CWDS
Child Welfare Digital Services

Child Welfare Digital Services Project

Risk and Issue Management Plan

November 2018

Revision History

Revision / Version #	Date of Release	Author	Summary of Changes
.01	08/01/2014	S. Tanniru	Original Draft Document
1.0	09/14/2014	S. Tanniru	Baselined SDLC Version
1.5	02/15/2016	S. Tanniru	Revise risk management process to allow for delegated authority on risk identification. Revise issue management process to allow for delegated authority on issue identification.
2.0	07/31/2016	C. Blehm	Revise Risk Management flow to align with agile development approach and add a table that describes the process flow. Revise Issue Management flow to align with agile development approach and add a table that describes the process flow. Revise Roles and Responsibilities. Integrate risk and issue management process from CWS/CMS into the new CWDS process and align to Agile. Incorporate all oversight and PMO comments.
3.0	08/13/2017	C. Blehm	Revise risk management workflow to allow for escalation of risks from service teams and release train and to identify security risks. Update procedure steps. Revise issue management workflow to allow for escalation of issues from service teams and release train and to identify security issues. Update procedure steps. Revise roles and responsibilities. Add executive summary. Develop objective criteria to determine when a service team risk/issue or release train risk should be escalated to a project risk/issue. Define process for the management of security risks/issues. Identify escalation process to the ELT. Developed Risk and Issue Log template for Service Teams.
3.1	8/21/18	S. Tanniru	Revised Risk and Issue closure criteria. Section 4.2 process number 5g, and section 5.2 process number 5g
3.2	8/21/18	J. Thomas	Revised Risk and Issue closure criteria. Section 4.2 process number 5g, and section 5.2 process number 5g.

Revision / Version #	Date of Release	Author	Summary of Changes
3.3	11/27/18	J. Thomas	Revised Risk and Issue closure criteria. Section 4.2 process number 5g, and section 5.2 process number 5g.

Table of Contents

1 EXECUTIVE SUMMARY 0

1.1 PURPOSE 0
1.2 DEFINITIONS 0
1.3 AUTHORITY LEVELS OF MANAGED RISKS AND ISSUES 2
1.4 ESCALATION CRITERIA FOR RISKS AND ISSUES 3

2 INTRODUCTION 4

2.1 PURPOSE 4
2.2 SCOPE 4
2.3 TERMS AND DEFINITIONS SPECIFIC TO RISK AND ISSUE MANAGEMENT 5
2.4 DOCUMENT MAINTENANCE 8
2.5 TRANSITION TO AGILE 8

3 ROLES AND RESPONSIBILITIES 9

4 RISK MANAGEMENT APPROACH 12

4.1 RISK MANAGEMENT PROCESS WORKFLOW 12
4.2 RISK MANAGEMENT PROCESS FLOW DESCRIPTION 14

5 ISSUE MANAGEMENT APPROACH 21

5.1 ISSUE MANAGEMENT PROCESS FLOW 21
5.2 ISSUE MANAGEMENT PROCESS FLOW DESCRIPTION 23

6 RISK AND ISSUE ESCALATION 30

6.1 AUTHORITY LEVELS OF MANAGED RISKS AND ISSUES 30
6.2 ESCALATION CRITERIA FOR RISKS AND ISSUES 31

7 RISK AND ISSUE MANAGEMENT TOOLS 33

7.1 PROJECT RISK DATABASE 33
7.2 PROJECT ISSUE DATABASE 33
7.3 CANDIDATE RISK FORM 33
7.4 CANDIDATE ISSUE FORM 34
7.5 SERVICE TEAM RISK LOG TEMPLATE 35
7.6 SERVICE TEAM ISSUE LOG TEMPLATE 35

1 Executive Summary

1.1 Purpose

The purpose of the Risk and Issue Management Plan is to identify, manage, and minimize negative impacts to the Child Welfare Digital Services (CWDS) Project by:

- Describing the methodology for managing security level risks and issues.
- Describing the criteria for when a service team or release train risk or issue should be escalated to the project level.
- Describing the methodology and tools for identifying, submitting, analyzing, prioritizing, tracking, mitigating, and retiring Project risks.
- Describing the methodology and tools for identifying, submitting, analyzing, prioritizing, tracking, resolving, and closing Project issues.
- Defining the roles and responsibilities of the Project team in the areas of Risk and Issue management.
- Institutionalizing the risk and issue management process for CWDS and setting the expectation that all digital service vendors will integrate with the risk and issue management process.

1.2 Definitions

Risk. A risk is something that may occur and cause unexpected or unanticipated outcomes. The outcome may have a positive or a negative effect. A positive effect is an opportunity, while a negative effect is a threat. Unanticipated outcomes that yield an opportunity for the project will be defined by quality processes in the CWDS Quality Management Plan.

Issues. Risks are distinct from an issue, which is an unexpected or unanticipated outcome that is currently causing an adverse impact to the project.

Risk Response Strategy. The process of developing strategic options, and determining actions, to enhance opportunities and reduce threats to the project's objectives. Risk response strategies can include:

- Accept - involves accepting the consequences of the risk. Acceptance can be active (e.g., developing a mitigation plan to be executed if the risk event occurs), or acceptance can be passive (e.g., taking no action, allowing the risk event to occur, and accepting the resulting consequences).
- Avoid - A risk response strategy that requires risk avoidance efforts to eliminate the threat to the project.
- Mitigate - Requires a calculated response to an Identified Risk, designed to eliminate or reduce the probability of risk occurrence.
- Transfer - includes transferring a negative impact risk by shifting the impact of a threat to the third party. Transferring a positive impact risk involves shifting the beneficial impact to be realized to another entity within or outside the project.

Risk Probability: The likelihood of the risk occurring, expressed as a percentage of either:

- 1 = <20%
- 2 = between 21-40%
- 3 = between 41-60%
- 4 = between 61-80%
- 5 = >80%

Risk Impact: Assesses the impact on the project if the risk occurs:

- 1 = Less than a 5% change to schedule, scope, budget, or quality
- 2 = 5 - 10% change to schedule, scope, budget, or quality
- 3 = 11 – 15% change to schedule, scope, budget, or quality
- 4 = 16 – 24% change to schedule, scope, budget, or quality
- 5 = 25% or greater change to schedule, scope, budget, or quality

Risk Timing: Defines when risk management activities must begin

- Within the next six months
- Six months to a year from now
- Over a year from now

Issue Priority: The importance of the issue severity, ranked Low, Medium or High.

