**Risk Management Framework**

Jose Flores

CSOL-530-02-SU22: Cyber Security Risk Management

Professor Victor Nzeata

August 19, 2022

**Risk Management Framework Process**

The Risk Management Framework (RMF) was created by the National Institute of Standards and Technology (NIST) to provide a step-by-step process to ensure your system is protected. It is a flexible risk-based approach framework that the Department of Defense (DoD) and other federal contractors use to improve their information security and risk management process. The steps RMF uses are: prepare, categorize, select, implement, assess, authorize and monitor.

**Prepare**

The prepare step was updated in the NIST publication 800 37 revs 2 when it was released in December 2018. The preparation step doesn’t require any additional activity; however, it does require assigning and tasking individuals with specific roles associated with the risk management team development (NIST, 2021). The risk management strategy is established to determine the risk tolerance that will be accepted. The risk management strategy will guide and inform higher authorities on making risk decisions based on set priorities, trade-offs, and other risk tolerances. It is paramount that the senior leaders and executives are involved in the preparation step to understand and effectively communicate with one another to meet the organization’s mission. Without the support of senior leaders and executives, there would be no baseline on what risks are acceptable or tolerated. Each role will have an assigned individual with specific responsibilities and tasks to meet. By assigning roles to individuals, there would be a point of contact in case questions or concerns arise. If this step is skipped or not completed, procedures will fall apart. No one will know who is in charge of what tasks; therefore, it is crucial to properly prepare to avoid poor performance.

**Categorize**

The categorize step is where we determine the impact concerning confidentiality, integrity, and availability (CIA). The NIST publication 800-60 *Guide for Mapping Types of Information and Information Systems to Security Categorize* and FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems* are guidelines to categorize your system. Confidentiality is to protect against unauthorized disclosure of data or information. Integrity ensures the data is accurate and there is no modification, altering, or tampering. Availability ensures that the data is available anytime without interruptions or delays. Each core component is evaluated separately on the potential impact on the organization if the core component was to be lost (FIBS 199, 2004). The potential impact scale ranges are low (limited effect), moderate (serious effect), and high (severe or catastrophic impact) (Stine, 2008). The core component is matched with the potential impact the organization will take and will be written like this.

Security Category Payroll’s System = {Confidentiality, Low), (Integrity, Moderate), (Availability, Moderate)}.

It is vital to carefully categorize your system effectively to determine the security controls you select. Miscategorization of your system will result in over-protecting or under-protecting your system. Having less than needed security controls can make your system vulnerable to attacks; however, having more security controls will exhaust your resources quickly.

**Select**

The select step is where the security and privacy control baseline is selected and tailored to protect our system. The NIST publication 800-53 rev 5 *Security and Privacy Controls for Information Systems and Organizations* has eighteen different security controls that may be implemented in the system (Joint Task Force, 2020). In this step, it is crucial to communicate to the cybersecurity engineers because they are the subject matter experts applying the security controls selected. A high-impact system will have more security controls than a low-impact system because you want to ensure your system is well protected. The select step is crucial because it will set the standard on what baselines will be used, and using the wrong baseline will have a domino effect on the upcoming steps.

**Implement**

The implementation step is where we start to implement the selected security controls we decided based on the impact levels. Each baseline family has in-depth security controls tailored to what is needed to protect our system. For example, the baseline Access Control (AC) can be further defined as Account Management (AC-2) or Separations of Duties (AC-5) base controls. Both security controls fall under Access Control; however, it specifies even more about what is needed to be controlled. The base control can have a controlled enhancement which can add functionality and specificity or increase the strength of the base control (800 -53). It is essential further to tailor the baseline security control to the system protection needs to create defense in depth.

**Assess**

The assessment step is where the security controls are reviewed with a security assessment report (SAR). A SAR is a document that provides a structured approach to correct any vulnerabilities or weaknesses found in the security control implements. The security control assessor (SCA) is overall responsible for executing, managing, and planning the SAR. Once the SAR is completed, initial remediation and recommendations are made to correct non-compliant security controls. It is essential to be thorough in the SAR because other documents will depend on how accurate and informative the assessment is.

