**Section 1: RMF Preparation**

**1.1 Roles and Responsibilities**

**Authorizing Official:**

|  |  |
| --- | --- |
| Name: | Ashley Smith |
| Title: | Authorizing Official |
| Work Phone: | 210-555-1214 |
| Responsibilities: | The operation of information systems or the use of a set of common controls at an acceptable level of risks to agency operations, agency assets, individuals, and other organizations. |

**Chief Information Officer:**

|  |  |
| --- | --- |
| Name: | Bradley Adams |
| Title: | Chief Information Officer (CIO) |
| Work Phone: | 210-555-1213 |
| Responsibilities: | Deploying and maintaining security policies, procedures, and control techniques to address security requirements |

**System Owner:**

|  |  |
| --- | --- |
| Name: | Kelly Johnson |
| Title: | System Owner |
| Work Phone: | 210-555-1219 |
| Responsibilities: | Procurement, deployment integration, modification, operation, maintenance, and disposal of the system. |

**Information Systems Security Officer:**

|  |  |
| --- | --- |
| Name: | Vern Madden |
| Title: | Information System Security Officer |
| Work Phone: | 210-555-1298 |
| Responsibilities: | Maintaining the appropriate operational security posture for an information system or program. |

**System Administrator:**

|  |  |
| --- | --- |
| Name: | Sophie Steele |
| Title: | System Administrator |
| Work Phone: | 210-555-1914 |
| Responsibilities: | Installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing and conducting backup, recovery, and reconstruction activities; implementing controls; and adhering to and enforcing organization security and privacy policies and procedures. |

**Information Owner:**

|  |  |
| --- | --- |
| Name: | Nellie Hull |
| Title: | Information Owner |
| Work Phone: | 210-555-1983 |
| Responsibilities: | Operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. |

**System User:**

|  |  |
| --- | --- |
| Name: | Annette Zuniga |
| Title: | System User |
| Work Phone: | 210-555-1984 |
| Responsibilities: | Authorized to access information and information systems to perform assigned duties. |

**Control Assessor:**

|  |  |
| --- | --- |
| Name: | Edmundo Fitzgerald |
| Title: | Control Assessor |
| Work Phone: | 210-555-3254 |
| Responsibilities: | Responsible for conducting control assessment. |

**Security Architect:**

|  |  |
| --- | --- |
| Name: | Cruz Spence |
| Title: | Security Architect |
| Work Phone: | 210-555-1256 |
| Responsibilities: | The Information security requirements necessary for protecting the organizations’s core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes. |

**1.2 Possible Risks for a Cloud-based Application**

List and describe risks associated with a cloud-based application. Be sure to include references for your sources of information.

**Ans:**

The Cloud-based applications have associated risks, the risks which are associated are given below in the table.

