Payroll System Case Study: Continuous Monitoring

Daniel Cordeiro Marques

University of San Diego

CSOL-530-01-SP21 - Cyber Security Risk Management

Dr. Michelle Moore

February 28, 2021

Payroll System Case Study: Continuous Monitoring

Dempsey et al. (2011) describe continuous monitoring as "maintaining ongoing awareness to support organizational risk decisions" (p. B-4). This last step of the NIST Risk Management Framework (RMF) ensures that the system operates at an acceptable risk level and that changes impacting the system's security posture are evaluated and addressed timely.

This paper offers an overview of the RMF as applied to the payroll system case study, summarizing and exemplifying each step's outputs. Finally, it provides a continuous monitoring strategy for the payroll system based on pre-existing policies, procedures, and software.

Risk Management Framework Overview

To ensure the system security alignment with the overall business strategy, organizations should connect risk management decisions, such as selected controls, to security requirements by following a structured approach such as the NIST RMF. The RMF proposes seven steps, and each step output feeds into the next, establishing "traceability of controls to the security and privacy requirements that the controls are intended to satisfy" (National Institute of Standards and Technology, 2018).

The following sections demonstrate the NIST RMF applied the payroll system.

Preparation

The first step in the risk management process is understanding the system's context within the organization. Knowledge collected from this phase is essential to manage risk successfully. It drives the system classification, how the organization will implement security controls, and supports the leadership in authorizing the system deployment. Activities during this step include identifying and assigning individuals to roles and responsibilities, establishing a risk management strategy for the system, assessing the system's risk in the organization context, identifying organization-wide control baselines and common controls, and the organization-wide continuous monitoring strategy.

Expected outputs include documented risk management strategy, roles and responsibilities, baseline and common controls, and documentation outlining the organization-wide continuous monitoring strategy.

System Categorization

After understanding the system's context and business implications, the organization categorizes it according to the impact of the loss of confidentiality, integrity, and availability of the handled information. The expected output is the system description and categorization results approved by senior leadership.

The payroll system was categorized considering three types of information: the employee's Personally Identifiable Information (PII), income details, and general information such as roles, location, and other compensation details. Using the categorization ratings proposed by Stine et al. (2008), the payroll system was identified as a high-impact system, as illustrated by

Table 1.

Table 1. Payroll system security categorization

Information Type	Confidentiality impact	Integrity impact	Availability impact
Personally Identifiable Information. The system must store and process the employees' Social Security Number (SSN), name, date of birth, bank account number, and home address to perform its functions.	**HIGH** Unauthorized disclosure of PII may lead to fines for infringing privacy laws. PII data can be used for fraud and to impersonate employees to gain additional access to information.	**HIGH** Modification to PII can help threats to impersonate employees and gain additional access to information. Change in banking details may redirect wages to a rogue account.	**MODERATE** If the banking information is not available, the organization may fail to pay wages timely, leading to employee satisfaction and potential legal issues.
Income Information. The payroll system handles the employees' wages, taxes paid, and deductions.	**HIGH** Unauthorized disclosure of income information could lead to fines for infringing privacy laws.	**HIGH** If the income information is not correct, the organization may fail to pay the right taxes leading to fines and penalties.	**MODERATE** If the income information is not available, the organization may fail to pay wages and taxes timely, leading to employee dissatisfaction and tax penalties.
General Information. The system stores other compensation details (including benefits), employees' roles and departments, and work location.	**LOW** Paid time off, employee absence, and related information is not typically available publicly, but these details are not sensitive.	**LOW** General information is mainly kept for internal records, and their modification does not result in substantial impact.	**LOW** If the general information is not available timely, employees might fail to access their benefits, leading to employee satisfaction issues.
System Categorization	**HIGH**	**HIGH**	**MODERATE**
	Overall system impact (based on the highest impact): **HIGH**		