**Authorize**

The authorization step prepares a plan of action and milestone (POA&M) detailing the remediation plan for the noncompliant security controls. The POA&M identifies, analyzes, and mitigates the risk in the system. It is important to identify how you will mitigate your risk by elaborating what steps will be taken to correct the issues or new controls used. It will create milestones and schedule deadlines dates to meet in order to continuously improve. In this step, the authorization package will be assembled to submit to the authorizing official for an Authority to Operate (ATO). The authorization package will include the security plan, SAR, POA&M, and supporting documentation used in POA&M. Without the approval of an ATO, we will need to start again from the beginning to see what steps were not accurate or correct.

**Monitor**

The final step of RMF is continuous monitoring of the system. This last step does not mean it ends; instead, it will continue until the RMF is decommissioned or reassessed. The POA&M will be updated throughout the time when new vulnerabilities are discovered. An effective monitoring program will include configuration management, security impact analyses, assessment of selected security control, security status reporting, and active involvement of authorization officials (Continuous Monitoring, 2022).

**Maintaining the Continuous Monitoring**

Information technology (IT) is constantly changing and evolving every day. New devices, laws, policies, procedures, vulnerabilities, personnel, threats, and other similar factors are introduced to the IT world. The continuous monitoring step must be able to adapt to these factors and implement control or changes to ensure the system is protected. The involvement of executive-level personnel, information system management, and authorization officials is critical because they will be the final decision makers when you recommend a new control or change. Changes to personnel, hardware/software/firmware, and environment will have new and updated controls to ensure the system remains under control.

**Personnel** **Change**

Personnel changes can range from entry to executive level in the cooperation. Regardless any change of personnel will trigger security controls to ensure the system remains secure. The Access Control (AC) security control family would help monitor account management for all personnel. Communication between the IT and Human Resource (HR) departments is essential when personnel leave or enter the organization. If personnel leave the organization, the HR department should communicate that the individual has left, and the account should be deleted immediately. However, continuous monitoring frequency should be established depending on each security control. The frequency will vary depending on the company's size, leave/hire turnover ratio, change of equipment, and other factors. This is why it is crucial to have authorization officials involved because they see the work environment rhythm and will decide if the recommendation is necessary or not. An executive-level change of personnel will have their account and privilege revoked. An entry-level personnel change will have their account deleted due to their limited access.

**Hardware/Software/Firmware Change**

When changing or upgrading the hardware/software/firmware, procedures must be implemented before installing the equipment. Configuration Management (CM) security control will help manage the systems when any system changes are done. The CM security control will work with the Maintenance (MA) security control. Shutting down the whole system during peak hours will impact the cooperation revenues because work will not be done. Therefore it is crucial to set up a schedule for maintenance to change or upgrade the system. However, it is also essential to frequently update your system because new threats and updates are introduced. Patch and system updates should be done weekly during nonworking hours. If the organization operates 24/7, a scheduled time frame should communicate where the organization is willing to accept the system offline. Management will know the optimal time to conduct these updates because they will see when the workflow is in an acceptable timeframe to shut the systems down.

Some supporting tools, such as vulnerability scanning programs can help manage your system. Although it shouldn’t be only used to define the continuous monitoring program, it should be used in conjunction with the other security controls. For instance, a network vulnerability scanner relies on a common vulnerability and exposure (CVE) database. The CVE is a database of software and firmware vulnerabilities that are known. This vulnerability scanner is excellent for tracking known vulnerabilities, but the unknown vulnerabilities will be an issue. Creating an IT department to constantly update and scan your system daily and weekly is necessary to maintain confidentiality, integrity, and availability in the systems. Having vendors update your system would relieve the workload; however, it will open possibilities for new threats in your system. Maintaining a strict access list on who can touch or view your hardware system is as important as who is updating it the systems. Proper background and security checks are recommended before vendors come into the building. This would alleviate any incidents if they were to occur through vendors.