Issue Management Approach: The process of identifying and resolving **issues** in a project or organization. The issue management approach for the CWDS Project encompasses the following steps:

1. Issue Identification
2. Issue Analysis
3. Issue Resolution Planning
4. Issue Resolution Plan Execution
5. Monitor and Control Issues

Risk Management Approach: The process of risk management includes identifying, analyzing and addressing risks in order to mitigate their negative effects on a project. The risk management approach for the CWDS Project encompasses the following processes:

1. Risk Identification
2. Risk Analysis
3. Risk Response Planning
4. Risk Response Plan Execution
5. Monitor and Control Risks

1.3 Authority Levels of Managed Risks and Issues

Entity Managing the Risk/Issue	Type of Risk/Issue	Tracking the Risk/Issue	Examples
Service Teams	Service Team Risk/ Issue that only impacts the team itself. The risk/issue is within the team's control to influence. Should be resolved by the end of the sprint.	Available options: • SharePoint List (template provided) • Excel Spreadsheet • Manual Board	• Resource constraints or availability within the service team. • Technology constraints that can be resolved within the team's influence. • Support service team impediments that are active for more than two sprints.
Agile Release Train (ART)	Release Risk/Issue that impacts the digital service teams involved in the current Program Increment (PI) or Release. The risk/issue is within the ART's control to influence. Should be resolved within the construct of the PI (within six sprints).	ART Release Program Board tracks PI risks and issues ⇩ ROAM Board (Manual) tracks potential Project risks and issues	• Environment build delays that impact more than one team. • Technology issues that cannot be resolved within the six sprints.
Information Security Lead (ISL)	Security Risk/Issue dealing with information security and the potential loss or breach of confidential data. The risk/issue is within the ISL's control to influence. Although it may qualify as a project-level risk or issue, it cannot be managed through the global Risk and Issue Log due to security policy and the confidentiality of the matter.	Confidential and Secure Risk and Issue Log stored on secured network drive	• Google drive is insecure and opens the project to vulnerabilities. • Firewall allows external access point.
Project Management Office (PMO)	Project-Level Risk/ Issue that is global in nature and impacts the entire project.	Clarity (mandatory)	• Technology constraints that require external entities. • Training, OCM or BPR issues with external stakeholders.

Entity Managing the Risk/Issue	Type of Risk/Issue	Tracking the Risk/Issue	Examples
			• Impacts of more than 10% to overall end schedule or budget. • Global resource constraints or delays.

1.4 Escalation Criteria for Risks and Issues

Entity	Escalates Based on Criteria			
	Agile Release Train (ART)	**Project**	**ELT**	**Board of Directors (BOD)**
Service Team	• When a risk/issue no longer impacts only the service team but starts to impact the entities involved in the current or next PI.	• When a risk/issue no longer impacts only the service team but starts to impact the entire project.		
Agile Release Train (ART)		• When a risk/issue no longer impacts only the ART, but starts to impact the multiple digital service teams. • When a risk/issue requires assistance from executive management to resolve.	• When a critical issue becomes an emergency (timing, control agency escalation, media distribution) and needs immediate attention.	
Project			• When a critical issue becomes an emergency (timing, control agency escalation, media distribution) and needs immediate attention.	
ELT				• When SPR or IAPD milestones are delayed by more than 10%.

2 Introduction

2.1 Purpose

The purpose of the Risk and Issue Management Plan is to identify, manage, and minimize negative impacts to the Child Welfare Digital Services (CWDS) Project by:

- Describing the methodology for managing security level risks and issues.
- Describing the criteria for when a serve team or release train risk or issue should be escalated to the project level.
- Describing the methodology and tools for identifying, submitting, analyzing, prioritizing, tracking, mitigating, and retiring Project risks.
- Describing the methodology and tools for identifying, submitting, analyzing, prioritizing, tracking, resolving, and closing Project issues.
- Defining the roles and responsibilities of the Project team in the areas of Risk and Issue management.
- Institutionalizing the risk and issue management process for CWDS and setting the expectation that all digital service vendors will integrate with the risk and issue management process.

2.2 Scope

The scope of this Risk and Issue Management Plan includes the process, constraints and approach to be used by the CWDS team to identify, analyze, plan, implement, monitor and close project risks and issues during the entire life of the project. Stakeholders and Contractors delivering or participating in the delivery of products to the CWDS team will be required to use this Risk and Issue Management Plan in the performance of their project activities.

A risk is something that *may* occur and cause unexpected or unanticipated outcomes. The outcome may have a *positive* or a *negative* effect. A positive effect is an opportunity, while a negative effect is a threat. Unanticipated outcomes that yield an opportunity for the project will be defined by quality processes in the CWDS Quality Management Plan.

Risks are distinct from an issue, which is an unexpected or unanticipated outcome that is *currently* causing an adverse impact to the project.

This plan includes processes and procedures related to risk and issue management for both the Child Welfare System New System (CWS-NS) project as well as the Child Welfare System/Case Management System (CWS/CMS).

2.3 Terms and Definitions Specific to Risk and Issue Management

Term	Definition
Candidate Risk	Being considered by the Project Risk Forum as a tangible risk that can be described and measured.
Candidate Issue	Being considered by the Project Issue Forum as a tangible issue that can be described and measured.
Identified Risk	A candidate risk becomes an identified risk when it has been determined that it can be described and measured. Each identified risk is recorded in the Project Risk Database as a risk item.
Identified Issue	A candidate issue becomes an issue when it has been determined that it can be described and measured. Each issue is recorded in the Project Issue Database as a issue item.
Issue	A matter that requires the attention of project management staff or a matter that is negatively impacting the success of a project task. A current situation or event that must be resolved to avoid adverse impact to the project.
Issue Manager	The staff member responsible for monitoring candidate issues during the issue identification and issue analysis activities.
Release Program Board	Tracks the planned feature sets and MVP for each of the six sprints in each PI. Tracks risks and issues within the PI sphere of influence.
Resolved Issue	An identified issue that is either no longer applicable or that has been resolved/closed.
Retired Risk	An identified risk that is either no longer applicable or that has been retired.
Risk	A potential event that may negatively impact the project if it occurs but may not impede the success of the project if mitigated effectively. Likewise, a potential event may also positively impact the project and provide opportunities for the project.

Term	Definition
Risk Acceptance	A risk response strategy that involves accepting the consequences of the risk. Acceptance can be active (e.g., developing a mitigation plan to be executed if the risk event occurs), or acceptance can be passive (e.g., taking no action, allowing the risk event to occur, and accepting the resulting consequences).
Risk Avoidance	A risk response strategy that requires risk avoidance efforts to eliminate the threat to the project.
Risk Analysis	Risk analysis involves classification and prioritization of risk items, providing recommendations for mitigating and measuring risk items, and reviewing risk item information with the Risk Manager, and the Project Manager or their designee.
Risk Identification	Risk identification focuses on identification of potential events and/or outcomes which may impact the overall success of the project. It occurs during evaluation of processes, operational execution (e.g., reviews, approvals by external entities) and/or performance against standards/guidelines.
Risk Impact	A description of the estimated impact to project operations or outcomes resulting from the occurrence of a risk event or outcome. Risk Impact is expressed as a number between one and five, with one representing the lowest impact and five representing the highest impact to the project.
Risk Manager	The staff member responsible for monitoring candidate risks during the risk identification and risk analysis activities.
Risk Measurement	The methods used to track the risk mitigation and to measure the effectiveness of the mitigation.
Risk Mitigation	A risk response strategy that requires a calculated response to an Identified Risk, designed to eliminate or reduce the probability of risk occurrence. • Elimination – removing the threat of the risk event occurring by eliminating the cause. • Reduction – reducing the exposure of the risk by either reducing the impact on the project, the probability of occurrence, or both.

