Cybersecurity Framework – Payroll Profile

Overview

The NIST Cybersecurity Framework (CSF) is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. This document comprises a "profile", a subset of recommendations specific to an industry, to provide the Payroll community with a simple cybersecurity assessment tool. Use this profile as a set of leading practices to improve cybersecurity, protect against fraud, and enhance privacy in your Payroll organization.

You can also assess how you're doing using the checklist feature:

- **In Place** – we have implemented this measure or another measure that yields a similar outcome.
- **In Progress** – we are working on implementing this or another measure that yields a similar outcome.
- **Under Consideration** – we have discussed the value of this measure but haven't implemented it.
- **N/A** – this measure does not apply to our business model.

Payroll Profile

Access Control

Risk areas addressed: Malware, Fraud, Unauthorized Access, Ransomware

Access control is important to understand who is making changes on your network – and to prevent unauthorized users from doing things they shouldn't. Develop strong access control protection with these controls:

Control Information	Status			
	In Place	In Progress	Under Consideration	N/A
Define what permissions each user type or role should have within your systems. For more information: AC-2	☐	☐	☐	☐
Use the principle of least privilege so users only have access to information and system actions that they really need in order to do their job. For more information: AC-2, AC-4, AC-6, SA-8 (14)	☐	☐	☐	☐
Limit the number of privileged users like System Administrators. For more information: AC-3	☐	☐	☐	☐
Regularly review users' roles and privileges to make sure they have the correct access levels and aren't over-privileged. For more information: AC-3	☐	☐	☐	☐

Control Information	Status			
	In Place	In Progress	Under Consideration	N/A
Prohibit access to sensitive data or systems except under certain necessary circumstances. For more information: AC-3 (05)	☐	☐	☐	☐
Classify your data correctly so that it can be handled appropriately; for example, tag all documents with PII as Private. For more information: AC-16	☐	☐	☐	☐
Remove or suspend accounts that may have been hit by a ransomware attack or have been otherwise compromised; this also includes routine removal of accounts for employees/contractors that are no longer with the company. For more information: SI-12	☐	☐	☐	☐

Awareness Training

Risk areas addressed: Malicious Code, Rootkits, Mobile Security, Phishing

Awareness Training is important for incident prevention. Many of the most common cybersecurity risks can be best addressed through prevention measures and awareness training is the first step to that. Ensure strong awareness training through these controls:

Control Information	Status			
	In Place	In Progress	Under Consideration	N/A
Have an awareness and training policy that talks about training frequency, topics, and who gets trained (for example, external contractors). For more information: AT-1	☐	☐	☐	☐
Provide security and privacy training to users according to your policy. For more information: AT-2	☐	☐	☐	☐
Perform anti-phishing and anti-malware awareness training, including a segment specific to mobile devices, in your training. For more information: AT-2	☐	☐	☐	☐
Provide practical exercises in training. For more information: AT-2(1), (3)	☐	☐	☐	☐
Make sure third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities. For more information: AT-3	☐	☐	☐	☐

Audit and Accountability

Risk areas addressed: Cloud Security, Brute Force, Data Manipulation, Phishing, Malicious Code

Audit and Accountability is important to ensure there you have insight into what's happening in your business and on your network, and so that key records are available in the event that they are needed. To achieve strong audit and accountability capabilities, leverage these controls:

Control Information	Status			
	In Place	In Progress	Under Consideration	N/A
Conduct a risk assessment to identify threats and vulnerabilities in your system. Gauge the likelihood and magnitude of harm and talk through potential adverse effects on individuals and the business. For more information: RA-3	☐	☐	☐	☐
Based on your risk assessment, define the types of events that will be monitored (watched) and/or logged (recorded), coordinate the logging with other groups in the organization, and periodically revisit the discussion as your needs may change. For more information: AU-02	☐	☐	☐	☐
Continuously review and analyze the audit information and create an appropriate reporting system. For more information: AU-06	☐	☐	☐	☐
Determine who should have access to audit information; protect your audit logs from unauthorized access. For more information: AU-09	☐	☐	☐	☐
Provide the means for authorized individuals to determine the identity of the producer of information. For more information: AU-10	☐	☐	☐	☐
Create unique user accounts for each user. Don't share accounts! This helps you match a specific user to their actions if an incident occurs. Risk Area Addressed: Tax Data Regulations	☐	☐	☐	☐