**Change to Environment**

Sharing a workspace with another organization is very risky; however, placing security control will make it manageable. Physical and Environmental Protection (PE), Awareness and Training (AT), and Access Control (AC) are the minimum baseline security controls that should be implemented. Depending if the same network is also being shared, the AC security control will be the first thing established. Regulating who has access to what files and data are essential because it should be need to know business. The other organization shouldn’t have access to the files, data, or work-related information. The access control list should be checked biweekly to ensure no authorized personnel is on the list. The AT security control will help employees understand how to secure their workspace. Training includes providing encrypted documents, locking your computer screen, and being aware of your surroundings. Unauthorized personnel may enter the area by tailgating, but with awareness and training, employees will maintain situational awareness when entering a secure space. Employees will also be taught the term shoulder surfing and maintain awareness when working on classified information. AT security control is recommended every six months to ensure employees maintain awareness when working. If corrective action has been taken with the department or employee or an incident has occurred, a training review should be conducted immediately.

The PE security control will help monitor access to the building and workspace. The organization should establish who has access to what facility and workspaces due to their roles and task. The IT maintenance personnel should have access to the IT area to conduct their updates in the system; however, the regular building maintenance personnel shouldn’t have access to it because it is not part of their responsibility. Visitors and contractors should be aware of two forms of identification prior to coming into the building to verify their identity. Restricted areas should be established, and an access approval list should be developed for personnel working there. The list should be monitored daily because personnel changes can happen overnight. The access list for who has approved visitors, vendors, and contractors should be monitored daily to maintain a strict access point.

Continuous monitoring is not a one-time event in the RMF system. It continuously updates and ensures the system is secured when changes are made. It is constantly adapting to new circumstances by implementing new security controls or changing the ones already established. Checking the security control frequently depends on what is being protected and when the organization allows it to be. Recommendations are made to the authorization officials; however, they have the last approval to agree or disagree with the proposal. Therefore, it is essential to have the authorization official onboard with the recommendations and explain why they are recommended. Continuous monitoring is a balance between frequently over-checking and under-checking the security controls. Frequently checking can disrupt the workspace but not checking enough can impact the organization if a threat enters the system.

# Information System Security Plan

## Information System Name/Title:

## Identifier: BH PR001

## Name: BioHuman’s Payroll

## Information System Categorization:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **LOW** | **X** | **MODERATE** |  | **HIGH** |

## Information System Owner:

## Name: John Bio

## Title: Owner/ CEO

## Agency: BioHuman

## Address: [5998 Alcalá Park](https://www.sandiego.edu/maps/) San Diego, CA 92110

## Phone number: (619) 260-4600

## Authorizing Official:

## Name: Macy Ticks

## Title: Authorizing Offical

## Agency: BioHuman

## Email: Macy.Ticks@biohuman.com

## Address: [5998 Alcalá Park](https://www.sandiego.edu/maps/) San Diego, CA 92110

## Phone number: (619) 260-4601

## Other Designated Contacts:

## Name: Johnny Martz

## Title: Information System Security Officer (ISSO)

## Email: Johnny.Martz@biohuman.com

## Address: [5998 Alcalá Park](https://www.sandiego.edu/maps/) San Diego, CA 92110

## Phone number: (619) 260-4700

## Name: Chris Giggles

## Title: Chief Information Security Officer (CISO)

## Email: Chris.Giggles@biohuman.com

## Address: [5998 Alcalá Park](https://www.sandiego.edu/maps/) San Diego, CA 92110

## Phone number: (619) 260-4705

## Name: Mariana Flo

## Title: Security Control Assessor (SCA)

## Email: Mariana.Flo@biohuman.com

## Address: [5998 Alcalá Park](https://www.sandiego.edu/maps/) San Diego, CA 92110

## Phone number: (619) 260-4710

## Name: Ruben Rod

## Title: Payroll Manager

## Email: Ruben.Rod@biohuman.com

## Address: [5998 Alcalá Park](https://www.sandiego.edu/maps/) San Diego, CA 92110

## Phone number: (619) 260-4720

## Name: Alex Diaz

## Title: Security Manager

## Email: Alex.Diaz@biohuman.com

## Address: [5998 Alcalá Park](https://www.sandiego.edu/maps/) San Diego, CA 92110

## Phone number: (619) 260-4725

## Assignment of Security Responsibility:

## Name: Jose Flores

## Title: Entry Level Cyber Security Analyst

## Email: jose.flores@biohuman.com

## Address: [5998 Alcalá Park](https://www.sandiego.edu/maps/) San Diego, CA 92110

## Phone number: (619) 260-4715

## Information System Operational Status:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **X** | **Operational** |  | **Under Development** |  | **Major Modification** |