Term	Definition
Risk / Issue Owner	Owners are responsible for ensuring the mitigation/resolution steps are defined upon the Risk/Issue creation and completed in addressing its closeout. Additionally, Owners are responsible for supplying the Risk and Issue Manager with updates on the progression of the mitigation/resolution. This is done by leaving comments in the comment field of the appropriate Risk/Issue within Jira. Updates are required each time there is one to report, however, ideally there is an update to report at least once per month.
Risk Opportunity	Risk opportunities arise when there are positive outcomes to a risk and an ability to maximize the chances of exploiting unexpected positive effects.
Risk Planning	Risk planning involves assigning risk ownership, developing risk mitigation, developing measurements, reviewing and approving risk mitigation and measurements, translating mitigation into action plans, and recording risk information changes in the Project Risk Database.
Risk Severity	A determination of the importance of the risk based upon: 1) potential impact of the risk on the project, 2) the probability of occurrence, and 3) the risk timeframe.
Risk Probability	The likelihood of the occurrence of the risk expressed as a percentage for the likelihood of risk occurrence.
Risk Timeframe	The period of time within which the risk is expected to occur [short-term (< 6 Months), medium-term (> 6 Months and < 1 Year), or long-term (> 1 Year)].
Risk Tracking and Control	Risk tracking and control involves the oversight and tracking of risk mitigation action plan execution, re-assessment of risks, reporting risk status, and recording risk information changes in the Project Risk Database.
Risk Transfer	A risk response strategy that includes transferring a negative impact risk by shifting the impact of a threat to the third party. Buying an insurance policy is an example of the risk transfer. Transferring a positive impact risk involves shifting the beneficial impact to be realized to another entity within or outside the project.
Resolved-Owned-Accepted-Mitigated (ROAM) Board	Tracks risks and issues that have been escalated from the Release Program Board that are potential project risks and issues.

2.4 Document Maintenance

The CWDS Risk and Issue Management Plan will be updated in real-time as processes and procedures change. A minor version change does not change the intent of the document and consists of spelling, grammatical and minor corrections. A major version is when a document's content is changed and represents a change in intent, change in process, or procedures. Please refer to the CWDS Configuration Management for further detail on version control.

During development of this CWDS Risk and Issue Management Plan, the guidelines and standards provided through the Project Quality Management Plan will apply; specifically all peer review requirements must be met.

2.5 Transition to Agile

As a result of the transition from a pure SDLC, waterfall risk and issue management approach to a more agile approach, the following high level principles were incorporated:

- Candidate risks and issues no longer require voting approval of a governing board – they are submitted for consideration to the risk and issue forum and accepted by the members of the forum that are present.
- Risk and issue identification is the responsibility everyone on the project. Product Owners, Service Managers and Scrum Masters work together to execute the risk and issue management process.
- Only risks and issues that rise to the level of a "project risk or issue" are managed at the Risk and Issue Forum – all other risks that can be influenced by the service team stay within the service team. However, based on specific criteria, service team risks and/or release level may need to be escalated to the project.
    - The project has institutionalized this process by providing the service teams with a mock template for tracking their individual risks and issues.
    - This template mirrors the same fields and process as the Project level Risk and Issue Log to make it easier for risk and issue escalation.
    - Service Team Risk and Issue Log template.

3 Roles and Responsibilities

The following tables describe the roles and responsibilities of the CWS-NS Project stakeholders in the risk and issue arena.

Role	Responsibility
Executive Leadership Team (ELT)	The ELT is comprised of representatives from CDSS, OSI and CWDA that has the following responsibilities: • Provide guidance and direction to risks and issues that are escalated for executive decision making. • With the Information security Lead, manage and provide guidance on identified security risks.
Information Security Lead	The ISL has the following responsibilities: • Identifies security level risks and escalates to the ELT as needed for management and guidance. • Tracks security risks and issues on a separate and confidential log.
Product Owner	Product Owners for all CWDS service teams (Digital Services, Operations or Project Services) have the following responsibilities: • Co-lead and coordinate Risk and Issue Identification efforts within the service team members along with the Service Manager by maintaining a service team Risk and Issue Log • Document Candidate Risks and Issues that rise to the level of a Project risk or issue • Lead and coordinate Risk Mitigation (if assigned owner of a Risk) • Lead and coordinate Issue Resolution (if assigned owner of an Issue)
Project Staff (includes core team members, stakeholders, SMEs, etc.)	Project Staff is comprised of core team members, stakeholders, Subject Matter Experts (SMEs) that have the following responsibilities: • Document candidate Risks and Issues • Lead and coordinate Risk Mitigation (if assigned owner of a Risk) Lead and coordinate Issue Resolution (if assigned owner of an Issue)
Release Manager	The Release Manager has the following responsibilities on behalf of all digital service teams engaged in a particular program increment or release:

Role	Responsibility
	• With the assistance of the DS teams, identifies release level risks. • Tracks release level risks and issues on the Release Program Board. • Escalates release level risks to project risks when specific criteria are met and adds the risk or issue to the ROAM Board. • Works with risk and issue owners to escalate release level risks and issues that to the project level.
Risk and Issue Forum	The Risk and Issue Forum meets bi-weekly and focuses on identifying new candidate risks and issues and managing existing risks and issues. The forum is comprised of the following entities: • Project Management Office (PMO) • Service Managers and Product Owners • Scrum Masters • Executive Leadership Team (ELT) • Risk and Issue Manager The responsibilities of the Risk and Issue Forum members is to: • Discuss candidate Risks and Issues • Conduct Risk and Issue analysis (validate risk statement, assign probability/impact/timing criteria, determine risk response strategy) • Assign ownership to Risks and Issues • Periodically assess if Risk and Issue information needs to be updated • Monitor Risk Mitigation efforts • Monitor Issue resolution efforts • Validate retirement of risks and validate resolution of issues
Risk and Issue Manager	The CWDS Risk and Issue Manager is a member of the Project Management Office (PMO) that has direct responsibility for the following: • Maintain Project Risks and Issues database in Clarity. • Facilitate bi-weekly Project Risks and Issues Meeting • Communicate and coordinate with owners to monitor active Project Risks and Issues • Communicate and coordinate with service teams and the Release train to assess criteria for escalation of local risks and issues. • Update the status of active Risks and Issues in Clarity.

