Security Risk Assessment

***Process***

***Version 1.0***

Security Risk Management

August 2015

|  |  |  |  |
| --- | --- | --- | --- |
| Revision History | | | |
| Version | **Date** | **Author** | **Change Description** |
| 0.1 | 06/10/2015 | Sampson | 1st Draft |
| 0.5 | 06/17/2015 | Kossi | Updated draft |

Table of Contents

[1 Introduction 3](#_Toc426696340)

[1.1 Objective 3](#_Toc426696341)

[1.2 Scope 3](#_Toc426696342)

[2 Roles and Responsibilities 3](#_Toc426696343)

[3 Security Risk Assessment Overview 5](#_Toc426696344)

[3.1 Information Security Assessment Methods 5](#_Toc426696345)

[3.2 Types of SRAs Required 6](#_Toc426696346)

[3.3 System Development Lifecycle and the SRA Process 7](#_Toc426696347)

[4 SRA Process 8](#_Toc426696348)

[4.1 Project Intake 9](#_Toc426696349)

[4.1.1 Project Intake Process Steps 9](#_Toc426696350)

[4.1.2 Scoping 10](#_Toc426696351)

[4.1.3 Exceptions to Project Intake 11](#_Toc426696352)

[4.2 Planning and Execution - by SRA Type 11](#_Toc426696353)

[4.2.1 SRA Workbook 11](#_Toc426696354)

[4.2.2 Required Documentation 11](#_Toc426696355)

[4.2.3 Product SRA Process 12](#_Toc426696356)

[4.2.4 Project SRA Process 12](#_Toc426696357)

[4.2.5 Advisory SRA Process 14](#_Toc426696358)

[4.2.6 Ad-hoc SRA - Advisory or Project Related 14](#_Toc426696359)

[5 Service Level Agreements 14](#_Toc426696360)

[5.1 SLAs 14](#_Toc426696361)

[5.2 Escalation Procedures 15](#_Toc426696362)

[6 Appendices 17](#_Toc426696363)

[6.1 Appendix A – SRA Process Flow 17](#_Toc426696364)

[6.2 Appendix B – References 21](#_Toc426696365)

# Introduction

Freddie Mac relies on Information Technology (IT) systems to process, transmit, and store information to support the mission of providing liquidity, stability and affordability to the housing market. The Information Security Risk Assessment (SRA) process identifies information security-related risk and plays a critical role in protecting the confidentiality, integrity and availability of Freddie Mac’s information systems.

## Objective

The SRA process establishes a systematic and consistent approach to identify, assess, and manage information security risks associated with projects, systems and applications during Freddie Mac’s System Development Lifecycle (SDLC) processes (i.e. Enterprise Development Methodology (EDM), Agile, Nimble). The process includes identification of projects or systems that will require an SRA, scoping of standards applicable to that project or system and execution of the various types of SRAs. The process supports iterative testing for agile solutions development and requires integration into the initial IT solution’s ideation and development phases in order to support Freddie Mac’s mission.

The SRA process will help support Freddie Mac’s mission by:

* Integrating Information Security (IS) concepts and standards early in the SDLC process to ensure IS is built into the system
* Enhancing security for the IT systems that store, process, or transmit Freddie Mac information
* Enabling management to make well-informed risk management decisions regarding information security risks that may impact the confidentiality, integrity and availability of the Freddie Mac IT systems
* Assisting Application/System and Technology owners in determining whether the residual risk is at an acceptable level or whether additional compensating controls should be implemented to further reduce or eliminate the residual risk
* Verifying compliance with baseline security configurations, IT controls and IS standards

## Scope

This document includes the process for Project and Advisory SRAs. Security Vendor Risk Reviews (SVRR) are completed through a separate process led by Enterprise Vendor Risk Management (VRM) and are not within scope of this document. This document is applicable to any system, product or component that supports a Freddie Mac business process or externally owned system or infrastructure that stores, processes or transmits Freddie Mac data.