## Information System Type:

|  |  |  |  |
| --- | --- | --- | --- |
| X | **Major Application** |  | **General Support System** |

## General System Description/Purpose

## Biohuman contracted Automatic Data Processing (ADP) to manage its payroll system. ADP is a well-known payroll and human resource service platform many organizations use. Biohuman uses the ADP software to manage personally identifiable information (PII) throughout its share drive. When PII is kept at rest in the system, it is encrypted so unauthorized personnel cant view it. The ADP software helps Biohuman manage its 5,000 employees by processing their biweekly paychecks and preparing their tax statements at the end of the year. All PII remains on-site and at its warm site to ensure confidentiality, integrity, and availability remains, and PII being handled in California will fall under the regulations of California Civil Code 1798.82)

## System Environment

## The payroll system will run on 2 Lenovo 2U servers utilizing the think system management. Biohuman has one site and is a small company; therefore only needs one server running. The second server will be a warm site within a radius of 150 miles away from the running server. The think system management will help back up the information to maintain a warm site on a different premise.

## System Interconnections/Information Sharing

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **System Name** | **Organization** | **Type** | **Agreement (ISA/MOU/MOA)** | **Date** | **FIPS 199**  **Category** | **C&A Status** | **Auth. Official** |
| BIO- 001 | Biohuman | Support | MOU | 09/02/2021 | Moderate | Certified and Accredited | Macy. T |
| BIO-002 | Biohuman | Support | MOU | 05/18.2022 | Moderate | Certified and Accredited | Macy. T |

## Related Laws/Regulations/Policies

## California Civil Code 1798.82

## California Consumer Privacy Act of 2018

## Minimum Security Controls

Security Control Baseline: Moderate

Access Control (AC)

The AC family will be implemented by the IT department and will consider the employee's duties and responsibilities when reviewing the account. The executive-level management team will review an access control list of personnel with special access to determine if they need such access. Basic access will be reviewed by the IT department to a final decision will be made by the manager.

Configuration Management (CM)

The CM family is implemented by the IT department and will manage the systems themselves. They will develop diagrams of where all the systems are connected to ensure quick access to the server is available. Macy Ticks will be overall in charge of implementing this control due to the high impact this security control has on the system.

Maintenance (MA)

The MA family is implemented by the IT department and will manage the systems themselves. They will create a schedule and communicate with different departments to ensure continuous work. Overnight working will be authorized with a site manager when conducting system maintenance. Johnny Martz and Chris Giggles will oversee this security control and ensure it is implemented correctly.

Physical and Environmental Protection (PE) and Awareness and Training

The PE family is implemented by the security manager, Alex Diaz. Alex will create a checklist for his team to conduct every day. The common area they will check is blind spots, server room, parking lot, and storage room. They will ensure all monitoring system is up and running with adequate storage memory. If a technical issue were to occur, Alex would contact the IT department. Alex's team will establish RFID access to different workspaces. They will also be in charge of teaching and training all new employees on premises. Lessons they will teach are insider threat, situational awareness, and physical red flag indicators in the building, such as unattended open doors, suspicious packages, and similar factors.

## Information System Security Plan Completion Date: August 13, 2022

## Information System Security Plan Approval Date: August 19, 2022

References:

Continuous Monitoring. (2022). The University of San Diego. <https://learn-us-east-1-prod->

fleet02-xythos.content.blackboardcdn.com

FIPS 199, standards for security categorization of federal ... - NIST. (2004). Retrieved August 13, 2022, from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

Joint Task Force. (2020). Security and Privacy Controls for Information Systems and organizations. CSRC. Retrieved July 30, 2022, from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

NIST RMF Quick Start Guide. (2021). Retrieved August 13, 2022, from https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/01-Prepare%20Step/NIST%20RMF%20Prepare%20Step-FAQs.pdf

Stine, K., Kissel, R., Barker, W., Fahlsing, J., & Gulick, J. (2008). Guide for Mapping Types of Information and Information Systems to Security Categories. CSRC. Retrieved July 11, 2022, from https://csrc.nist.gov/publications/detail/sp/800-60/vol-1-rev-1/final