Assessment, Authorization, and Monitoring

Risk areas addressed: Cloud Security, Phishing, Malicious Code

Assessment, Authorization, and Monitoring builds on the previous family by giving you further transparency into what's happening – not just on your network, but across the whole business. These controls help limit unauthorized activity and detect suspicious behavior.

Control Information	Status			
	In Place	In Progress	Under Consideration	N/A
Manage the exchange of information between systems, verifying individuals and systems have authorization before accepting data. For more information: CA-3, CA-3(6)	☐	☐	☐	☐
Develop and implement a system-wide continuous monitoring strategy. For more information: CA-7	☐	☐	☐	☐
Authorize internal connections within your system. Document each connection and continuously review these connections. For more information: CA-9	☐	☐	☐	☐
Monitor your network for potential cybersecurity events, like malicious code and unauthorized mobile code. For more information: CM-01, CM-04, CM-05	☐	☐	☐	☐
Configure firewalls or a system-wide intrusion detection system to detect and prevent attempted attacks. For more information: SI-04 (1), DP-2	☐	☐	☐	☐
Continuously monitor your systems for indicators of potential attacks like unauthorized connections or use. Analyze these data and adjust accordingly to make sure you capture what you need. It may also help to obtain legal guidance regarding monitoring activities. For more information: SI-4	☐	☐	☐	☐
Receive security alerts from external sources and have a method of sending out those alerts to all relevant stakeholders. For more information: SI-05	☐	☐	☐	☐
Require that providers of your external system services comply with your organizational security and privacy requirements. Routinely assess partners to check they are meeting their contractual obligations through audits, testing, and reports as agreed to by both parties. For more information: SA-9, SC-04, PL-4 (1)	☐	☐	☐	☐

Configuration Management

Risk areas addressed: Ransomware, Malicious Code, Eavesdropping, FTC Safeguards, Wi-Fi-Working from Home

Configuration Management is important for establishing and maintaining a product's baseline performance and attributes. What should things look like under normal, optimal conditions? Having a good baseline makes it easier to detect when something is out of place or operating incorrectly. For consistent configuration management, consider these controls:

Control Information	Status			
	In Place	In Progress	Under Consideration	N/A
Create a baseline of network operations and expected data flows for users and systems to assist in detecting incidents. For more information: RP-1	☐	☐	☐	☐
Restrict the use of system functions like ports, protocols, software, and services. You can also configure desktop extensions to disable .exe and java files. For more information: CM-07	☐	☐	☐	☐
Put in place employee confidentiality and security standards agreements. For more information: CM-07(2)	☐	☐	☐	☐
Utilize anti-virus and anti-malware software across your systems; consider requiring employee-owned computers and mobile devices to demonstrate proof of anti-virus protection as well. For more information: SI-01	☐	☐	☐	☐
Set up computers to install automatic patch updates or require employees using their own computers and mobile devices to regularly check for and install security patches. For more information: CM-10, SI-02 (5)	☐	☐	☐	☐
Make sure computers are loaded with approved software and used in accordance with contract agreements. For more information: CM-10	☐	☐	☐	☐
Create a policy around software installation by users, and monitor compliance with the policy. Track the use of the software by your employees, especially peer-to-peer file sharing software. For more information: CM-11	☐	☐	☐	☐
Enforce information policies against sending sensitive data through email. Risk Area Addressed: W-2 Theft	☐	☐	☐	☐

Identification and Authentication

Risk areas addressed: Unauthorized access, Wi-Fi- Working from Home, W-2 Theft, Brute Force, Eavesdropping, Business Email Compromise, Cloud Security, Fraud