Role	Responsibility
	Provide status reports to Risk and Issue Forums, Project team and the Executive Leadership Team.
Scrum Master/ Project Manager	Scrum Masters for all CWDS service teams (Digital Services, Operations or Project Services) have the following responsibilities: • Facilitate Risk and Issue Identification efforts within the service team and maintain service team Risk and Issue Log • Document Candidate Risks and Issues that rise to the level of a Project risk or issue • Lead and coordinate Risk Mitigation (if assigned owner of a Risk) • Lead and coordinate issue resolution (if assigned owner of an issue)
Service Manager	Service Managers for all CWDS service teams (Digital Services, Operations or Project Services) have the following responsibilities: • Co-Lead and coordinate Risk and Issue Identification efforts within the service team members along with the Product Owner by maintaining a service team Risk and Issue Log • Document Candidate Risks and Issues that rise to the level of a Project risk or issue • Lead and coordinate Risk Mitigation (if assigned owner of a Risk) • Lead and coordinate Issue Resolution (if assigned owner of an Issue)

4 Risk Management Approach

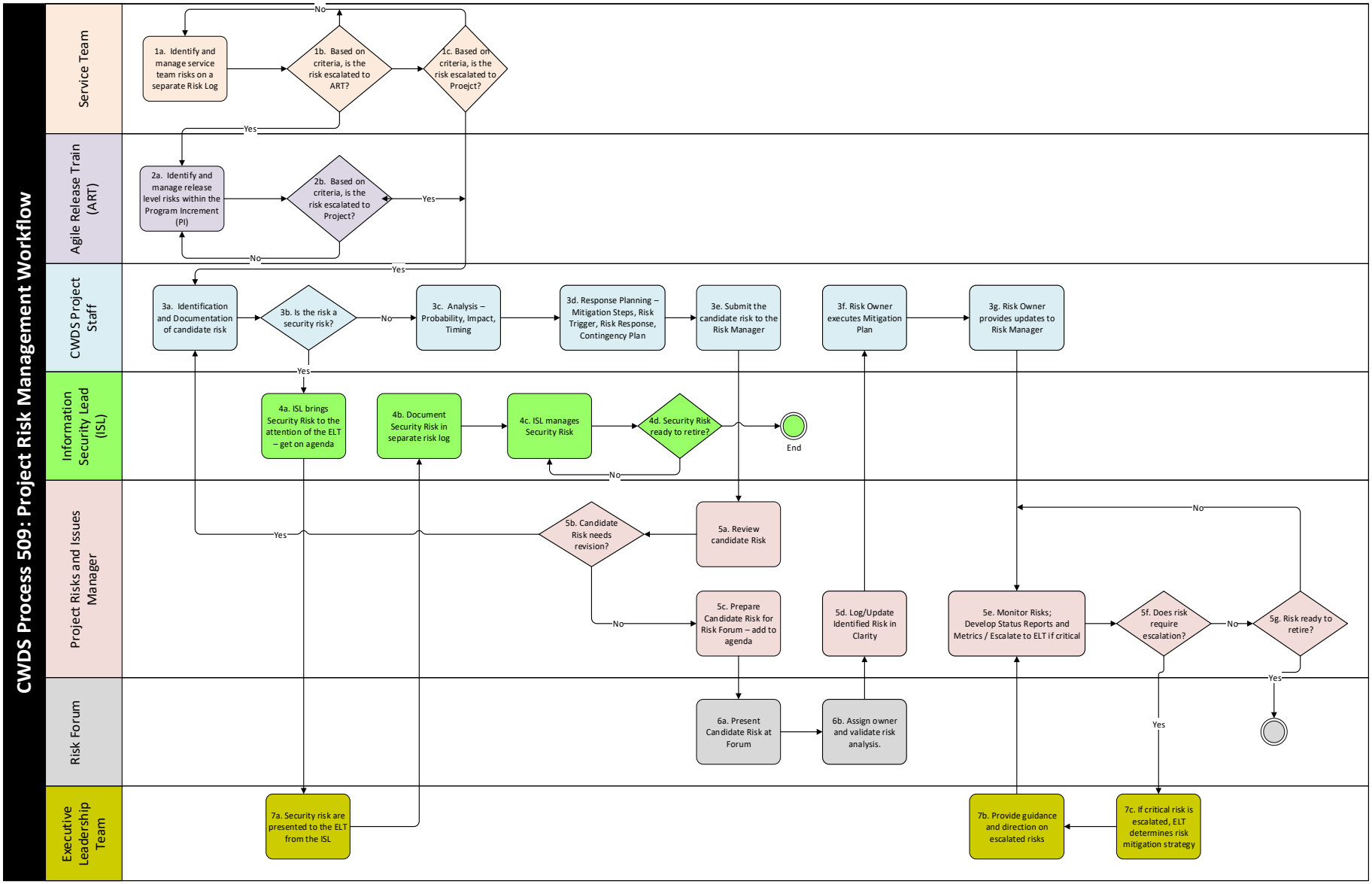
In business, risk management is defined as the process of identifying, monitoring and managing potential risks in order to minimize the negative impact they may have on an organization. A risk is the possibility of an issue that has not occurred yet, and if it occurs, it would have a negative impact on a project (risk threat) or a positive benefit to the project (risk opportunity). Risks can become issues if they are not addressed properly.

The process of risk management includes identifying, analyzing and addressing risks in order to mitigate their negative effects on a project. The risk management approach for the CWDS Project encompasses the following processes:

1. Risk Identification
2. Risk Analysis
3. Risk Response Planning
4. Risk Response Plan Execution
5. Monitor and Control Risks

4.1 Risk Management Process Workflow

The following page illustrates the Risk Management Process Flow for the CWDS Project. The workflow process is located on SharePoint as CWDS Process 509: Risk Management Process Workflow.


CWDS Process 509: Project Risk Management Workflow
Service Team
Agile Release Train (ART)
CWDS Project Staff
Information Security Lead (ISL)
Project Risks and Issues Manager
Risk Forum
Executive Leadership Team
1a. Identify and manage service team risks on a separate Risk Log
1b. Based on criteria, is the risk escalated to ART?
1c. Based on criteria, is the risk escalated to Proejct?
No
Yes
2a. Identify and manage release level risks within the Program Increment (PI)
2b. Based on criteria, is the risk escalated to Project?
Yes
No
Yes
3a. Identification and Documentation of candidate risk
3b. Is the risk a security risk?
No
Yes
3c. Analysis – Probability, Impact, Timing
3d. Response Planning – Mitigation Steps, Risk Trigger, Risk Response, Contingency Plan
3e. Submit the candidate risk to the Risk Manager
3f. Risk Owner executes Mitigation Plan
3g. Risk Owner provides updates to Risk Manager
4a. ISL brings Security Risk to the attention of the ELT – get on agenda
4b. Document Security Risk in separate risk log
4c. ISL manages Security Risk
4d. Security Risk ready to retire?
End
No
5b. Candidate Risk needs revision?
Yes
5a. Review candidate Risk
No
5c. Prepare Candidate Risk for Risk Forum – add to agenda
5d. Log/Update Identified Risk in Clarity
5e. Monitor Risks; Develop Status Reports and Metrics / Escalate to ELT if critical
5f. Does risk require escalation?
No
5g. Risk ready to retire?
No
Yes
Yes
6a. Present Candidate Risk at Forum
6b. Assign owner and validate risk analysis.
7a. Security risk are presented to the ELT from the ISL
7b. Provide guidance and direction on escalated risks
7c. If critical risk is escalated, ELT determines risk mitigation strategy

