|  |  |
| --- | --- |
| Element | Description |
| Program |  |
| System/Application | Click here to enter text. |
| Version number | Click here to enter text. |
| CR Number |  |
| Date |  |
| Submitter (Contact Information) |  |
| SIA reviewed by Project SSO |  |
| Initiative/Release Name |  |

# Purpose:

The purpose of this checklist is to develop a set of questions for conducting Security Impact Analysis (SIA) as required by NIST SP800-53 rev. 4, CM-4. This checklist is intended for System Security Officers to use as a guide when analyzing Change Requests (CRs) for potential security risks. *As needed, questions should be modified, added, or removed in order to improve the effectiveness and scope of this checklist.*

|  |  |
| --- | --- |
| Element | Description |
| Project Type |  |
| Description of System Changes | Click here to enter text. |
| Known Baseline Changes (to security configuration baselines) | Click here to enter text. |
| Security Risks | Click here to enter text. |
| Planned Deployment Initiation Date |  |
| Planned Deployment Completion Date |  |
| Systems and Subsystems Impacted by Change | . |
| Current Security Categorization of Impacted System |  |
| Initiative/Release Background | Click here to enter text. |

# Review of CRs during Business Requirements Phase:

The following questions are used in order to identify potential security risks prior to hardware and software acquisitions, architecture modifications, code modifications, and/or new code development.

**Application Changes**

|  |  |  |  |
| --- | --- | --- | --- |
| Impact ID | Change | Yes | No |
| AP-1 | Change in the operating system, security software, firmware or hardware that affects the accredited security countermeasure implemented. |  |  |
| Ap-2 | Change to the configuration of the system (e.g., a workstation is connected to the system outside of the approved configuration) |  |  |
| AP-3 | Change to the system hardware that requires a change in the approved security countermeasure. |  |  |
| AP-4 | Change in the user interface that affects security controls |  |  |
| AP-5 | Change in the security policy (e.g., access control policy) |  |  |
| AP-6 | Change in supporting security components or functionality. |  |  |
| AP-7 | Change in the activity requiring a different security mode of operation. |  |  |
| AP-8 | Creation or modification of an external connection. |  |  |
| AP-9 | Creation or modification of Trust relationships. |  |  |
| AP-10 | Modification of a subscribing system affecting the security of the system. |  |  |

**Network (GSS) Changes**

|  |  |  |  |
| --- | --- | --- | --- |
| Impact ID | Change | Yes | No |
| NT-1 | Change in the operating system, security software, firmware, or hardware that affects the accredited security countermeasure implemented. |  |  |
| NT-2 | Change to the configuration of the servers or network architecture. |  |  |
| NT-3 | Changes to core, distribution, and perimeter IT security infrastructure or devices. |  |  |
| NT-4 | Inclusion of an additional (separately accredited) system |  |  |
| NT-5 | Modification of system ports, protocols or services |  |  |
| NT-6 | Creation or modification of an external connection |  |  |

**Environmental Changes**

|  |  |  |  |
| --- | --- | --- | --- |
| Impact ID | Change | Yes | No |
| EV-1 | Change to the physical structure of the facility or the operating procedures |  |  |
| EV-2 | Change in critically and or sensitivity level that causes a change in the countermeasures required. |  |  |
| EV-3 | Findings from security assessments and audits including internal IT security scans, physical or information security inspections, and internal/external control reviews. |  |  |
| EV-4 | A breach of security, a breach of system integrity, or an unusual situation that appears to invalidate the accreditation by revealing a flaw in security design. |  |  |
| EV-5 | Change in threat or system risk. |  |  |
| EV-6 | Modifications to cryptographic modules or services, deviations from FIPS-140-2. |  |  |

# Review of CRs during Business Requirements Phase:

The following questions are used in order to identify potential security risks prior to hardware and software acquisitions, architecture modifications, code modifications, and/or new code development.

