,** which involve running through hypothetical incident scenarios, enable teams to practice their response strategies, enhancing readiness for actual incidents. Together, these practices improve your organization's ability to detect, respond to, and recover from cyberthreats and attacks.

Implementation Examples

Example 1: Schedule regular risk and vulnerability assessments. Conduct assessments periodically to evaluate evolving threats and scan for known vulnerabilities, prioritizing areas needing immediate attention and timely patching.

Example 2: Engage qualified professionals for penetration tests. Hire cybersecurity experts or third-party services to perform penetration tests, ensuring an objective review of potential security gaps in systems and applications. Ensure that penetration tests are conducted within a clearly defined scope and with documented, mutually agreed upon rules of engagement.

Example 3: Conduct tabletop exercises with key stakeholders. Organize tabletop exercises with staff involved in incident response to simulate different cyberattack scenarios, helping everyone understand roles and improve response coordination. Ensure that any third-party cybersecurity or IT service providers are included in tabletop exercises and are aware of the business's service level agreement (SLA) expectations.

Example 4: Document findings and actions plans. After each assessment, test, or exercise, document the results, identify areas for improvement, and create prioritized action plans to address any identified vulnerabilities or gaps in the business's cybersecurity defenses.[17]

Mappings to External Control Standards

- NIST ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded.
- NIST ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties.
- CIS 18 v8.1 Safeguard 7.1: Establish and Maintain a Vulnerability Management Process.
- CIS 18 v8.1 Safeguard 7.2: Establish and Maintain a Remediation Process.

16 https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools
17 See also IO.04.08 Prioritized Risk Register

OOSF.04.6 – Zero-Trust Architecture

Zero-Trust architecture (ZTA) is a security model that operates under the principle of "never trust, always verify," assuming that threats could come from both outside and from within the business's network. Rather than relying on perimeter defenses alone, ZTA enforces strict identity verification, access control, and continuous monitoring for every user and device attempting to access resources, regardless of their location. By segmenting access and verifying each request, ZTA minimizes the risk of unauthorized access and lateral movement inside a network.

Implementation Examples

Example 1: Enforce strong identity verification. Implement multi-factor authentication (MFA) and identity verification processes for every user and devise to ensure that only verified individuals can access network resources.

Example 2: Apply least privilege access. Limit access permissions based on job role or function, granting users only the minimum access they need to perform their tasks.

Example 3: Continuously monitor and assess activity. Use tools like SIEM and Network Detection and Response (NDR) to monitor network activity, looking for any anomalies that could signal a security threat.

Example 4: Segment the network with microsegmentation. Break down the network into smaller zones or segments, controlling access to each part separately so that if one area is compromised, threats cannot move as easily into other areas of the network.

Mappings to External Control Standards

- NIST PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties.
- CIS 18 v8.1 Safeguard 5.1: Establish and Maintain an Inventory of Accounts.

OOSF.04.7 – Mobile Device Management Solution

A mobile device management (MDM) solution is an important tool for securing and managing mobile devices used within a business, particularly when employees use smartphones, tablets, or laptops to access company data remotely. MDM solutions enable IT administrators to monitor, manage, and secure mobile devices from a central console, enforcing security policies such as device encryption, app controls, and remote wipe capabilities. By implementing an MDM solution, businesses can reduce the risk of data leaks, protect sensitive information on mobile devices, and maintain compliance with cybersecurity standards even when employees work from outside the office.

Implementation Examples

Example 1: Establish device enrollment and inventory tracking. Use MDM to register all devices accessing an owner operator or small fleets' data and keep an updated inventory of devices and their configurations.

Example 2: Enforce security policies on all devices. Set and apply policies for password requirements, device encryption, and screen lock settings to ensure that mobile devices meet the business's security standards.

Example 3: Enable remote wiping capabilities. Configure MDM to allow remote wiping of devices in case they are lost or stolen, further protecting sensitive information from unauthorized access.

Example 4: Restrict and manage app usage. Use MDM to limit which applications can be installed or accessed on devices, helping control data exposure and prevent the use of risky or unauthorized apps.