4.2 Risk Management Process Flow Description

The following table describes the CWDS Project Risk Management Process Flow and the Procedural Steps:

Process Number	Description
1a	**Service teams identify and manage service level Risks within the team on a separate Risk Log.** Risk management is a responsibility for all project members. All service teams have the ability to manage service team specific risks inside the service team. The service teams are expected to keep their own documentation (log, database, post it notes on a poster) to track and manage these service team specific risks. See section 7.5 for Service Team Risk Log template.
1b	**Based on criteria, is the Risk escalated to the ART?** If the risk can no longer be managed within the service team and meets the criteria for escalation, the service team escalates the risk to a Release-level risk managed on the Release Program board. See section 6 for Risk and Issue Escalation.
1c	**Based on the criteria, is the Risk escalated to the Project?** If the risk can no longer be managed at either the service team level or the Release team level and it meets the criteria for escalation, the service team escalates the risk to a Project-level risk managed through the global Risk and Issue Log. See section 6 for Risk and Issue Escalation.
2a	**The Agile Release Train (ART) manages release level risks within the Program Increment (PI).** Release-level risks are identified by the digital service teams participating in a program increment (PI) during the planning process. For any feature or MVP defined in sprints 1-6 of the PI, the digital service teams document red sticky notes with the risk on the Release Program Board. These are risks that are within the ART's influence to manage.
2b	**Based on criteria, is the risk escalated to the project?** If the risk can no longer be managed within the ART and meets the criteria for escalation, the release manager escalates the risk to a Project-level Risk. The red sticky is transferred from the Release Program Board to the ROAM Board and placed in one of four quadrants: Resolved, owned, Accepted or Mitigated.

Process Number	Description
	The Release Manager works with the owner of these escalated risks to document the risk on a candidate risk or issue form and submit to the project.

3a	**Project Staff identifies and documents candidate risk.**
	Risk identification focuses on identification of potential events which could impact the overall success of the project. Project Risks can be identified by many entities including the following:
	• CWS-NS Service Teams:
	  • Service Manager/Scrum Master of a Service Team actively work service team centric risks within their service team.
	  • Service Manager/Scrum Master of a Service Team may identify and document a candidate Project risk that impacts cross-functional teams or has the potential to impact the overall project.
	• Project Management Office (PMO) – PMO may identify and document candidate risks. In addition, PMO reviews risks identified by IV&V and IPOC in order to determine which of those risks, if any, shall be documented as a candidate risk.
	• Project Staff – all project staff have the ability to identify and document a candidate Project risk that has the potential to impact the overall project
	• CWS/CMS – Legacy system risks are included on the global risk register and all candidate risks from CWS/CMS follow the same process as those from CWS-NS.
	• Security Risks - Security Risks may be identified through the Risk Forum, but they cannot be managed through this Forum. Due to the sensitive nature of the potential security risks and in accordance to policy, they must be managed in a separate governance forum to reduce external vulnerabilities.
	• Checks and Balances Oversight - The C&B team may identify risks through their independent oversight process. Once identified, the PMO will work with the executive leadership to determine of these risks should be escalated to a project level risk.

3b	**Is the Risk a Security Risk?** SAM 5305, SAM 5305.6, SIMM 5305A, SIMM 5305B and C, Government Code 6254.19 and Government Code 13400 – 13407 states that security risks must be managed and tracked with a

Process Number	Description
	restricted audience and not open to public review. The current Risk and Issue governance process is open to all project staff and does not allow for the confidential nature of discussing security risks. These risks must go through a separate governance process with the ELT.

3c	**Project Staff conducts Risk Analysis – Probability, Impact and Timing**
	The Service Team, PMO, or any other entity identifying and documenting a candidate risk is responsible for performing risk analysis that includes the following:
	• Probability: The likelihood of the risk occurring, expressed as a percentage of either:
	  • 1 = <20%
	  • 2 = between 21-40%
	  • 3 = between 41-60%
	  • 4 = between 61-80%
	  • 5 = >80%
	• Impact: Assess the impact on the project if the risk occurs:
	  • 1 = Less than a 5% change to schedule, scope, budget, or quality
	  • 2 = 5 - 10% change to schedule, scope, budget, or quality
	  • 3 = 11 – 15% change to schedule, scope, budget, or quality
	  • 4 = 16 – 24% change to schedule, scope, budget, or quality
	  • 5 = 25% or greater change to schedule, scope, budget, or quality
	• Timing Scale: Defines when risk management activities must begin
	  • Within the next six months
	  • Six months to a year from now
	  • Over a year from now

3d	**Project Staff conducts Risk Response Planning** Risk response planning is the process of developing options and determining actions to enhance opportunities and reduce threats to the project`s objectives. It includes the identification and assignment of individuals or parties to take responsibility for each agreed risk response.

Process Number	Description
	The CWDS Service Team, PMO, or any other entity identifying and documenting candidate risk may develop a mitigation plan with respect to the risk being identified. Allowable risk responses are: • Accept - Decision is made not to make changes to project plan to deal with the risk, or no suitable response plan can be identified. The project can live with the consequences of the risk event, and deal with it effectively should the event occur. • Avoid - Change the project plan to eliminate the risk or the condition that causes the risk, or do not perform the activity that causes the risk. • Mitigate - Reduce the probability and/or impact of a risk within an acceptable threshold before the risk occurs by defining active mitigation steps. • Transfer - Transfer risk to a third party who will carry the risk impact and ownership of the response
3e	**Project Staff submit the candidate risk to the Risk Manager.** The entity responsible for identifying the risk should complete the candidate Risk Form and present the candidate risk at the next Risk and Issue Forum.
3f	**Risk Owner executes Mitigation Plan.** The Risk Mitigation Plan is executed after the Risk Forum assigns an owner and validates the Mitigation Plan developed by the risk owner.
3g	**Risk Owner provides updates to Risk Manager.** As the Risk Mitigation Plan is executed, the owner of the Risk provides updates to the Project Risks and Issues Manager. The owner may update the Risk in Clarity (if he or she has access); otherwise the Project Risks and Issues Manager will make the updates in Clarity.
4a	**ISL brings Security Risks to the attention of the ELT.** Due to the sensitive nature of the potential security risks and in accordance to policy, they must be managed in a separate governance forum to reduce external vulnerabilities.
4b	**ISL documents the Security Risk in a separate security log.** SAM 5305, SAM 5305.6, SIMM 5305A, SIMM 5305B and C, Government Code 6254.19 and Government Code 13400 – 13407 states that security risks must be managed and tracked with a restricted audience and not open to public review.