| **Security Impact Questions** | **Y** | **N** | **NA** | **Comments/ Explanations** |
| --- | --- | --- | --- | --- |
| 1. New Hardware: | | | | |
| a. Is new hardware being used?  b. Does the hardware meet FIPS requirements?  c. Has the new system architecture been approved by TRB? |  |  |  | Click here to enter text. |
|  |  |  | Click here to enter text. |
|  |  |  | TRB consult forthcoming |
| 1. Are system documents published in Share Center (i.e. SDD, ICD; Business Requirements, Testing results)? Provide specific information for Share Center link |  |  |  | Click here to enter text. |
| 1. COTS Software: | | | | |
| a. Is new COTS software being procured? |  |  |  | Click here to enter text. |
| b. Has security of the software and architecture design been evaluated? |  |  |  | Click here to enter text. |
| c. How are accounts administered? |  |  |  |  |
| d. Are there application-specific security audit logs? |  |  |  | Click here to enter text. |
| e. Does the COTS software have a need for continual security patching? |  |  |  | Click here to enter text. |
| f. Are instructions for secure application configurations adequately documented? |  |  |  |  |
| g. Is the application capable of ensuring data encryption in transit and at rest? |  |  |  |  |
| h. Was the COTS software presented to TRB? |  |  |  | TRB consult forthcoming |
| i. Has a baseline been created and documented? | ☐ |  | ☐ | Baseline will be updated upon implementation |
| 1. Form Fields: | | | | |
| a. Will new form fields be introduced to web applications? |  |  |  | Click here to enter text. |
| b. Has testing been scheduled for XSS and SQL Injection, etc.? |  |  |  | Click here to enter text. |
| 1. IP Addresses:   Will additional IP addresses be introduced? If so, what are those addresses? |  |  |  | Click here to enter text. |
| 1. PHI/PII Data Elements: | | | | |
| a. Are additional PII/PHI elements being introduced? |  |  |  | Click here to enter text. |
| b. Will these data elements exist in Test Environments? |  |  |  | Click here to enter text. |
| 1. Authentication Methods: | | | | |
| a. Are authentication methods being added or modified? |  |  |  | Click here to enter text. |
| b. Are credentials encrypted both in transit and at rest? |  |  |  | Click here to enter text. |
| c. Is the sensitive data encrypted in transit and at rest? |  |  |  | Click here to enter text. |
| 1. Interconnections: | | | | |
| a. Are any new Interconnections being introduced? |  |  |  | Click here to enter text. |
| b. Is the connection External to CMS- controlled networks? |  |  |  | Click here to enter text. |
| c. Have required interconnection documents been completed? |  |  |  | Click here to enter text. |
| 1. Information Output Changes | | | | |
| a. Are any new reports, emails and/ or displays being created that includes PII/PHI? |  |  |  | Click here to enter text. |
| b. Do new report, emails and/or display designs include provisions and markings to alert the recipient/reader that the information may be sensitive? |  |  |  | Click here to enter text. |

# Review of CRs in Post Development and Testing Phase

The following questions are used to ensure security testing is performed after development.

| **Security Impact Questions** | **Y** | **N** | **NA** | **Comments/ Explanations** |
| --- | --- | --- | --- | --- |
| 1. Version Control: | | | | |
| a. Is there evidence of version control with the software?  b. Has Separation of Duties been enforced?  c. Has Least Privilege been enforced? |  |  |  |  |
|  |  |  | Druva Cloud console allows for configuration of granular permissions to ensure a least privilege approach. |
|  |  |  | Druva Cloud console allows for configuration of granular permissions to ensure a least privilege approach. |
| 1. Have unnecessary programmer comments been removed from code before being promoted to the test environment? |  |  |  |  |
| 1. Has debug code been removed before being promoted to the test environment? |  |  |  | Click here to enter text. |
| 1. Is the source code available for static code scanning/analysis? |  |  |  | Click here to enter text. |
| 1. Have static code scans provided satisfactory results (Low risk vulnerabilities)? |  |  |  | Click here to enter text. |
| 1. If necessary, has remediation been performed to resolve High and Medium risk vulnerabilities before promoting code to the test environment and PROD? |  |  |  | Click here to enter text. |
| 1. Do technical security tests and/or vulnerability scans need to be performed by security in order to validate secure implementation (i.e., IBM App Scan, HP Fortify, etc.)? |  |  |  | Click here to enter text. |
| 1. Have default passwords been changed for remote system interconnections and database connections? |  |  |  | Click here to enter text. |

# User Access to all Test and PROD and PHI/PII Considerations:

The following are questions to consider in determining if Separation of Duties and Least Privilege are enforced for user access to all Test and PROD environments. These questions will be enhanced to better isolate the location of PII/PHI, and how access is controlled and audited. Users who may need this access are generally User Acceptance Testers, Developers, and/or Helpdesk personnel.

| **Security Impact Questions** | **Y** | **N** | **NA** | **Comments/ Explanations** |
| --- | --- | --- | --- | --- |
| 1. Can any of the users defined above promote code into the VAL environment? |  |  |  |  |
| 1. Can any of the users defined above promote code into the PROD environment? |  |  |  |  |
| 1. Sensitive Data: | | | | |
| a. Is there sensitive, PHI / PII data in the Test environment? |  |  |  |  |
| b. If the data is sensitive, is it the same as the data in PROD? |  |  |  |  |
| 1. Can the data in VAL be changed? If so, what type of problem does this cause? |  |  |  |  |
| 1. Roles: | | | | |
| a. What are the other roles? |  |  |  |  |
| b. Are any of these roles able to update data? |  |  |  |  |
| c. If so, how will those roles be tested? |  |  |  | Click here to enter text. |
| 1. If there is logging of system access for is there a regular process to review the logs? |  |  |  |  |
| 1. To address least privilege access, will the users have access to only those functions and data required to perform their job responsibilities? |  |  |  |  |
| 1. Is there any combination of duties / access to be granted that violates segregation of duties? |  |  |  |  |
| 1. Will access be removed as soon as it is no longer needed? |  |  |  |  |
| 1. Is data stored on removable media? |  |  |  |  |
| 1. Will new access roles be created? |  |  |  |  |

Review of CRs in Post Implementation Phase:

The following questions are used to ensure security testing is performed after implementation.