Identification and Authentication is important to reduce fraud and manage risks around user access into company information assets. This can include both organizational and non-organizational users both of which require strictly defined access controls. Utilize these controls:

Control Information	Status			
	In Place	In Progress	Under Consideration	N/A
Develop policy around identification, such as checking a driver's license before adding a new user, and authentication, such as requiring a user to log in. Designate someone to review the policy and keep it up to date. For more information: IA-01	☐	☐	☐	☐
Perform some level of identity proofing, to include background checks, on all employees or anyone who will be interacting with sensitive applications or data. For more information: SA-9 (14)	☐	☐	☐	☐
Create access agreements for your systems that are continuously reviewed and updated. Verify individuals requiring access to systems and have these agreements signed prior to granting access. For more information: PS-06	☐	☐	☐	☐
Require Multi-Factor Authentication (MFA) for access to email, sensitive applications and data, or Single Sign-on accounts. For more information: IA-02 (1) (2)	☐	☐	☐	☐
Flag external emails with a warning message for the recipient in your organization. For more information: IA-04 (4)	☐	☐	☐	☐
Require users to change any default passwords before first use. For more information: IA-05	☐	☐	☐	☐
Authenticate any services like external computers or applications before establishing communications with devices, users, or internal applications. For more information: IA-03, IA-09	☐	☐	☐	☐
Define the circumstances and situations where re-authentication is required (for example, a user must log in again every 12 hours). For more information: IA-11	☐	☐	☐	☐
Conduct stricter identity proofing for users who will have access to sensitive systems and applications, such as network administrators. For more information: IA-12	☐	☐	☐	☐
Utilizing cameras in the workplace can help identify unauthorized access and deter employees from fraud such as workers' compensation schemes. For more information: PE-6	☐	☐	☐	☐

Incident Response

Risk areas addressed: Tax Data Regulations, Data Breach, Denial of Service, Workers Comp Schemes, Malicious Code

Incident Response is important for quickly and efficiently recovering from an event. Being prepared means you can quickly react to an incident, which is imperative to reducing the long-lasting effects of the event. Utilize these controls for strong incident response capabilities:

Control Information	Status			
	In Place	In Progress	Under Consideration	N/A
Develop an Incident Response Plan to have ready in the event of a breach or other attack. Use checklists and process flows to map out step by step response actions, including who will do what and lists of contact information, such as law enforcement. (*Note – the IRS Security Summit has templates for an Incident Response Plan to help get you started.)* For more information: IR-1, RP-1, AE-1	☐	☐	☐	☐
Using your Incident Response Plan as a guide, train employees on how to identify and respond to a breach, including your organization's process for reporting a breach to appropriate authorities like the IRS stakeholder liaisons. For more information: IR-2 (3)	☐	☐	☐	☐
Ensure that your system is set up to handle all aspects of your incident response plan. For more information: IR-8	☐	☐	☐	☐
Since some employees may take advantage of workers comp and other fraud schemes, regularly conduct employee monitoring for any breaches or incidents, and respond quickly. For more information: IR-5	☐	☐	☐	☐

Program Management

Risk areas addressed: FTC Safeguards, Mobile Security, Data Theft, Business Email Compromise, Malicious Code, Phishing

Program Management is important to the overall security of your information systems. It is imperative to your security posture to clearly define and assign roles, manage security personnel and programs, and plan for the future. For strong program management, utilize these controls:

Control Information	Status			
	In Place	In Progress	Under Consideration	N/A
Designate an employee or a team to lead your security initiatives. For more information: PM-02	☐	☐	☐	☐