Process Number	Description
	The ISL may choose to use an Excel spreadsheet, a SharePoint Log, or some other database tool, as long as the data is restricted and access is secure.
4c	**ISL manages the Security Risk.** The ISL should manage the risk in the same manner as project risks are managed: • Conduct Risk Analysis – Probability, Impact and Timing • Conduct Risk Response Planning • Execute the Mitigation Plan • Monitor the Risk
4d	**Is the Security Risk ready to retire?** If a Risk has been successfully mitigated or if that Risk is no longer applicable, the ISL will inform the ELT that the Risk can be retired. The Risk along with the reason as to why it should be retired will be presented at the ELT Meeting. If the ELT agrees, the Risk will be retired and updated as such in the Security Risk Database. However, if the ELT does not agree to retire the Risk, the ISL will need to address the concerns of the ELT and continue to mitigate the Risk.
5a	**Risk and Issue Manager reviews Candidate Risk.** After the candidate risk form is completed, it is submitted to the Project Risk and Issue Manager for review. This review includes verification that the fields of the candidate risk form, including the risk statement, are correctly filled out.
5b	**Does the candidate Risk need revision?** The Project Risks and Issues Manager will discuss with the submitter of the risk if any revisions are needed to the candidate risk form.
5c	**Risk and Issue Manager prepares Candidate Risk for Risk Forum.** An agenda is distributed to all Risk Forum attendees no less than 24 hours in advance of each bi-weekly meeting. Any new candidate risks should be included on the agenda and the submitter should be prepared to present the candidate risk at the Forum.
5d	**Log/Update identified Risks in Clarity.** The Project Risk and Issue Manager will log candidate risks as well as update existing risks in the Risk Database.
5e	**Risk and Issue Manager monitors Risks.**

Process Number	Description
	The Project Risks and Issues Manager will monitor active risks, make updates in the Risk Database, develop and provide Open Risk Logs for the Risk Forum, Project Team, as well as the Executive Leadership Team.
5f	**Does risk require escalation?** A Risk Mitigation step or steps may require Executive Decision(s) based on the criteria specified in in the CWDS Project Governance Plan. Based on those criteria, the Project Risk and Issue Manager will escalate such a Risk Mitigation step or steps to the Executive Leadership Team (ELT) for guidance and direction. Typically, all critical risks or risks that are aged more than 180 days are escalated to the ELT.
5g	**Is the risk ready to close?** A Risk may be eligible for closure if it is no longer applicable, can no longer occur, the consequence takes effect or the trigger date has passed (which may essentially turn it into an Issue). In any of these instances, the Risk and Issue Manager will present the Risk for closure along with the justification at the next Forum Meeting. Forum attendees will have the opportunity to offer any objections that may not have been considered by the Risk and Issue Manager before finalizing its closure. Final authority in determining closure for Risks and Issues lies with the Project Administration Director. After the meeting, the Risk shall be closed and updated as such in the Risk and Issue Management Project in Jira accordingly.
6a	**Risk Forum participants present Candidate Risk at Risk Forum.** Once a candidate risk is submitted and added to Clarity, the Project Risk and Issue Manager brings it for consideration to the Risk Forum which is comprised of the ELT, Product Owners, Service Managers and Scrum Masters. The Risk Forum will discuss the candidate risk and perform functions that include, but are not limited to, the following: • Assign an owner for the risk • Validate Risk Analysis • Define and Validate Mitigation plan developed by the owner • Monitor Risk Mitigation activities and closure of the risk

Process Number	Description
6b	**Risk Forum participants assign owner, validate risk analysis and continue to monitor risks.** Monitoring of risks will include reassessment of risk information to determine if any changes are needed including changes to information related to probability, impact, timing, or mitigation plans. Monitoring of risks will also include an analysis of the risk trigger events to determine if a risk has been realized and should be escalated to an issue.
7a	**Security Risks are presented to the ELT by the ISL.** The ELT reviews any security risks that are escalated to the ELT for governance (outside of the normal Risk Forum). The ELT will provide guidance and direction with respect to the escalated security risks that require Executive decision(s).
7b	**Provide guidance and direction to escalated risks.** The ELT will provide guidance and direction with respect to the escalated project risks that require Executive decision(s). The Risk owner shall resume execution of the mitigation plan after ELT has provided guidance and direction.
7c	**If critical risk is escalated, ELT determines the risk mitigation strategy.** Based on business objectives or strategy, the ELT may opt to change the risk response of a critical project risk or provide suggestions for additional risk mitigation steps to be included.

5 Issue Management Approach

In business, issue management is the process identifying and resolving issues in a project or organization. Using the Issue Management Process, staff can identify and resolve issues quickly, before they have an undesirable impact.

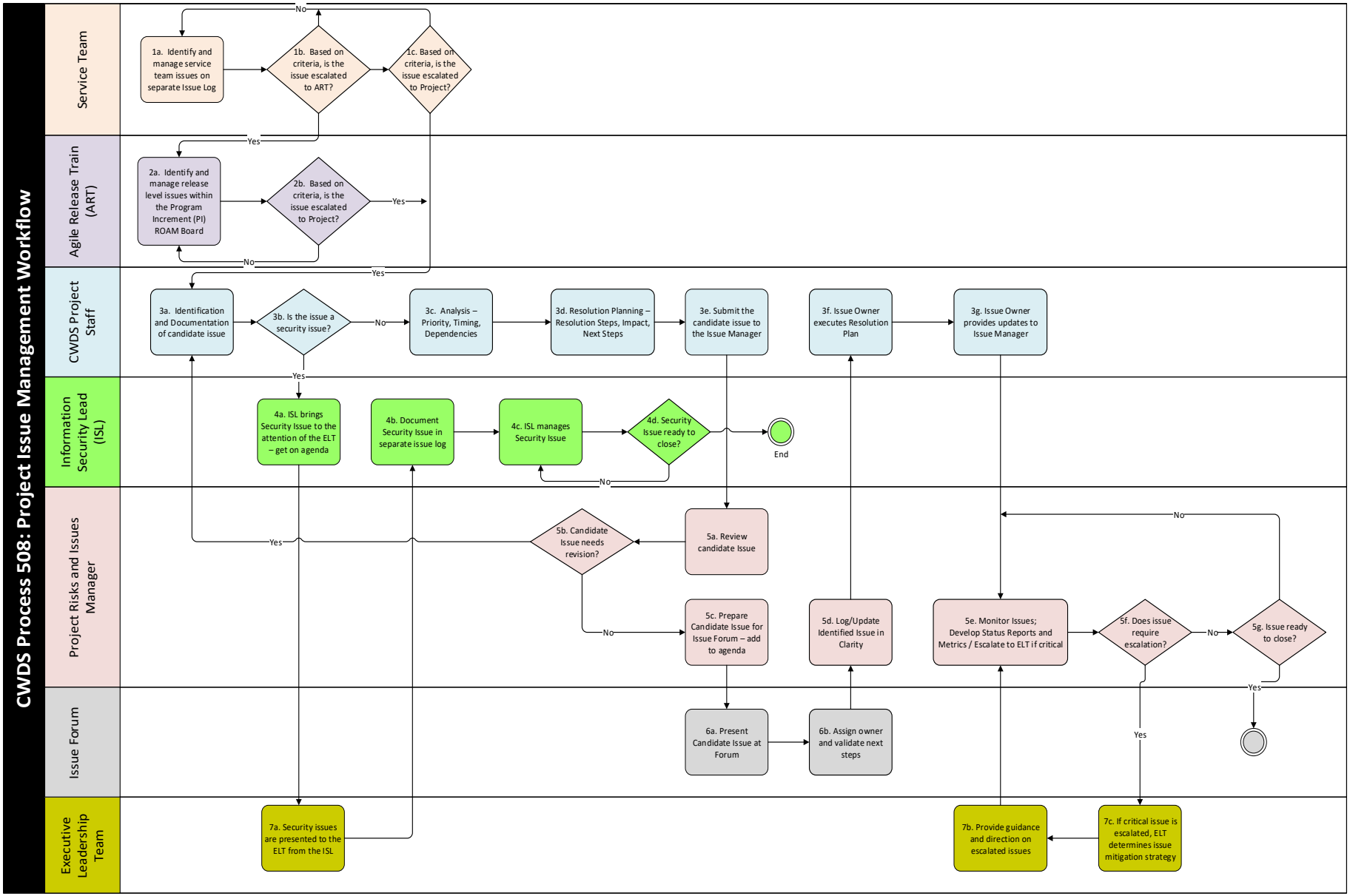
An issue is a known event that is currently negatively impacting the project's chance for success. An issue must be resolved as soon as possible, otherwise it will have detrimental effects on the project.