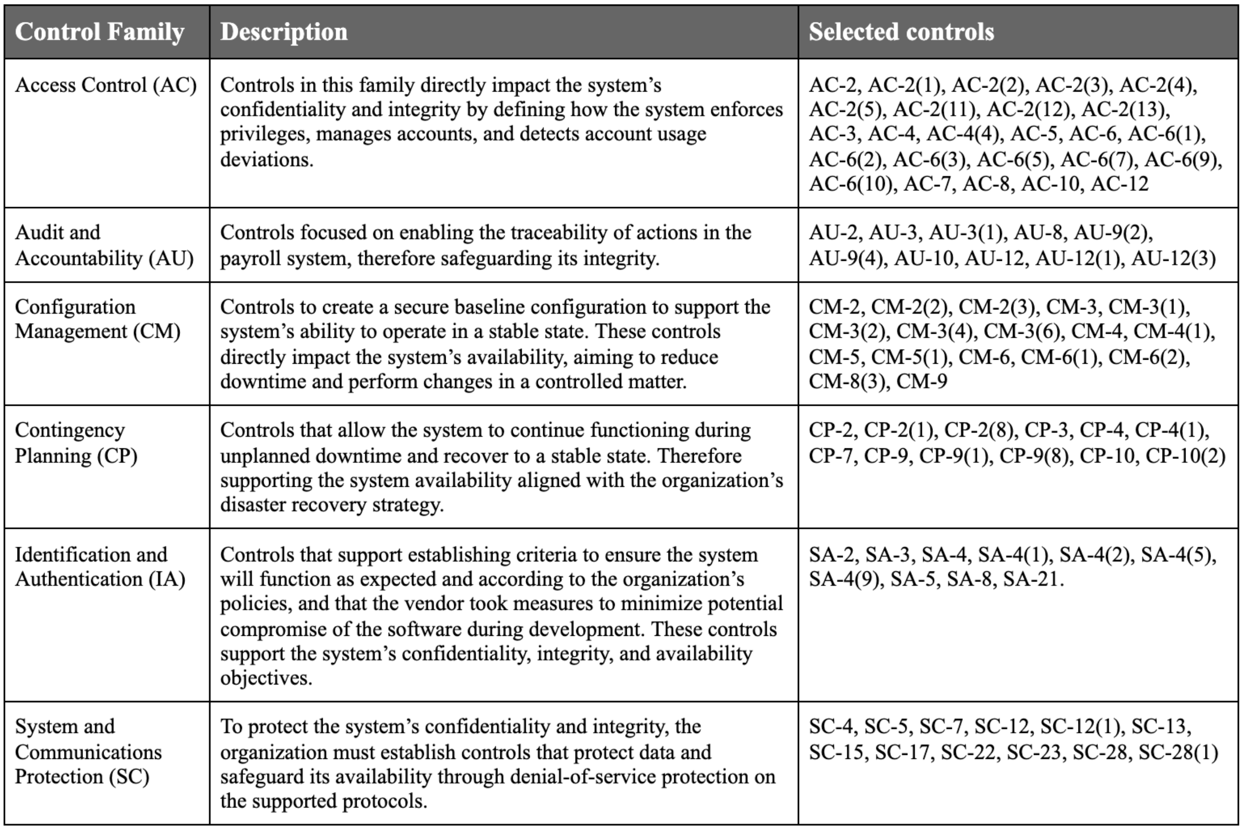
Security Control Selection

Based on the system security categorization, the organization selects and subsequently tailors baseline security controls to mitigate the risk to an acceptable level. The output expected from this step includes a revised and approved control baseline that the organization will implement to safeguard the system.

As proposed by the National Institute of Standards and Technology (2006, p. 4), the high baseline offered by NIST SP 800-53B (National Institute of Standards and Technology, 2020) serves as the foundation to define security controls for the payroll system. During the tailoring phase, controls not applicable to the system (such as wireless access controls) were removed, leaving only those supporting the system operations according to the business objectives. Figure 1 illustrates the resulting baseline.

Figure 1.