# Roles and Responsibilities

Roles and responsibilities related to the SRA tasks are listed in Table 2-1 below. These responsibilities only include the tasks required in context of the SRA processes; they do not include all stakeholders’ responsibilities related to their job functions or other IS functions.

Table ‑: Roles and Responsibilities

| Roles | Responsibilities |
| --- | --- |
| **Project / System Roles** | |
| Project Manager (PM) | * Respond to SRA Analyst requests timely * Ensure changes to Levels of Effort (LOE) are updated in Planview after the 10 day project intake period * Provide all required documentation within a timely manner * Coordinate receipt of required documentation and follow up questions and requests * Ensure required test environments are available for technical testing |
| IT Owner | * Attend SRA closing meeting * Update Management Action Plan (MAP) with remediation actions * Review SRA reports/emails * Acknowledge SRA report findings for moderate/low risk reports |
| Business Technology Officer (BTO) | * Review SRA reports/emails for high risks * Acknowledge SRA report findings for high risk reports * Update MAP with remediation actions |
| Application Owner | * Review SRA reports/emails for high risks * Manage risk acceptances for identified risks that will not be remediated |
| 1st Line Risk and Controls Officer (RCO) | * Review SRA report * Facilitate completion of MAP and risk acceptance |
| **Information Security Roles** | |
| SRA Analyst | * Engage with PM immediately after being assigned to the SRA * Schedule kick off scoping meeting and refine LOE, as necessary * Provide applicable IS standards to Project Team * Review design documentation and the completed assessment workbook questionnaire * Execute the SRA assessment and document findings in the SRA report * Facilitate IS Risk peer and management reviews of report and findings * Coordinate and hold the SRA closing meeting * Finalize the SRA report and send for signature |
| Security Testing (ST) Analyst | * Attend scoping meeting and determine types of technical testing required for the project * Provide updated LOEs, as necessary * Review design documentation to ensure test plan is accurate * Complete and compile technical testing and provides results to SRA Analyst for incorporation into SRA report |
| Information Security Resource Manager (ISRM) | * Attend project intake meeting and add project information with SRA allocations (name and LOE) to IS Resource Tracker * Updates Project Engagement Portal (PEP) with LOE estimate within project intake Service Level Agreement (SLA) timelines * Track and approve Planview allocations for SRA Analysts and notify SRA Analyst and SRA SME of allocation approval |
| SRA SME | * Attend project intake meeting * Determine if SRA is needed and provides LOE estimate and SRA types to ISRM * Notify SRA Analysts of assignment to SRA by entering SRA in SharePoint SRA Tracker |
| IS Compliance | * Attend closing meeting * Work with Action Plan Owner(s) to create MAP for each open risk * Track risks to closure |
| BISO | * Review SRA report * Facilitate completion of MAP and risk acceptance |

# Security Risk Assessment Overview

## Information Security Assessment Methods

There are three primary methods of IS assessments or testing that are completed by IS during a project[[1]](#footnote-1). Sometimes, all three methods are done during a project or only one. Table 3-1 below explains each of these testing methods, who is responsible for identifying whether the assessment needs to be completed and how the assessments are reported.

Table ‑: IS Assessment Methods

| **Assessment Method** | **Description** | **Responsible for Assessment** | **Intake** | **Reporting** |
| --- | --- | --- | --- | --- |
| Security Risk Assessment (SRA) | Assesses risks associated with project, product or vendor’s compliance to IS Standards | IS Risk Team – SRA analyst | * SRA Subject Matter Expert (SME) identifies need for SRA at project intake meeting. * Vendor Risk Management (VRM) identifies need for vendor review during pre-Procurement meetings | SRA Report or Security Vendor Risk Review (SVRR) report |
| Application Code Review (ACR) | Scans custom code for vulnerabilities using tools such as HP Fortify; requires source code to complete | Security Testing (ST) Team | ST Team determines need for ACR on each project. ACRs are done independently from the SRA process, but may be consolidated for reporting purposes. | ACR Report created; stand-alone if no SRA required or included in SRA Report |
| Dynamic Analysis Security Testing (DAST) | Technical testing for vulnerabilities in systems using manual methods and tools such as Burp suite, Appscan, etc. | ST Team | SRA SME determines if DAST needed during an SRA. | DAST Report created; incorporated into SRA report |