Mappings to External Control Standards

- NIST ID.AM-01: Inventories of hardware managed by the organization are maintained.
- CIS 18 v8.1 Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory.

OOSF.04.8 – Prioritized Risk Register

A prioritized risk register is a structured document that helps businesses identify, assess, and rank cybersecurity risks based on their potential impact and likelihood of occurrence. By listing risks in order of priority, businesses can focus on addressing the most critical threats first, ensuring that resources are directed to areas that pose the greatest danger to operations and data security. A well-maintained risk register is essential for informed decision-making, enabling proactive risk management and supporting compliance with cybersecurity standards. This approach improves resilience by ensuring that the owner operator or small fleet is prepared to mitigate high-priority risks before they materialize.

Implementation Examples

Example 1: Identify and categorize risks. Document potential cybersecurity risks, categorizing them based on the type of threat (e.g., phishing, ransomware, insider threats) to gain a comprehensive view.

Example 2: Assess impact and likelihood. Rate each risk according to its potential impact on the business and the likelihood of it occurring, helping to prioritize high-risk threats.

Example 3: Assign mitigation strategies. Develop specific actions or controls to address each risk, focusing first on the most critical risks that need immediate attention.

Example 4: Regularly review and update the register. Schedule periodic reviews of the risk register to adjust priorities, add new risks, and update mitigation plans as the cybersecurity landscape changes.

Mappings to External Control Standards

- NIST ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.
- CIS 18 v8.1 Safeguard 7.2: Establish and Maintain a Remediation Process.

OOSF.04.9 – Documented Change Control Process

A documented change control process is essential for managing modifications to IT systems and network infrastructure in a controlled and secure manner. This process involves formally evaluating, approving, and recording changes to ensure they are necessary, tested, and implemented with minimal disruption to operations. By documenting each step—from request to implementation and review—businesses can reduce the risk of introducing new vulnerabilities, improve system stability, and maintain compliance with cybersecurity standards. A well-structured change control process promotes consistency, accountability, and transparency in how changes are managed.

Implementation Examples

Example 1: Establish a change request system. Set up a formal system for submitting change requests that includes details such as the reason for the change, potential impact, and affected systems.

Example 2: Create a change approval process. Develop a procedure to review and approve changes, involving key stakeholders and designated security personnel or security service provider staff to assess risks and ensure alignment with security policies.

Example 3: Test changes before implementation in live environments. Require testing in a controlled environment to identify potential issues and minimize disruption before deploying changes in a live environment.

Example 4: Document and review all changes. Record details of each change, including outcomes and lessons learned, and conduct periodic reviews to refine the change control process and address any recurring issues.

Mappings to External Control Standards

- NIST ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked.

OOSF.04.10 – Network Intrusion Prevention System

Network intrusion prevention systems (NIPS) are security tools designed to monitor network traffic for suspicious or malicious activity and actively block or mitigate potential threats in real time. Unlike intrusion detection systems (IDS) which only alert on detected threats, NIPS can automatically take action, such as drooping malicious packets or isolating affected devices to prevent attacks from compromising the network. This proactive defense helps businesses protect sensitive data, minimize disruption and reduce the risk of unauthorized access or malware spreading across the network.

Implementation Examples

Example 1: Deploy NIPS at key network points. Position NIPS at strategic locations, such as entry points to critical networks or near sensitive data storage to effectively monitor and protect essential assets.

Example 2: Configure NIPS with specific detection rules. Customize NIPS rules to detect and respond to common threats specific to the environment.

Example 3: Regularly update NIPS signatures and rules. Keep the system's detection signatures up to date to protect against new threats, ensuring that it can recognize the latest attack methods.

Example 4: Integrate NIPS with security monitoring tools. Connect NIPS to a SIEM system to correlate intrusion data with other security events, gaining deeper insight into potential threats and network activity.

Mappings to External Control Standards

- NIST DE.CM-01: Networks and network services are monitored to find potentially adverse events.
- CIS 18 v8.1 Safeguard 13.8: Deploy a Network Intrusion Prevention Solution.