Selected and tailored security controls for the payroll system



Control Family	Description	Selected controls
Access Control (AC)	Controls in this family directly impact the system's confidentiality and integrity by defining how the system enforces privileges, manages accounts, and detects account usage deviations.	AC-2, AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-2(5), AC-2(11), AC-2(12), AC-2(13), AC-3, AC-4, AC-4(4), AC-5, AC-6, AC-6(1), AC-6(2), AC-6(3), AC-6(5), AC-6(7), AC-6(9), AC-6(10), AC-7, AC-8, AC-10, AC-12
Audit and Accountability (AU)	Controls focused on enabling the traceability of actions in the payroll system, therefore safeguarding its integrity.	AU-2, AU-3, AU-3(1), AU-8, AU-9(2), AU-9(4), AU-10, AU-12, AU-12(1), AU-12(3)
Configuration Management (CM)	Controls to create a secure baseline configuration to support the system's ability to operate in a stable state. These controls directly impact the system's availability, aiming to reduce downtime and perform changes in a controlled matter.	CM-2, CM-2(2), CM-2(3), CM-3, CM-3(1), CM-3(2), CM-3(4), CM-3(6), CM-4, CM-4(1), CM-5, CM-5(1), CM-6, CM-6(1), CM-6(2), CM-8(3), CM-9
Contingency Planning (CP)	Controls that allow the system to continue functioning during unplanned downtime and recover to a stable state. Therefore supporting the system availability aligned with the organization's disaster recovery strategy.	CP-2, CP-2(1), CP-2(8), CP-3, CP-4, CP-4(1), CP-7, CP-9, CP-9(1), CP-9(8), CP-10, CP-10(2)
Identification and Authentication (IA)	Controls that support establishing criteria to ensure the system will function as expected and according to the organization's policies, and that the vendor took measures to minimize potential compromise of the software during development. These controls support the system's confidentiality, integrity, and availability objectives.	SA-2, SA-3, SA-4, SA-4(1), SA-4(2), SA-4(5), SA-4(9), SA-5, SA-8, SA-21.
System and Communications Protection (SC)	To protect the system's confidentiality and integrity, the organization must establish controls that protect data and safeguard its availability through denial-of-service protection on the supported protocols.	SC-4, SC-5, SC-7, SC-12, SC-12(1), SC-13, SC-15, SC-17, SC-22, SC-23, SC-28, SC-28(1)

Security Control Implementation

Next, the organization implements the baseline and updates it based on information obtained during this phase. For instance, the system might not offer the functionality required to implement one of the selected controls, raising the need for a mitigating strategy. The organization can modify the system's security plan to address the issue or apply additional countermeasures as a workaround.

With the payroll system, the strategy was to reuse the existing infrastructure and security services to implement the selected controls. For example, the organization leveraged its Active Directory (AD) for authentication, the centralized log server to store audit logs, and the existing policies and procedures for backup, contingency planning, and backup.

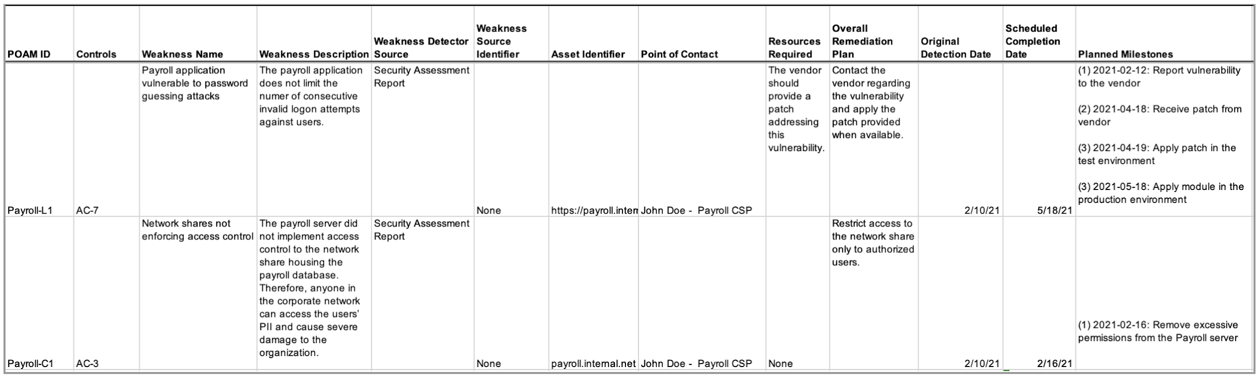
Security Control Assessment

The organization must verify that the controls were implemented correctly, operate as intended, and produce the desired outcome. To perform the activity, assessors can use three methods to evaluate the controls: examine, interview, and test (National Institute of Standards and Technology, 2014, p. D-1). After the organization selects an assessor, they establish an assessment plan, outline the controls to be evaluated, perform the assessment, and report all findings and recommendations to remediate any issues identified. Finally, the organization uses the report to create a Plan of Action and Milestones (POA&M) to address the vulnerabilities.