## Types of SRAs Required

Within the SRA method of assessment, there are four primary types that can be completed: Vendor, Advisory, Product and Project. Advisory, Product and Project are the only SRAs that are within scope of this process, but the Security Vendor Risk Review (SVRR) is discussed in Table 3-2 to define the coverage of each review.

Table ‑: SRA Types

| **SRA Type** | **Description** | **When Required1[[2]](#footnote-2)** | **Output** |
| --- | --- | --- | --- |
| Product | Type of advisory review covering the purchase of new software/ hardware not already available through Freddie Mac standards; or major upgrades to existing software / hardware approved in Technology Portfolio Insight (TPI/Troux)  *For process details see 4.2.1* | Requirement for all new products and major product upgrades that will be introduced to the Freddie Mac environment. Product SRAs are required to complete the Technical Architecture Assurance (TAA) process. | Email; lists observations on risks the product may introduce, should the product be brought into Freddie Mac |
| Advisory | Advisories are used for ad-hoc SRAs as part of the Enterprise Development Lifecycle (EDM) process, for example, for Proof of Concepts (POC), or outside of EDM through request.  *For process details see 4.2.3* | Advisories should be planned for when a POC will be used or for complicated / large projects where a formal review during design would be beneficial.  IS may initiate an ad-hoc project SRA at the request of management and it may occur in pre-production or production environments. | Report; list observations on risks the project or POC may introduce to Freddie Mac or findings that will or do affect production.  Observations do not require a MAP; Findings will |
| Project | Review security risk associated with any new IT systems or changes to existing IT systems. Most project SRAs are associated with a project, but ad-hoc project SRAs may also be initiated outside of a formal project for review of systems in the production environment.  *For process details see* *4.2.2* | Project SRAs are formal reviews of projects occurring during the project lifecycle and finalizing in Phase 2, prior to deployment. The IS Risk team will determine need for a project SRA on a project-by-project basis following the intake meeting.  IS may initiate an ad-hoc project SRA if there are findings discovered not related to a project being reviewed, at the request of management or to perform formal re-reviews of applications in production. | Report; lists findings that will require remediation actions (following MAP process) |
| Security Vendor Risk Review (SVRR) | IS is an assessment partner within the Enterprise VRM process. SVRR focuses on the vendor’s overall information security program. Application level security and integration into the Freddie Mac environment would still need to be covered by a Project SRA. Initiation of a SVRR is done through the Enterprise VRM and Procurement processes.  *For process details see the SVRM SOP available on the IS Homefront* *site* | Vendor reviews are required when vendors are hosting, processing or storing Freddie Mac data. Each new vendor will be reviewed on a case-by-case basis after triggering a possible review during the Procurement initiation process and completion of Enterprise VRM’s Inherent Risk Form (which replaced the DDR). | Report; lists findings of the vendor’s information security program. Provided within comprehensive VRM report and MAP managed by VRM and business area vendor managers. |

## System Development Lifecycle and the SRA Process

The Enterprise Development Methodology (EDM) is one of the frameworks for delivering technology products and services to Freddie Mac IT customers both internal and external. The EDM consists of the following phases:

* Phase 0: Ideation – requirements gathering
* Phase 1: Design – solutions design
* Phase 2: Construction - Development
* Phase 3: Deployment – deployment of solution
* Phase 4: Operations and Maintenance

SRAs are most often completed in Phase 1 and 2 of the EDM Process. As noted in Table 3-1 above, occasionally an Ad Hoc Project SRA will be completed in Phase 4. Product SRAs can be completed at any time during the EDM process as needed for new technologies and are required for product approval through Architecture’s Technical Architecture Assurance (TAA) process.