Additional Resources

The guidance found in this document is drawn from several cybersecurity standards, frameworks and best practice publications. Further reading on the controls outlined herein may be found in the resources listed below.

Center for Internet Security. (2021). CIS Controls v8.1 Retrieved from https://www.cisecurity.org/controls/cis-controls-list

Cybersecurity and Infrastructure Security Agency. (2020). Domain-Based Message Authentication, Reporting and Conformance (DMARC). Retrieved from https://www.cisa.gov/resources-tools/resources/domain-based-message-authentication-reporting-and-conformance-dmarc

Cybersecurity and Infrastructure Security Agency. (2020). Workforce Framework for Cybersecurity (NICE Framework). Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

Cybersecurity and Infrastructure Security Agency. (2020). Incident Response Plan (IRP) Basics. Retrieved from https://www.cisa.gov/resources-tools/resources/incident-response-plan-irp-basics

Cybersecurity and Infrastructure Security Agency. (2021). Multi-Factor Authentication (MFA). Retrieved from https://www.cisa.gov/resources-tools/resources/multi-factor-authentication-mfa

Cybersecurity and Infrastructure Security Agency. (2021). Enterprise VPN Security. Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-073a

Protect your personal information and data. (2024, July 29). Consumer Advice. https://consumer.ftc.gov/articles/protect-your-personal-information-and-data

Federal Trade Commission. (2016). Protecting Personal Information: A Guide for Business. Retrieved from https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business

National Cybersecurity Center of Excellence. (2019). Data Integrity: Recovering from Ransomware and Other Destructive Events. Retrieved from https://www.nccoe.nist.gov/data-integrity-recovering-ransomware-and-other-destructive-events

National Institute of Standards and Technology. (2012). Computer Security Incident Handling Guide (SP 800-61 Rev. 2). Retrieved from https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Institute of Standards and Technology. (2016). Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security (SP 800-46 Rev. 2). Retrieved from https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final

National Institute of Standards and Technology. (2024). Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (SP 800-171 Rev. 3). Retrieved from https://csrc.nist.gov/pubs/sp/800/171/r3/final

National Institute of Standards and Technology. (2016). Security Considerations for Network Segmentation (SP 800-125B). Retrieved from https://csrc.nist.gov/publications/detail/sp/800-125b/final

National Institute of Standards and Technology. (2017). Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B). Retrieved from https://pages.nist.gov/800-63-3/sp800-63b.html

National Institute of Standards and Technology. (2018). Risk Management Framework for Information Systems and Organizations (SP 800-37 Rev. 2). Retrieved from https://csrc.nist.gov/publications/detail/

sp/800-37/rev-2/final
National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5). Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
Federal Trade Commission. (2018). Cybersecurity for Small Business. Retrieved from https://www.ftc.gov/business-guidance/small-businesses/cybersecurity
National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce. http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Acronyms