While assessing the payroll system, the assessors observed five issues (classified according to risk ratings proposed by the National Institute of Standards and Technology (2012)), including one very-high-risk vulnerability, one high-risk, two moderate-risk, and one low risk. Figure 2 illustrates the POA&M developed by the organization outlining the actions the responsible team will take to address the vulnerabilities identified in the payroll system.

Figure 2.

Plan of Action and Milestones (POA&M) to address vulnerabilities in the payroll system.



POAM ID	Controls	Weakness Name	Weakness Description	Weakness Detector Source	Weakness Source Identifier	Asset Identifier	Point of Contact	Resources Required	Overall Remediation Plan	Original Detection Date	Scheduled Completion Date	Planned Milestones
Payroll-L1	AC-7	Payroll application vulnerable to password guessing attacks	The payroll application does not limit the numer of consecutive invalid logon attempts against users.	Security Assessment Report	None	https://payroll.intern	John Doe - Payroll CSP	The vendor should provide a patch addressing this vulnerability.	Contact the vendor regarding the vulnerability and apply the patch provided when available.	2/10/21	5/18/21	(1) 2021-02-12: Report vulnerability to the vendor (2) 2021-04-18: Receive patch from vendor (3) 2021-04-19: Apply patch in the test environment (3) 2021-05-18: Apply module in the production environment
Payroll-C1	AC-3	Network shares not enforcing access control	The payroll server did not implement access control to the network share housing the payroll database. Therefore, anyone in the corporate network can access the users' PII and cause severe damage to the organization.	Security Assessment Report	None	payroll.internal.net	John Doe - Payroll CSP	None	Restrict access to the network share only to authorized users.	2/10/21	2/16/21	(1) 2021-02-16: Remove excessive permissions from the Payroll server

Security Authorization

The Economist Intelligence Unit (2013) noted that "the main reason for the success of strategic initiatives at their businesses is leadership buy-in and support" (p. 8). The authorization step allows the leadership to review the control implementation and decide if it is sufficient to safeguard the system according to its strategy. Therefore, this step is critical to capture leadership support while ensuring accountability throughout the process. During this phase, the Authorizing Official (AO) receives a package with the information collected during the previous steps - the risk management strategy, organization missions and objectives, system security classification, security plans, baseline controls, the assessment report, and POA&M - that helps to decide in approving or denying the system's operation and under which conditions.

The AO authorized the system to operate during this phase based on the team's remediation plans. The POA&M provided leadership comfort that the blueprint of milestones will reduce the payroll system's risk to an acceptable level.

Continuous Monitoring

Risk management is a process, and changes in the system should be continuously revised to ensure the effectiveness of controls. A successful continuous monitoring strategy "addresses monitoring and assessment of security controls for effectiveness, and security status monitoring" (Dempsey et al., 2011, p. 5). Activities include monitoring changes in the system, ongoing control assessments, impact analysis, and authorization.

Continuous Monitoring Strategy For the Payroll System

To efficiently utilize the organization's resources and ensure alignment with the overall objectives, the payroll system continuous monitoring (CM) strategy should leverage and expand existing policies, procedures, and supporting infrastructure to fit its goals. Four aspects constitute the payroll system CM strategy: configuration management, security impact analyses, and continuous control assessment.

Configuration Management For The Payroll System

The organization must consider three perspectives when defining how to manage the payroll system configuration: the hosting server and database, the payroll software configuration, and the supporting documentation. The organization should consider using a Configuration Management System (CMS) to automate the identification of deviations from the operating system (OS) and database baseline, manage changes in the baseline, and enforce compliance with applicable policies. A version control system like Git (Chacon & Straub, 2021) can track the payroll software configuration files and documentation changes.