IS involvement in any project should be as early in the process as possible to ensure IS standards are addressed during the design phases of a project and the project teams understand the standards that IS will be testing against in Phase 2.

Agile style development processes will require a more iterative testing process, but does not change the concept of early involvement of IS in the lifecycle. Additionally, while the phases do not line up with EDM, the final testing of the solution will need to occur shortly before release to ensure the SRA covers the solution most closely aligned with the production environment. Exact activities for the SRA team during Agile developments are still being worked and are being treated on a project by project basis. PMs should discuss sprint timelines with the assigned SRA Analyst to determine the most appropriate testing cycle.

# SRA Process

The SRA process begins with the IT PMO driven project intake process that formalizes the gathering of LOEs for the various groups needed within IT for each project. During project intake, the IS Risk team resources and review types are determined and a kick off scoping meeting is initiated by the assigned SRA Analyst for in scope projects to fine tune the LOEs and discuss expectations, testing methods and get a better understanding of the project. SRAs, depending on the type, can happen in Phase 1 or 2. Product and advisory SRAs typically occur in Phase 0 or 1, as they document possible risk (observations) regarding a design or introduction of a product. Project SRAs occur in Phase 2 as that review encompasses the developed system through final documentation review and technical testing in the later testing environments to mirror how the system will operate in production.

As noted in *Table 3‑1: SRA Types,* there may be ad-hoc SRAs that are not initiated through the formal ITPMO intake process, however they would still follow a process path similar to the high level diagram in Figure 4-1. These steps would start with an intake process conducted by the SRA Analyst through a kick off scoping meeting, followed by planning and execution. Intake can be initiated by the SRA Analyst through request from IS Management or from another party by emailing the Data Security Risk Management inbox (see section 4.1.3 Exceptions to Project Intake for details). Figure 4-1 provides a relative diagram of these steps and where the majority of the SRAs conducted fit within the EDM process. The sections below detail each of the high level steps – intake, planning and Phase 1 SRAs, and execution and Phase 2 SRAs. Detailed process flows are included in Appendix A.

Figure ‑: High Level SRA Process Diagram

## Project Intake

Project intake includes reviewing project information submitted by a PM seeking resources for required IS testing activities. The purpose is to understand and document scope and provide levels of effort (LOE) and named resources back to the project team for expected testing activities.

### Project Intake Process Steps

The SRA SME and ISRM attend the IT PMO project intake meeting, where they are able to interview PMs who have submitted resource request (PEP) forms to be reviewed at the meeting. During the meeting, the SRA SME will try to gain an understanding of the project enough to be able to determine if Risk team resources are needed, types of SRAs required and the corresponding LOE. The SRA SME may request additional documentation, clarification or a quick follow up meeting from the PM as needed to provide these estimates.

The SRA SME provides an estimated LOE and recommended resource name to the ISRM for entering into the PEP form. While each project is reviewed separately, the SRA SME follows guidelines in determining which SRA types are required and the estimated LOEs for each. These are described in Table 4-1 and 4-2.

Table ‑: Guidelines for determining if an SRA is required

| **Project Description** | **SRA Type** | **Request Phase** |
| --- | --- | --- |
| New Commercial off the Shelf (COTS) or internally produced application or Operation System | Product SRA | 1 |
| Major version upgrade to an existing application (ex. Version 4 to version 5) | Product SRA  Note: a project SRA may be required and will be determined at project intake or during the advisory SRA discussions, as applicable | 1 |
| Proof of Concept (POC) required | Advisory SRA  Note: Project SRA may be required if POC is validated; will need to go back through project intake to determine appropriate next steps | 1 |
| New hardware is being deployed | Project SRA | 2 |
| New system interconnections or new or changing Graphical User Interfaces (GUI) | Project SRA | 2 |
| Change in legal data classification in transit/change in data flow | Project SRA | 2 |