Control Information	Status			
	In Place	In Progress	Under Consideration	N/A
Create a written information security plan to protect both user-facing and back-end system components. Be sure to account for physical security, too – who is allowed access to your building, and safety features like the location of fire extinguishers. For more information: PT-1, SC-02	☐	☐	☐	☐
Inventory and track all computers and mobile devices that have been issued, as well as other hardware. For more information: PM-05	☐	☐	☐	☐
Implement an insider threat program that includes a cross-department handling team to prevent and respond to insider threats. For more information: PM-12	☐	☐	☐	☐
Establish a security and privacy workforce development and improvement program. For more information: PM-13	☐	☐	☐	☐
Create a policy for identifying, handling, protecting, and storing (and deleting!) sensitive or classified information, especially personally identifiable information (PII) or federal tax information (FTI) both on internal and external systems. Come up with policies for correcting or deleting inaccurate PII and how that is relayed to users. For more information: PM-17	☐	☐	☐	☐
Restrict the processing of PII and other sensitive information and who has authority to view, access, and modify it. For more information: PM-22, PT-2, PL-8	☐	☐	☐	☐
Perform a privacy impact assessment before adding any new technologies, systems, or processes dealing with personally identifiable information. For more information: RA-8	☐	☐	☐	☐

System Controls

Risk areas addressed: Data Theft, Cloud Security, Phishing, Malicious Code, FTC Safeguards, Eavesdropping, Denial of Service, Business Email Compromise, Tax Data Regulations, Ransomware, Mobile Security, Cross-Site Scripting, GLBA

System Controls are important to securing your overall systems against a variety of cyber threats through best practices like system checks, encryption, and load balancing. Strong systems controls include:

Control Information	Status			
	In Place	In Progress	Under Consideration	N/A
Isolate security functions from non-security functions and segment your networks to prevent lateral movement from an infiltrator. For more information: SC-03	☐	☐	☐	☐
Protect non-production environments by keeping links secret and requiring authentication; reduce the use of actual user data in non-production environments. For more information: SA-3 (2)	☐	☐	☐	☐
Perform load balancing on your networks. Not only will this make your network more efficient, but it can help deter unwanted traffic and provide denial of service. For more information: SC-05 (2)	☐	☐	☐	☐
Establish supply chain risk management processes like knowing the components of any commercial application and restricting external access to applications. For more information: SC-01	☐	☐	☐	☐
Generate error messages that provide steps for corrective actions yet not providing any revealing information that could be exploited. Reveal these error messages only to assigned roles in the organization. For more information: SI-11	☐	☐	☐	☐
For systems that accept data inputs, perform validity checks on inputs to keep malicious scripts or erroneous data from being entered. For more information: SI-10, SI-10 (6)	☐	☐	☐	☐
Put in measures to prevent the exfiltration of information and conduct infiltration tests to assess vulnerability. Use boundary protection mechanisms on designated system components. For more information: SC-07 (10), SC-07 (12), RA-5, SI-21	☐	☐	☐	☐
Back up user and system information and system documentation. Be sure to have data security for all your backups and a data retention policy. For more information: CP-09	☐	☐	☐	☐
Implement processes and tools to protect the confidentiality and integrity of transmitted information. For more information: SC-08	☐	☐	☐	☐
Block ads and popups online. Risk Area Addressed: Ransomware	☐	☐	☐	☐
Display file extensions for downloads and other apps, especially executable files. Risk Area Addressed: Ransomware	☐	☐	☐	☐
Use end-to-end email encryption and/or digital signatures to fight phishing. For more information: SA-8 (18)	☐	☐	☐	☐

Control Information	Status			
	In Place	In Progress	Under Consideration	N/A
Set up spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; update these when releases are made available. For more information: SI-08	☐	☐	☐	☐
Route internal communications traffic to authenticated proxy servers. For more information: SC-07 (8)	☐	☐	☐	☐
Use a DNS blacklist check to ensure mail server IP addresses. For more information: SC-20	☐	☐	☐	☐
Block outbound port 25 for all non-mail sending hosts to protect against phishing. For more information: SC-07 (3)	☐	☐	☐	☐