Finally, the team supporting the system should follow the organization's change management process before performing any modifications (including patches and performance updates) to the payroll system. Before completing the change, the person responsible should perform an impact analysis to determine potential security implications.

Security Impact Analysis On Changes To The Payroll System

Johnson et al. (2011) define security impact analysis as “the analysis conducted by qualified staff within an organization to determine the extent to which changes to the system affect the security posture of the system” (p. 12). When a change to the payroll system is necessary (for instance, when the vendor releases a software update), the organization must first evaluate it in a test environment to observe potential side effects due to incompatibility and vulnerabilities. If the system functions as expected, the team can execute the change. The organization should also perform additional impact analysis in the production environment once the change process completes.

Continuous Control Assessment

To ensure the system is still authorized to operate, the organization must continuously assess its compliance with the baseline controls. In addition to the CMS’s automated verification, the security team must perform quarterly scans and yearly penetration tests to identify potential vulnerabilities. The audit team must also verify the control implementation annually and report the results to leadership as part of the system authorization.

Ongoing Authorization

The authorization package should be updated with the assessment results and security impact analysis output as part of the system's ongoing authorization. The AO can use this information to determine if the system still operates under an acceptable risk level almost in real-time. This process is only triggered when changes in the risk landscape (for instance, new threats or new vulnerabilities) or the system's security posture occur.

The organization can automate the ongoing authorization process using a combination of the CMS and the workflow provided by a service desk system, particularly the ticketing functionality. For instance, considerable deviations in the baseline or modifications in the payroll system can trigger a ticket sent to the AO for approval.

Conclusion

A successful risk management strategy must support the organization's security objectives and its mission. The steps proposed by the NIST Risk Management Framework (National Institute of Standards and Technology, 2018) provide a structured approach that aligns the risk management requirements with the organization's goals while safeguarding the system's confidentiality, integrity, and availability. As the risk landscape is continually evolving, the continuous monitoring step helps the leadership identify changes in the system's security posture and reassess it still offers an acceptable risk level, timely addressing any concerns.

References

Chacon, S., & Straub, B. (2021). *Pro Git: Everything you need to know about Git* (2nd ed.). Apress. https://git-scm.com/book/en/v2

Dempsey, K., Chawla, N., Johnson, L., Johnston, R., Jones, A., Orebaugh, A., Scholl, M., & Stine, K. (2011). *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* [Special Publication (SP) 800-137]. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-137

The Economist Intelligence Unit. (2013). *Why good strategies fail: Lessons for the C-suite*. Project Management Institute. https://www.pmi.org/-/media/pmi/documents/public/pdf/learning/thought-leadership/why-good-strategies-fail-report.pdf

Johnson, L., Dempsey, K., Ross, R., Gupta, S., & Bailey, D. (2011). *Guide for Security-Focused Configuration Management of Information Systems* [Special Publication (SP) 800-128]. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-128

National Institute of Standards and Technology. (2006). *Minimum Security Requirements for Federal Information and Information Systems* [Federal Information Processing Standards Publications (FIPS PUBS) 200]. U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/fips/200/final

National Institute of Standards and Technology. (2012). *Guide for Conducting Risk Assessments* [Special Publication (SP) 800-30] (Revision 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-30r1

National Institute of Standards and Technology. (2014). *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans* [Special Publication (SP) 800-53A] (Revision 4). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53Ar4

National Institute of Standards and Technology. (2018). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [Special Publication (SP) 800-37] (Revision 2). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-37r2

National Institute of Standards and Technology. (2020). *Control Baselines for Information Systems and Organizations* [Special Publication (SP) 800-53B] (Revision 5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53B

National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organizations* [Special Publication (SP) 800-53] (Revision 5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

Stine, K., Kissel, R., Barker, W., Fahlsing, J., & Gulick, J. (2008). *Guide for Mapping Types of Information and Information Systems to Security Categories [Special Publication (SP) 800-60]* (Revision 1, Vol. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-60v1r1