Project SRA hours depend on the scope and size of the project; the SRA SME reviews the time assigned by architecture and engineering for solutions as a basis for the LOE. In addition to the hours listed below, the Risk team will estimate the hours required by the Security Testing (ST) team. The current LOE for Security Technical Testing is 32 hours.[[3]](#footnote-3)

Table ‑: Guidelines for estimating LOEs

|  |  |  |
| --- | --- | --- |
| **Type / Size** | **Size Description** | **Estimated Hours for SRA Analyst** |
| Product SRA | N/A | 8 hours |
| Advisory SRA / POC | N/A | 32 hours |
| Project / Small | <20 hours architecture solution time | 18 hours |
| Project / Medium | 20-40 hours architecture solution time | 24 hours |
| Project / Large | 40-60 hours architecture solution time | 32 hours |
| Project / Major Initiative or complicated architecture | >60 hours architecture solution time | TBD; will depend on the scope of the project and is case by case |

The ISRM verifies availability of recommended resource in Planview, and either confirms the assigned resource or recommends a different resource to the SRA SME. The SRA SME opens an SRA in the SharePoint SRA Tracker[[4]](#footnote-4) which alerts the assigned Analyst that they have an assignment. The SRA Analyst then begins the kick off and scoping activities.

### Scoping

For Project and Ad Hoc (POC) Advisory SRAs, the assigned SRA Analyst emails the PM to set up a scoping meeting (product SRAs do not require a scoping meeting). During the scoping meeting, the PM, ST Analyst and SRA Analyst review the project details and scope using the scoping worksheet that is part of the IS Standards Assessment Workbook (“SRA workbook”).

The SRA Analyst requests an overview of the project, description of the changes or new system, project timeline and milestone dates for phase 2 architecture assessment completion and User Acceptance Testing (UAT) environment availability. The SRA Analyst provides the PM with an overview of the SRA process and requirements for testing and answers any questions on estimated durations.

After the scoping meeting, the SRA and ST Analyst refine the SRA and technical testing LOEs and provide updates to the ISRM. The ISRM then submits the LOE estimate and named resource in the PEP within the required timelines documented in the Project Intake Process.[[5]](#footnote-5) The PM can then enter the resource allocation requests in Planview and the ISRM approves those resource allocations. At the appropriate time in the testing process, the SRA Analyst is responsible for submitting requests for the required technical testing as determined with the ST Analyst.

In addition, the SRA Analyst will document meeting notes and send a follow up message to the PM summarizing the testing decisions made and understanding of the dates. This will serve to ensure the SRA Analyst has the right information and as evidence within the EDM process that the scoping meeting has occurred and the SRA team has been engaged on that project.

### Exceptions to Project Intake

As noted previously, there are cases where a review is ad-hoc in nature, either for a project, advisory or product. Some of these are initiated by the SRA team, while others need to be requested by PMs during a project or for remediation or request by management. PMs or other stakeholders that need to request an SRA outside the project intake process should do the following:

1. Non-project specific product SRAs (e.g. developer tools) are requested through a Product SRA request form on the SRA SharePoint site. This request is specific to product SRAs and requests the name and version of the product, requestor name, project code if available and attachments.
2. If for remediation or an advisory review not associated through a project, contact the IS Risk team via the shared mailbox, Data Security Risk Management. The ISRM will be requested to verify there is no requirement for the request to be submitted through the PEP project intake process prior to the IS Risk team processing the request.

## Planning and Execution - by SRA Type

### SRA Workbook

The SRA workbook’s purpose is to provide a standardized method to document assessment results and provide guidance for testing each of the applicable IS standards. Additionally, it can be provided to the project teams after tailoring as a list of the applicable IS standards for that project. The assessment procedures and questions are meant as guidelines for the SRA analyst and may be tailored for each project or system.