The issue management approach for the CWDS Project encompasses the following steps:

1. Issue Identification
2. Issue Analysis
3. Issue Resolution Planning
4. Issue Resolution Plan Execution
5. Monitor and Control Issues

5.1 Issue Management Process Flow

The following illustrates the Issue Management process flow for the CWDS Project. The workflow process is located on SharePoint as CWDS Process 508: Issue Management Process Workflow.


CWDS Process 508: Project Issue Management Workflow
Service Team
Agile Release Train (ART)
CWDS Project Staff
Information Security Lead (ISL)
Project Risks and Issues Manager
Issue Forum
Executive Leadership Team
1a. Identify and manage service team issues on separate Issue Log
1b. Based on criteria, is the issue escalated to ART?
1c. Based on criteria, is the issue escalated to Project?
No
Yes
2a. Identify and manage release level issues within the Program Increment (PI) ROAM Board
2b. Based on criteria, is the issue escalated to Project?
Yes
No
Yes
3a. Identification and Documentation of candidate issue
3b. Is the issue a security issue?
No
3c. Analysis – Priority, Timing, Dependencies
3d. Resolution Planning – Resolution Steps, Impact, Next Steps
3e. Submit the candidate issue to the Issue Manager
3f. Issue Owner executes Resolution Plan
3g. Issue Owner provides updates to Issue Manager
Yes
4a. ISL brings Security Issue to the attention of the ELT – get on agenda
4b. Document Security Issue in separate issue log
4c. ISL manages Security Issue
4d. Security Issue ready to close?
End
No
5b. Candidate Issue needs revision?
5a. Review candidate Issue
Yes
No
5c. Prepare Candidate Issue for Issue Forum – add to agenda
5d. Log/Update Identified Issue in Clarity
5e. Monitor Issues; Develop Status Reports and Metrics / Escalate to ELT if critical
5f. Does issue require escalation?
No
5g. Issue ready to close?
Yes
Yes
6a. Present Candidate Issue at Forum
6b. Assign owner and validate next steps
7a. Security issues are presented to the ELT from the ISL
7b. Provide guidance and direction on escalated issues
7c. If critical issue is escalated, ELT determines issue mitigation strategy

5.2 Issue Management Process Flow Description

The following table describes the CWS-NS Project Issue Management Process Flow from the previous page.

Process Number	Description
1a	**Service teams identify and manage service level Issues within the team on a separate Issue Log.** Issue management is a responsibility for all project members. All service teams have the ability to manage service team specific issues inside the service team. The service teams are expected to keep their own documentation (log, database, post it notes on a poster) to track and manage these service team specific issues. See Section 7.6 for Service Team Issue Log template.
1b	**Based on criteria, is the Issue escalated to the ART?** If the issue can no longer be managed within the service team and meets the criteria for escalation, the service team escalates the issue to a Release-level issue managed on the Release Program Board. See section 6 for Risk and Issue Escalation.
1c	**Based on the criteria, is the Issue escalated to the Project?** If the issue can no longer be managed at either the service team level or the Release team level and it meets the criteria for escalation, the service team escalates the issue to a Project-level issue managed through the global Risk and Issue Log. See section 6 for Risk and Issue Escalation.
2a	**The Agile Release Train (ART) manages release level issues within the Program Increment (PI).** Release-level issues are identified by the digital service teams participating in a program increment (PI) during the planning process. For any feature or MVP defined in sprints 1-6 of the PI, the digital service teams document red sticky notes with the issue on the Release Program Board. These are issues that are within the ART's influence to manage.
2b	**Based on criteria, is the risk escalated to the project?** If the risk can no longer be managed within the ART and meets the criteria for escalation, the release manager escalates the risk to a Project-level Risk. The red sticky is transferred from the Release Program Board to the ROAM Board and placed in one of four quadrants: Resolved, owned, Accepted or Mitigated.

Process Number	Description
	The Release Manager works with the owner of these escalated risks to document the risk on a candidate risk or issue form and submit to the project.

3a	**Project Staff identifies and documents the candidate issue.**
	Issue identification focuses on a problem, ***currently occurring***, that must be resolved because it is something that is negatively impacting the project objectives such as scope, schedule, cost or quality. Project Issues can be identified by many entities including the following:
	• CWS-NS Service Teams:
	  • Service Manager/Scrum Master of a Service Team actively works service team centric issues within their service team.
	  • Service Manager/Scrum Master of a Service Team may identify and document a candidate Project issue that impacts cross-functional teams or has the potential to impact the overall project.
	• Project Management Office (PMO) – PMO may identify and document candidate issues. In addition, PMO reviews issues identified by IV&V and IPOC in order to determine which of those issues, if any, shall be documented as a candidate issue.
	• CWS/CMS – Legacy system issues are included on the global issue register and all candidate issues from CWS/CMS follow the same process as those from CWS-NS.
	• Security Issues - Security Issues may be identified through the Issue Forum, but they cannot be managed through this Forum. Due to the sensitive nature of the potential security issues and in accordance to policy, they must be managed in a separate governance forum to reduce external vulnerabilities.
	• Checks and Balances Oversight - The C&B team may identify issues through their independent oversight process. Once identified, the PMO will work with the executive leadership to determine of these issues should be escalated to a project level issue.