|  |  |
| --- | --- |
| **ID** | **Control or Control Enhancement Name** |
| AC-3 | Access Enforcement: Cloud platforms store large amounts of confidential data which is prone to attack due to misconfigurations, weak encryption, and flawed Access Control mechanisms. The data can be secured by implementing Role-based Access Control (RBAC), and Multifactor Authentication (MFA), so that only valid users can access the data. |
| SC-12 | Cryptographic Key Establishment and Management: Due to limitations in cloud platforms, sometimes weak encryption standards are used for authentication due to compatibility issues. To mitigate this risk, strong encryption standards e.g. AES-256 must be used. |
| PE-2 | Physical Access Authorization: The users with admin rights can lead to misuse of elevated privileges both intentionally or unintentionally which can lead to the loss of CIA. To overcome this least privilege must be provided to the user and a regular audit must take place to make sure that rights are only given when they are required and they are not being misused. |
| SI-4 | System Monitoring: Lack of a monitoring mechanism can lead to a threat in the form of unauthorized access, data manipulation, and other attacks on the cloud platform. To cover this risk a SIEM solution along with other security applications must be deployed. |
| SC-5 | Denial of Service Protection: The DDoS is the simplest attack on Availability which can turn down the platform to a critical level. To mitigate the attack on Availability, applications like auto-scaling and Load balancers must be used. |
| CP-9 | System Backup: The Cloud platforms are prone to multiple kinds of attacks, system, and network-related failures which can lead to loss of resources as well as business continuity. To fulfill this requirement, regular backups along BCP plans are mandatory requirements. |
| PT-4 | Privacy monitoring and auditing: The private data must be protected at any cost, if the data is stolen by the attacker, it will lead to the loss of data as well as financial liabilities according to the data protection law of that specific country. To secure the data, data encryption along with auditing and data anonymization must be done. |
| CM-6 | Configuration settings: The misconfiguration of security applications e.g. firewalls can lead to a big security breach. To fix this issue, audit tools are used. Vulnerability assessment can also fix these issues. |
| RA-5 | Vulnerabilities Scanning: The vulnerabilities can lead to exploitation of cloud platform e.g. insecure APIs can lead to unauthorized access, for this purpose vulnerability scans are performed, which could be internal or external (with the help of 3rd party). |
| IA-2 | Identification and Authentication: The user accounts must be identified, if it is a legit user or not. If the user is not verified, it can lead to unauthorized access. To address this issue one of the ways is MFA. |
| SI-10 | Information Input Validation: the information input must be standardized e.g. if it is required to upload a non-executable file (PNG, jpeg, etc.) into a website, the executable file must not be allowed, in this way, attacks like SQL injections can be avoided. To address this issue well established framework must be followed so that there is no such flaw in web designing. |
| SC-7 | Boundary Protection: The boundaries of cloud platforms must be protected e.g. Network Boundaries. The network boundaries can be provided by multiple zones e.g. Demilitarization Zone (DMZ), Virtual Private Cloud (VPC), etc. |
| SR-5 | Component Authenticity: It is a risk of the cloud platform one of its examples is Vendor Lock In limitation due to which the migration becomes a troublesome task. To overcome this issue open standard-based multi-cloud implementation must be implemented. |

References:

* NIST 800-53
* NIST 800-37

**1.3 System Categorization**

The categorization has already been determined by another team as:

SC information system = {(confidentiality, LOW), (integrity, MODERATE), (availability, LOW)}

This results in a high-water mark of MODERATE.

**Section 2: Selecting Security Controls**

List the security controls that have been selected based on the System categorization using FIPS-200 guidance and the NIST SP-800-53 baseline security controls.

Ans.

In Table 1, the controls are deployed according to the given high-water mark of Moderate. The controls are divided into 20 different families in the NIST SP-800-53 Framework. According to the requirements provided by FIPS-200, the following controls apply to the given system. Not all controls are deployed, as many controls are elaborated to showcase the understanding of the NIST framework.

Table 1. Security Controls for a high-water mark of moderate.