### Required Documentation

Prior to starting execution of any SRA, the SRA Analyst will require a minimum amount of documentation and specific environments to begin the assessment. Depending on the project, the SRA Analyst may request additional documentation. The table below describes these requirements.

Table ‑: SRA Documentation and Environment Requirements

| SRA Type | | Requirements |
| --- | --- | --- |
| Product SRA | * Software vendor, name and exact version * Product security white papers, data sheets and release notes as applicable | |
| Project SRA | * Approved Phase 2 architecture document (near final draft can be provided to start SRA) * Engineering design document * Completed SRA Workbook questionnaire * UAT environment for technical testing | |
| Advisory SRA - POC | * Design documentation (architecture document, engineering design document, etc.) * Test environment | |
| Ad-hoc SRA (Advisory or Project) | * As much information as possible about the identified change/risk * Additional information as requested by the SRA SME | |

### **Product SRA Process**

The Product SRA is a short, research-based SRA to determine if there are any existing vulnerabilities in a technology before introducing the product into the Freddie Mac environment. The basic steps to complete this type of SRA are as follows:

* The SRA Analyst reviews standard, public vulnerability databases and reviews documents provided by the Project Team.
* The SRA Analyst composes and sends an email to the IT Owner and Project Manager with the risk analysis listed as observations. The email will note either no risks or list the risks for the product.
* The Product SRA is complete; if a Project SRA is needed, this is determined during project intake.

The Project Manager and IT Owner review the risk analysis email and the IT Owner makes a decision regarding continued acceptance of the product, if risks are identified. The email is the official review of the product and can be used as evidence during TAA or other reviews where Product SRAs are required.

### Project SRA Process

Project SRAs are most often conducted in alignment with an IT project, through one of the system development lifecycles used at Freddie Mac. Ad-hoc project SRAs can be requested by management and this process is discussed in section 4.2.6. The overall Project SRA process consists of planning and execution steps (see Appendix A for complete process diagrams). Planning includes identifying and communicating the IS standards that are applicable to the project and tailoring the SRA Workbook for that project. If applicable and appropriate environments are available, the ST Analyst may conduct iterative technical testing during this phase.

Project execution begins in EDM phase 2 and after the requested documentation and completed questionnaire is received. If security technical testing (such as DAST) will be conducted, this must be completed in the environment most closely resembling the production environment (often, UAT) and that portion of the testing starts when the environment is ready and associated credentials and URL(s) is provided to the ST Analyst. Execution consists of testing steps, iterative feedback on findings, reporting and SRA closure.

The basic steps to complete this type of SRA are as follows:

Planning:

* The SRA Analyst provides the assessment methodology and the SRA workbook to the Project Team
* The SRA workbook contains the list of standards applicable for the project, an overview of the assessment procedures that will be used to test those standards and the SRA questionnaire to be completed by the project team
* All requests for documentation are submitted with due dates depending on project milestone dates provided by PM during scoping or subsequent status meetings
* The Project Manager provides the SRA workbook to the Project Team members who will complete the SRA Questionnaire worksheet of the SRA workbook
* The Project Team provides the completed SRA Questionnaire and the draft Phase 2 Architecture to the SRA Analyst
* The SRA Analyst reviews the Phase 2 documentation and verifies that the assessment standards are still applicable; if changes to the assessment standards must be made, the SRA Analyst will update the SRA workbook and resend it to the Project Team
* The ST Analyst reviews the Phase 2 documentation and determines if any changes to the security technical testing plan are required; if changes are required the ST Analyst will notify the SRA Analyst and the Project Team

Non-technical testing

* The Project Team sends the final draft or approved Phase 2 Architecture document to the Analyst (note: the approved Phase 2 architecture is a required document for SRA reporting, however the final draft may be used to start the assessment)
* The SRA Analyst completes the Phase 2 assessment using the assessment procedures in the SRA workbook to assess the system’s compliance with IS Standards
* The SRA Analyst will review the global enterprise risks list and determine if any of the findings are known infrastructure or global risks