| **Security Impact Questions** | **Y** | **N** | **NA** | **Comments/ Explanations** |
| --- | --- | --- | --- | --- |
| 1. Audit Logs: | | | | |
| a. Have audit logs been generated?  b. If so, how are they used?  c. Are Audit Logs being sent to a central repository? |  |  |  |  |
|  |  |  | Audit logs are generated for each administrative task as well as user backup action history. |
|  |  |  |  |
| 1. Has appropriate documentation been updated (i.e., SDD, ICD, IS RA, CP and SSP)? |  |  |  | SSP will need to be updated. |

# Security Assessment Results and Recommendations

|  |  |
| --- | --- |
| **Element** | Description |
| Summary of Security Impact |  |
| Supported Business Requirement |  |
| **Primary Proposed Solution** | |
| Primary Proposed Solution | Click here to enter text. |
| Primary Proposed Solution Validation Technique | Click here to enter text. |
| **Alternate Proposed Solution** | |
| Alternate Proposed Solution | Click here to enter text. |
| Alternate Proposed Solution Impact Mitigation |  |
| Alternate Proposed solution Impact Mitigation | Click here to enter text. |
| Alternate Proposed Solution Validation Technique |  |
| **Testing Worksheet** | |
| Please describe the tests which needs to be performed against the change: |  |
| Please provide a description of the test results for each change (or provide reference to another document with test results). |  |
| **Analysis Worksheet** | |
| Analysis, Recommendations, and Requirements |  |

|  |  |
| --- | --- |
| **Security Assessment** | **Recommendation** |
| Click here to enter text. | **Approved**  **Not Approved**  **Return for Additional information** |

**System Security Officer (Print Name)**

**System Security Officer (Signature)** **Date**

**System Maintainer (Print Name)**

**System Maintainer (Signature)** **Date**

**CMS ISSO (Print Name)**

**CMS ISSO (Signature)** **Date**

**1. AC**: Will change(s) to system effect how the system limits: (i) information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems); and (ii) the types of transactions and functions that authorized users are permitted to exercise.

If so, describe.

**2. AT**: Will change(s) affect required system training to ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities?

If so, describe.

**3. AU**: Will change(s) affect how system audit requirements to (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

If so, describe.

**4. CM:** Will change(s) to the system impact the (i) baseline configuration and inventory of organizational information systems; (ii) establishment and enforcement of security configuration settings; and (iii) ability to monitor and control changes to the baseline configurations and to the constituent components of the systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycle.

If so, describe.

**5. CP:** Will change (s) to the system impact the (i) contingency plans for emergency response, backup operations, and disaster recovery for organizational information systems (ii) availability of critical information resources and continuity of operations in emergency situations.

If so, describe.

**5. IA:** Will change(s) to the system impact how it (i) identifies users, processes acting on behalf of users, or devices; and (ii) authenticates (or verifies) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

If so, describe.

**6. MA:** Will change(s) to the system impact how (i) periodic and timely maintenance is performed; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

If so, describe.

**7**. **IR:** Will change(s) to the system impact the (i) operational incident handling capability for information system, including, detection, analysis, containment, recovery, and user response activities, (ii) the ability to effectively track, document and report incidents to CMS or other external entities.

If so, describe.

**8. PE:** Will change(s) to the system/system environment change how (i) physical access to information systems, equipment, and the respective operating environments is limited to authorized individuals; (ii) the physical plant and support infrastructure for information systems is protected; (iii) supporting utilities for information systems is provided; (iv) and (v) appropriate environmental controls in facilities are provided.

If so, describe.

**9**. **PL:**  Will change(s) to the system/system environment impact the (i) system security plan for information system that describe the security controls in place for the information system (ii) change the rules of behavior for individuals accessing the information systems.

If so, describe.

**10. SC:** Will change(s) to the system effect how (i) communications (i.e., information transmitted or received by organizational information systems) are monitored, controlled, and protected at the external boundaries and key internal boundaries of the information systems; and (ii) architectural designs, software development techniques, and systems engineering principles that promote effective information security are implemented.

If so, describe.

**11.** **RA:** Will change(s) to the system impact how information systems (i) are assessed every three years or whenever a significant change occurs to the information system to determine if security controls are effective in their application; (ii) plans of action with milestones (POAMs) designed to correct deficiencies and reduce or eliminate vulnerabilities; (iii) authorization for processing including any associated information system connections by a designated senior agency official; and (iv) monitoring for continued effectiveness of the controls.

If so, describe.

**12. SA:** Will change(s) to the system effect the information system for (i) any changes to Service Acquisition policy or procedure. (ii.) how the resources are allocated. (iii.) any information system documentation. (iv.) any software usage or implementation. (v.) any external services outside of the information boundary. (v1.) any internal development or integration.

If so, describe.

**13. SI:** Will change(s) to the system effect how (i) system flaws are identified, reported, and corrected in a timely manner; (ii) malicious code protection is employed; (iii) system events are monitored and detected; (iv) the correct operation of security functions is verified; and (v) information is checked for accuracy, completeness, validity, and authenticity.

If so, describe.