|  |  |
| --- | --- |
| **ID** | **Description** |
| AC-1 | Access Control Policy and Procedures: Define policies for access control and also explain the working with the help of documentation of procedures. |
| AC-2 | Account Management: The accounts must be managed according to the priority level e.g. Admin privileges must be reviewed after every quarter. |
| AC-3 | Access Enforcement: To check that access is properly controlled and no point is unmanaged. Improper access can lead to vulnerability. |
| AC-17 | Remote Access: The remote access establishment must be secure, if the RDP is taking place at another end the channel must be properly encrypted. |
| AT-1, AT-2 | Security Awareness and Training Procedures: To give awareness to the employees via different mediums e.g. emails, banners, etc. Also, give training to the employees regarding the importance of Information Security, |
| AT-3 | Role-Based Security Training: Each relevant role must be trained and explained the role and the level of access it can have on the system so that there is no misuse of rights. |
| AU-2 | Audit Events: The events must be recorded in the form of logs so that an audit can be performed on them. |
| AU-6 | Audit Review, Analysis, and Reporting: The logs that are collected must be reviewed and analyzed for gaps in the system. After the gaps are identified, gaps must be communicated to the stakeholders. |
| AU-12 | Audit Generation: The important events must be recorded in the form of logs. |
| CA-2 | Security Assessments: The security of the system must be regularly assessed to check if there is some loophole or not. |
| CA-3 | System Interconnections: The communication and connectivity between the systems must be checked, if they are secure or not, If not, the issue must be resolved. |
| CA-7 | Continuous Monitoring: All the important security incidents must be monitored and all the positive events must be responded and also false positives must be identified. |
| CM-1 | Configuration Management Policy and Procedures: The configurations, or the baseline requirements of the system must be specified in policies and procedures. |
| CM-3 | Configuration Change Control: All the major changes must follow the process of change management and they must be recorded properly. |
| CM-6 | Configuration Settings: The baseline requirements of the system must be available |
| CP-2 | Contingency Plan: In case of a node failure, there must be a backup plan to keep the business continuity. |
| CP-3 | Contingency Training: In case of failure, the team must be trained to regain from the failure with the help of backup. |
| CP-9 | Information System Backup: The critical systems e.g. infrastructure systems must be backed up regularly. |
| IA-2 | Identification and Authentication: the user must identify himself and authenticate, in most cases 2FA (Two Factor Authentication) is configured. |
| IA-5 | Authenticator Management: Authentication must be managed by some mechanism e.g. tokens. |
| IR-1 | Incidence Response Policy and Procedures: There must be a playbook to respond to the incidents which must be according to the policy and it should be the part of procedure. |
| IR-4 | Incident Handling: If the incident is positive, the course of action must be defined. |
| IR-6 | Incident Reporting: The incident must be reported to the concerned individual via a proper mechanism e.g. SOC L1 will escalate the event to the L2. |
| MA-2 | Controlled maintenance: While the maintenance work is going on, it must be supervised by proper mechanisms e.g. CCTV, screen sharing, etc. |
| MA-3 | Maintenance Tools: The maintenance tools for systems must be predefined and they must be available when required. |
| MP-2 | Media Access: The access must be controlled and must be given to the relevant person on a specified project. |
| MP-4 | Media Storage: The media storage must be secured from all kinds of attacks e.g. Cyber or Physical attacks. |
| MP-5 | Media Transport: The process of media transport must be defined and it should be foolproof to keep information secure. |
| PE-3 | Physical Access Control: The Physical access of Information assets must be secured e.g. via CCTV cameras, Door access cards, Security doors, etc. |
| PE-6 | Monitoring Physical Access: The physical access must be monitored physically e.g. by the security guard as well as online e.g. with the help of CCTV cameras. |
| PL-2 | System Security Plan: The system security must be properly planned and documented so that there is no issue in case of emergency. |
| PL-4 | Rules of Behavior: The users must be governed by their specified use. |
| PS-2 | Position Risk Designation: The risk must be defined against the specified position in the hierarchy. |
| PS-6 | Access Agreements: The access must be taken after the authorization letter from the customer, without that access must not be granted. |
| RA-1 | Risk Assessment Policies and Procedures: Risk must be assessed according to the process mentioned in policies and it should be performed according to the specified procedures. |
| RA-3 | Risk Assessment: The risk assessment must be completed to prioritize the important assets which are more important. |
| RA-5 | Vulnerabilities Scanning: The loopholes in the system must be scanned by proper procedure and tools which must be defined earlier. |
| SC-5 | Denial of Service Protection: The Availability of the system must be ensured e.g. for securing websites from DDoS attacks, Load Balancers are used. |
| SC-7 | Boundary protection: The communications at the boundaries must be protected with the help of equipment e.g. firewalls. , Etc. |
| SC-13 | Cryptographic Protection: The sensitive data must be encrypted instead of being in plaintext, the secure algorithms like SHA-256 must be used. |
| SI-3 | Malicious Code Protection: The applications must be secured against all kinds of attacks e.g. SQL injection. |
| SI-4 | Information System Monitoring: The information system must be monitored against malicious activity. |
| SI-7 | Software, Firmware, and Information Integrity: The software and Important information must be verified based on HASH values. |

Provide appropriate organization-assigned parameters for these specific controls.