Security Technical testing

* The ST Analyst completes the Phase 2 technical testing following the Security Testing Procedures
* The ST Analyst provides the SRA Analyst with a report on all technical security findings for incorporation into the SRA report

SRA Report compilation

* The SRA Analyst reviews all findings documented in the technical testing report and the SRA workbook and determines risk ranking on all findings. The SRA Risk Calculator is used as guidance to determine impact and likelihood of a finding based on system categorization and finding details
* The SRA Analyst uses the latest SRA Report template to compile the SRA report. The SRA report incorporates:
  + Valid technical findings from the ST Analyst’s testing
  + Findings from the SRA Analyst’s assessment against the IS Standards
  + Inherited risks from global enterprise infrastructure, and SVRR and Product SRAs
* The SRA Analyst will conduct internal QA reviews and pre-review of the findings with the PM and project teams as needed

Closing

* The SRA Analyst schedules an SRA closing meeting and sends the draft SRA Report to the meeting attendees, who should consist of the following:
  + SRA Analyst and SRA Senior Analyst or Manager
  + PM
  + Technical leads for project
  + Appropriate signatory for report, depending on risk level
  + Representative from the IS Compliance team (SRA REM)
  + Representatives from the associated business area’s first and second lines
* All invited attendees should attend the formal closing meeting or send representatives in their place. At the closing meeting, the SRA Analyst will review the report details as needed, focusing the discussion on the findings and risk levels.
* The SRA Analyst finalizes the SRA report and sends for signature
  + High risk systems will be sent to the BTO for signature
  + Low/Medium risk systems will be sent to the IT Owner (“Supported By” role) for signature and a copy sent to the BTO
  + Application Owners should be copied on all SRA report submissions
* After the report is finalized, the SRA moves into the remediation steps per the IS Compliance team’s Remediation process.

### **Advisory SRA Process**

Advisory SRAs are most often used to review POCs, but may also be used in an ad-hoc fashion as requested by management. The process reviewed in this section is applicable to the POC review through the system development lifecycle. (The ad-hoc SRA process is in section 4.2.4).

As with the Project SRA, the SRA Analyst scopes the security standards listed in the SRA workbook and provides the workbook to the project team to answer the questionnaire. The SRA Analyst also requests any POC related design documentation. The Project Manager collects and sends the POC design documentation to the SRA Analyst for review and testing commences with the available information.

To complete the Advisory process, the SRA Analyst completes an email or report, depending on the findings identified, and sends to the PM and IT owner for review. Findings in the advisory reviews are observations only unless they pose a security risk to the current environment (e.g. Production data used in a non-production environment). Observations do not need to be documented in a MAP.

Completion of the Advisory SRA is not the same as a Project SRA where findings identified must be remediated or accepted (unless as noted in exception above). POCs or pre-production systems that get an Advisory SRA must be analyzed by an SRA SME to determine if a Project SRA is needed prior to being deployed into production.

### **Ad-hoc SRA - Advisory or Project Related**

Ad-hoc SRAs are requested on an as needed basis by Freddie Mac Senior Management or when a risk is discovered that is not covered under another SRA. These are classified as either advisory (producing observations only) or project (producing findings) for the purposes of clearly defining process and outcome. It is possible that ad-hoc project SRAs may not relate specifically to an IT project, but may be a review of a production system.

There are no discrete steps for ad-hoc SRAs. These SRAs still consist of planning steps, including meeting with the IT support team or project team, defining which standards are applicable to what is being reviewed and defining the assessment plan; and execution steps. The items specifically requested for each of these SRAs is wholly dependent on the type, scope, location of the system being reviewed. Items requested may include: white papers, design and documentation review with risk observations, technical testing, coordinating of risk management, etc. Ad-hoc SRAs are conducted by Senior SRA Analysts only.