Additional Controls

Below are additional controls to consider when improving your cybersecurity posture. These controls address cybersecurity concerns that may be outside the NIST 800-83 controls, such as fraud mitigation and additional Payroll-specific needs. The controls below are listed with the corresponding Risk Area it can address. Some additional controls include:

Control Information	Status			
	In Place	In Progress	Under Consideration	N/A
Enable use of IP PINS for victims of identity theft. Risk Area Addressed: Synthetic Identities	☐	☐	☐	☐
Share information with others in the industry, such as lists of known synthetic identities, known deceased individuals/SSNs, etc. Risk Area Addressed: Synthetic Identities	☐	☐	☐	☐
Report Business Email Compromise scam attempts to the MS-ISAC, local law enforcement, and the Internet Crime Complaint Center (IC3). Risk Area Addressed: Business Email Compromise	☐	☐	☐	☐
Report tax-related suspicious emails to the IRS via your stakeholder liaison. Risk Area Addressed: Business Email Compromise	☐	☐	☐	☐
Verify new business entities before performing any business with them. You can perform an SSN or EIN/EFIN check, for example through the Social Security Administration's eCBSV tool, or use a phone call, physical letter, or review of documentation to confirm their legitimacy. Risk Area Addressed: Synthetic Identities	☐	☐	☐	☐
Flag SSNs that are less than ten years old or those of known deceased individuals. Risk Area Addressed: Synthetic Identities	☐	☐	☐	☐

Control Information	Status			
	In Place	In Progress	Under Consideration	N/A
Require commission program documentation to include thresholds or expected limits; flag and audit frequent commissions or figures above a risk threshold. Risk Area Addressed: Commission Schemes	☐	☐	☐	☐
Limit access to your own EIN to prevent falsified W-2s. Risk Area Addressed: Synthetic Businesses	☐	☐	☐	☐
Utilize biometric timecards for your employees. Risk Area Addressed: Falsified Wages/Timesheet Fraud	☐	☐	☐	☐
Regularly change the people who perform sensitive roles like timesheet approval. Risk Area Addressed: Falsified Wages/Timesheet Fraud	☐	☐	☐	☐
Create clear permissions and procedures for high-risk actions. Risk Area Addressed: Unauthorized Deposits	☐	☐	☐	☐
Flag anomalies such as large budget variations in payroll expenses, direct deposit changes, company name changes, etc. Require out of band approval (like a second person approving the change) for deviations from regular processes. Risk Area Addressed: Ghost Employees, Timesheet Fraud, Synthetic Businesses	☐	☐	☐	☐
Check employee database for duplicate SSNs; require unique direct deposit/bank accounts or SSN for all employees. Risk Area Addressed: Ghost Employees	☐	☐	☐	☐
Randomly inspect database for employees with P.O. boxes instead of a physical address or those claiming no deductions. Risk Area Addressed: Ghost Employees	☐	☐	☐	☐
Publicize training and legal information about how to properly classify and provide forms to different types of employees (e.g. 1099, W-2 etc.). Risk Area Addressed: Misclassified Employees	☐	☐	☐	☐
Ensure there is appropriate collaboration with immigration, unions, and other agencies when classifying your employees. Risk Area Addressed: Misclassified Employees	☐	☐	☐	☐
Require injuries and claims to be filed promptly to maximize the potential for corroborating evidence such as camera footage. Risk Area Addressed: Workers Comp Schemes	☐	☐	☐	☐
Where appropriate, ensure that consumers understand their right to access and/or opt out of their personal data collection. Risk Area Addressed: State-specific Controls	☐	☐	☐	☐
Ensure your employees understand the criminal and monetary penalties for unauthorized disclosure of taxpayer data. Risk Area Addressed: Tax Data Regulations	☐	☐	☐	☐

Control Information	Status			
	In Place	In Progress	Under Consideration	N/A
Consider cyber insurance as an option available to many businesses. Closely inspect their policies, such as whether they pay out in the event of a ransomware attack. Risk Area Addressed: Ransomware	☐	☐	☐	☐