Ans.

In Table Two, the parameters of the controls are defined so that the controls can be applied effectively.

Table 2. Security Control ID and organizational-controlled parameters description

|  |  |
| --- | --- |
| **Security Control ID** | **Organization-controlled Parameters** |
| AT-1 | a. Develop, document, and disseminate to all employees, and stakeholders (3rd parties and contractors)  c. Review and update the current awareness and training:  1. Policy **review annually** and following security incidents, change requests, and regulatory changes; and  2. Procedures **must be reviewed Annually** following **changes in incidents and regulations**, |
| AU-4 | Control: Allocate audit log storage capacity to accommodate logs for **6 to 12 months**.  (1) AUDIT LOG STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE  Transfer audit logs **weekly** to a different system, system component, or media other than the system or system component conducting the logging. |
| CA-3 | a. Approve and manage the exchange of information between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements user agreements; nondisclosure agreements; **Data sharing agreement**];  c. Review and update the agreements **after 12 months.** |
| CP-4 | a. Test the contingency plan for the system **annually** using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: **Backup testing, disaster recovery tests, etc**. |
| IR-4 | Control Enhancements:  (1) INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES  Support the incident handling process using **SOAR [Security, Orchestration, Automation, and Response]**.  (5) INCIDENT HANDLING | AUTOMATIC DISABLING OF SYSTEM  Implement a configurable capability to automatically disable the system if **unauthorized access** **or malware** is detected.  (11) INCIDENT HANDLING | INTEGRATED INCIDENT RESPONSE TEAM  Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in **2 hours**. |
| PE-2 | (2) PHYSICAL ACCESS AUTHORIZATIONS | TWO FORMS OF IDENTIFICATION  Require two forms of identification from the following forms of identification for visitor access to the facility where the system resides: **ID Cards, Employee cards, visitor passes, etc.**  (3) PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS  Restrict unescorted access to the facility where the system resides to personnel with [Selection (one or more): security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained within the system; **Biometric verification**]. |
| PM-23 | Control: Establish a Data Governance Body consisting of **Senior IT managers, InfoSec officers, and legal experts** with **responsibilities of managing and auditing IT resources and getting the issues fixed. Also penalizing the cause of that issue.** |

**Section 3: Implement and Assess Security Controls**

Using the templates provided in this attachment, complete the policies and documents for each of the following:

* Configuration Management Policy (CM-1)
* Maintenance Policy (MA-1)
* Acceptable Use Policy (PS-6)
* Contingency Planning Policy (CP-1)
* Identification and Authentication Policy (IA-1)
* Security Awareness Training Policy (PM-13)

In your submission submit the completed templates for your instructor to review.

Describe the process associated with implementing and documenting security controls. Estimate the timeline and number of people you might need to complete all 238 controls.

**Section 4: Assess Security Controls**

A representative table of your results is shown below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Security Control** | **Examine** | **Interview** | **Test** |
| AC-1 | Review the access control policy and associated procedures with the RMF Framework. | Interview policy owners and other access control policy implementation owners. | Verify the policies with the help of specified tools if the policies are effectively implemented or not. |
| AC-2 | To examine the account management process for creation, deletion, and disabling accounts. | Interview the system administrator to check the account management policy. | Verify the policy and the implementation of account management by the policy. |
| AC-3 | Review the documentation related to the access enforcement mechanisms and system configuration settings. | Interview the system administrator about the access enforcement rule. | The test checks if the authorized users can access the system and if no unauthorized access is possible. |
| AC-4 | To check the information flow between the multiple systems. | To check the flow of information among different systems with the help of an information security officer. | To verify if the information flow is working correctly e.g. if the restricted information can be accessed or not. |
| AC-5 | To review the segregation of duties and procedures related to it. | To check with System/ Network administrators about the separate roles of users. | To check if the different roles can work separately without interference from one another. |
| AC-6 | To check documentation related to the principle of least privilege. | To contact the system administrator to review the privileges. | To check the privileges from low level to high level if they can access or not. |