BCP – Business Continuity Plan

CIS – Center for Internet Security

CSF – Cybersecurity Framework

DMARC – Domain based Message Authentication, Reporting, and Conformance

DKIM – Domain Keys Identified Mail

DRP – Disaster Recovery Plan

EDR – Endpoint Detection and Response

EOL – End of Life

IOC – Indicator of Compromise

IRP – Incident Response Plan

IT – Information Technology

MDM – Mobile Device Management

MFA – Multi-Factor Authentication

MSP – Managed Services Provider

MSSP – Managed Security Services Provider

NIDS – Network Intrusion Detection System

NIPS – Network Intrusion Prevention System

NIST – National Institute of Standards and Technology

NMFTA – National Motor Freight Traffic Association

OS – Operating System

PII – Personally Identifiable Information

PKI – Public Key Infrastructure

SaaS – Software as a Service

SEG – Secure Email Gateway

SIEM – Security Incident and Event Management

SMB – Small to Medium Business

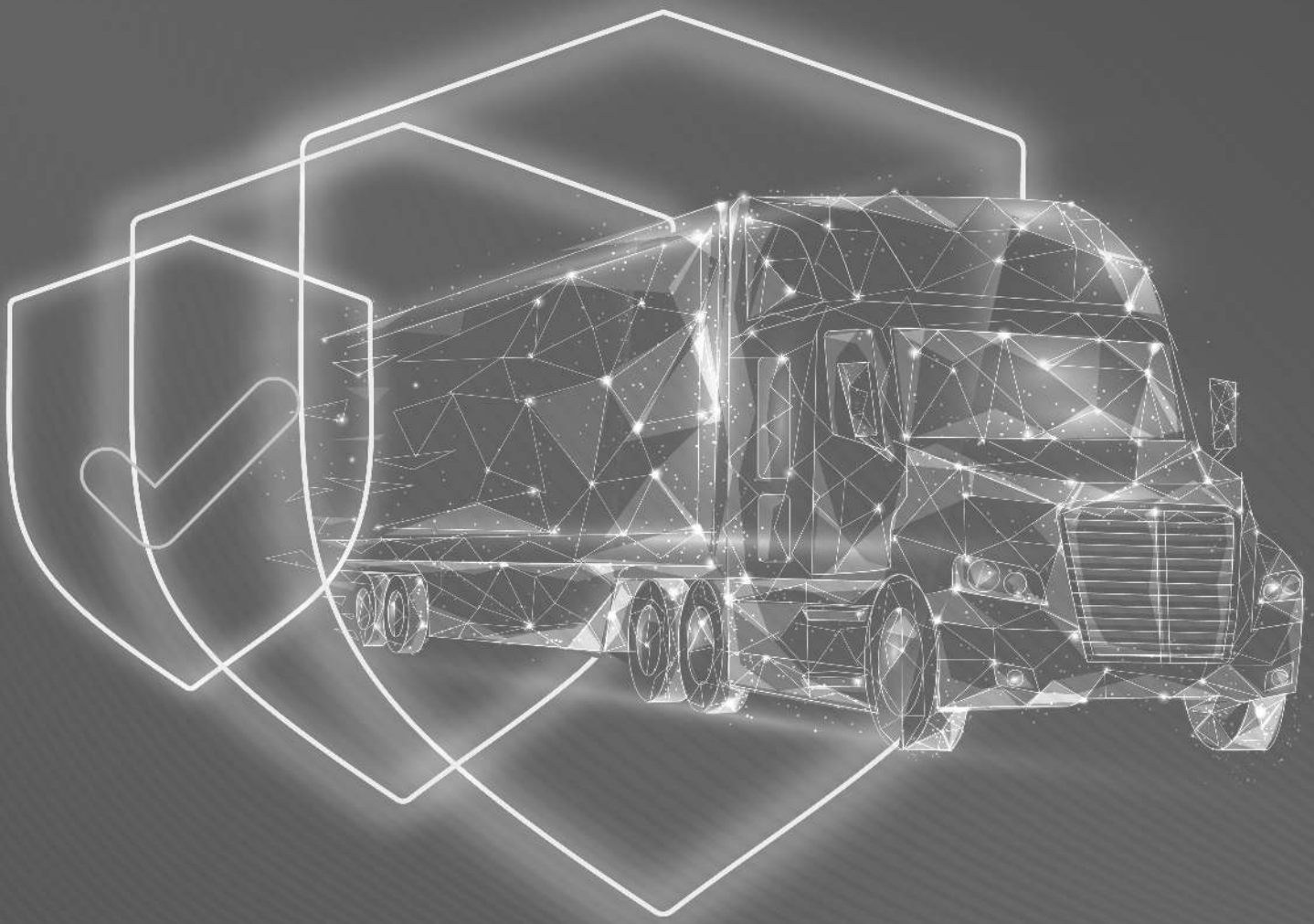
SPF – Sender Policy Framework

SSL – Secure Sockets Layer

TLS – Transport Layer Security

VPN – Virtual Private Network

ZTA – Zero-Trust Architecture



NMFTA™
National Motor Freight Traffic Association, Inc.

CYBER