# Service Level Agreements

## SLAs

Service Level Agreements (SLAs) have been identified for certain actions within the SRA lifecycle. Some of the timeframes are dependent upon SRA Analyst workload. The SRA Analyst will communicate expected deviations from the SLAs to the PM at the beginning of the project. The ability to meet the SLA is heavily dependent on responsiveness of the PMs, timely submission of documentation and coordination of testing. For details on the SLAs, refer to Table 5-1 below.

Figure ‑: SRA SLAs

|  |  |  |
| --- | --- | --- |
| **Task Name** | **Responsibility** | **Time to Complete** |
| **Project Intake**: The goal is to initiate the kick off meeting and update the LOE within the 10 day SLA required to provide LOEs. The following durations are guidance to meet this timeframe. | | |
| Assign SRA Analyst to SRA | SRA SME | 2 days\* from Intake meeting |
| Conduct Project Scoping Meeting | SRA Analyst | 2 days after assignment |
| Provide updated LOE to ISRM | SRA Analyst | 1 day after scoping meeting |
| Complete LOE in PEP | ISRM | 5 days for high priority; 10 days for all others (total time from project intake meeting) |
| Approve LOE in Planview | ISRM | Within 1 day of notification of Planview allocation |
| **SRA Execution Timeframes** |  |  |
| Product SRA completion | SRA Analyst | Within 2 days of receiving all information required. |
| ST Technical Testing Completed | ST Analyst | Within 4 days of receiving the appropriate URL, credentials or other technical information required to perform tests |
| ST Technical Testing Report | ST Analyst | Within 1 day of technical testing completion |
| Draft Advisory SRA Report | SRA Analyst | Within 10 days of receiving all requested documents and technical test results |
| Final Advisory SRA Report or Email Completed | SRA Analyst | Within 8 days after draft (only if there are findings otherwise email sent within 5 days of draft) |
| Draft Project SRA Report Completed | SRA Analyst | Within 15 days of receiving all requested documents and technical test results in accordance with the size of the project. This includes internal QA and approval processes and the pre-closing and closing meetings. |
| Final Project SRA Report | SRA Analyst | Within 8 days after draft |

*\*business days*

## Escalation Procedures

In order to meet the SLAs and allow for timely deployment to production, the SRA Analyst must be able to meet with the PM to review the scope and receive requested documentation in a timely manner. The following procedures will be followed to escalate issues.

1. Initial: Email sent requesting a kick off meeting, documentation request or required technical testing information request (e.g. URL or credentials). Email will be sent with requested response date.
2. First follow up: If the response date is not met, the SRA Analyst will send a follow up email repeating the original request with an expected response date of 3 days
3. Second follow up: After 3 days from the first follow up, there is still an unfilled request, the SRA Analyst will send another follow up, escalating to the SRA Manager and the PM’s Manager
4. Third follow up: The third and final follow up will escalate to the IT Lead informing them of the delays that may / will occur due to the delay in setting up a scoping meeting, receiving documentation or receiving technical testing information.

# Appendices

## Appendix A – SRA Process Flow







1. Other security technical testing and scanning occurs outside of the SRA process and is not covered in this document. In addition, the technical security testing team is enhancing their testing capabilities, processes and nomenclature. [↑](#footnote-ref-1)
2. More description of determining when to perform each type of SRA is provided in Section 4.2: Project Intake Process Steps. [↑](#footnote-ref-2)
3. As of July 2015, DASTs are only conducted for internal web servers / services / GUIs. This capability will grow and guidelines for LOEs for additional functions will be added as available. [↑](#footnote-ref-3)
4. Previously this was a responsibility of the PM – to enter an SRA Request. PMs will no longer enter SRA requests for the engagement with IS to start. [↑](#footnote-ref-4)
5. The scoping meeting must be conducted within two days of the SRA Analyst assignment in order to ensure that the LOE will be provided within the Project Intake timelines. [↑](#footnote-ref-5)