3b	**Is the Issue a Security Issue?** SAM 5305, SAM 5305.6, SIMM 5305A, SIMM 5305B and C, Government Code 6254.19 and Government Code 13400 – 13407 states that security issues must be managed and tracked with a restricted audience and not open to public review. The current Issue

Process Number	Description
	governance process is open to all project staff and does not allow for the confidential nature of discussing security issues. These issues must go through a separate governance process with the ELT.
3c	**Project Staff conducts Issue Analysis – Priority, Timing and Dependencies** The Service Team, PMO, or any other entity identifying or documenting a candidate issue is responsible for performing issue analysis that includes the following: • Impact: Description of the impact of the issue on the Project including any impact on the Project scope, schedule, cost, or quality. • Priority: Whether the issue is of Low, Medium, or High priority for the Project to resolve. • Timing: Identify the due date that this issue needs to be resolved by. • Dependencies: Identify if the issue is causing any downstream dependencies on other service teams.
3d	**Project Staff conducts Resolution Planning.** The Service Team, PMO, or any other entity identifying and documenting candidate issue may develop a resolution plan with respect to the issue being identified. If the entity identifying the issue has a recommendation for the issue resolution, they have an opportunity to document their suggestion. However, the issue owner is ultimately responsible for determining the appropriate resolution plan for resolving the issue.
3e	**Project Staff submit the candidate issue to the Issue Manager.** The entity responsible for identifying the issue should complete the candidate Issue Form and present the candidate issue at the next Risk and Issue Forum.
3f	**Issue Owner executes Resolution Plan.** The Issue Mitigation Plan is executed after the Issue Forum assigns an owner and validates the Resolution Plan developed by the issue owner.
3g	**Issue Owner provides updates to Issue Manager.** As the Issue Resolution Plan is executed, the owner of the issue provides updates to the Project Issue Manager. The owner may update the Issue in Clarity (if he or she has access); otherwise the Project Risk and Issue Manager will make the updates in Clarity.

Process Number	Description
4a	**ISL brings Security Issues to the attention of the ELT.** Due to the sensitive nature of the potential security Issues and in accordance to policy, they must be managed in a separate governance forum to reduce external vulnerabilities.
4b	**ISL documents the Security Issue in a separate security log.** SAM 5305, SAM 5305.6, SIMM 5305A, SIMM 5305B and C, Government Code 6254.19 and Government Code 13400 – 13407 states that security Issues must be managed and tracked with a restricted audience and not open to public review. The ISL may choose to use an Excel spreadsheet, a SharePoint Log, or some other database tool, as long as the data is restricted and access is secure.
4c	**ISL manages the Security Issue.** The ISL should manage the issue in the same manner as project Issues are managed: • Conduct Issue Analysis – Impact, Priority, Timing, Dependencies • Conduct Issue Resolution Planning • Execute the Mitigation Plan • Monitor the Issue
4d	**Is the Security Issue ready to retire?** If an Issue has been successfully mitigated or if that Issue is no longer applicable, the ISL will inform the ELT that the Issue can be retired. The Issue along with the reason as to why it should be retired will be presented at the ELT Meeting. If the ELT agrees, the Issue will be retired and updated as such in the Security Issue Database. However, if the ELT does not agree to retire the Issue, the ISL will need to address the concerns of the ELT and continue to mitigate the Issue.
5a	**Risk and Issue Manager reviews Candidate Issue.** After the candidate issue form is completed, it is submitted to the Project Risk and Issue Manager for review. This review includes verification that the fields of the candidate issue form, including the issue statement, are correctly filled out.
5b	**Does the candidate Issue need revision?** The Project Risks and Issues Manager will discuss with the submitter of the issue if any revisions are needed to the candidate issue form.

Process Number	Description
5c	**Risk and Issue Manager prepares Candidate Issue for Issue Forum.** An agenda is distributed to all Issue Forum attendees no less than 24 hours in advance of each bi-weekly meeting. Any new candidate issues should be included on the agenda and the submitter should be prepared to present the candidate issue at the Forum.
5d	**Log/Update identified Issue in Clarity.** The Project Risk and Issue Manager will log candidate issues as well as update existing issues in the Risk Database.
5e	**Risk and Issue Manager monitors Issues.** The Project Risks and Issues Manager will monitor active issues, make updates in the Issue Database, develop and provide Open Issue Logs for the Issue Forum, Project Team, as well as the Executive Leadership Team.
5f	**Does issue require escalation?** An issue resolution plan or step may require Executive Decision(s) based on the criteria specified in in the CWDS Project Governance Plan. Based on those criteria, the Project Risk and Issue Manager will escalate such a Resolution step or steps to the Executive Leadership Team (ELT) for guidance and direction. Typically, all critical issues or issues that are aged more than 60 days are escalated to the ELT.
5g	**Is the issue ready to close?** An Issue may be eligible for closure if it has been successfully resolved with a long-term solution, as opposed to a short term solution or quick workaround. Another motive for closure would be if the Issue is no longer applicable. In either of these instances, the Risk and Issue Manager will present the Issue for closure along with the justification at the next Forum Meeting. Forum attendees will have the opportunity to offer any objections that may not have been considered by the Risk and Issue Manager before finalizing its closure. Final authority in determining closure for Risks and Issues lies with the Project Administration Director. After the meeting, the Issue shall be closed and updated as such in the Risk and Issue Management Project in Jira accordingly.
6a	**Issue Forum participants present Candidate Issue at Issue Forum.**

Process Number	Description
	Once a candidate issue is submitted and added to Clarity, the Project Risk and Issue Manager brings it for consideration to the Issue Forum which is comprised of the ELT, Product Owners, Service Managers and Scrum Masters. The Issue Forum will discuss the candidate issue and perform functions that include, but are not limited to, the following: • Assign an owner for the issue • Validate issue analysis • Validate resolution plan developed by the owner • Monitor issue resolution activities and closure of the issue
6b	**Issue Forum participants assign owner, validate issue response plan and continue to monitor issues.** The Project Issues and Issues Manager will monitor active issues, make updates in the Issue Database, develop and provide status reports for the Issue Forum, Project Team, as well as the Executive Leadership Team. Monitoring of issues will include reassessment of the Issue information to determine if any changes are needed including changes to information related to priority, impact or resolution plans. Monitoring of issues will also include an analysis of the issue resolution events to determine if an issue has introduced any unknown or adverse impacts to the [project and requires the introduction of a new risk.
7a	**Security Issues are presented to the ELT by the ISL.** The ELT reviews any security issues that are escalated to the ELT for governance (outside of the normal Issue Forum). The ELT will provide guidance and direction with respect to the escalated security issues that require Executive decision(s).
7b	**Provide guidance and direction to escalated issues.** The ELT will provide guidance and direction with respect to the escalated project issues that require Executive decision(s). The Issue owner shall resume execution of the resolution plan after ELT has provided guidance and direction.
7c	**If critical issue is escalated, ELT determines the issue resolution strategy.** Based on business objectives or strategy, the ELT may opt to change the issue resolution of a critical project issue or provide suggestions for additional resolution steps to be included.

6 Risk and Issue Escalation

6.1 Authority Levels of Managed Risks and Issues

This section provides guidance on defining the types of risks and issues that can be managed by each entity of the organization and offers some examples of the types of risks and issues that fall within that sphere of authority.

Entity Managing the Risk/Issue	Type of Risk/Issue	Tracking the Risk/Issue	Examples
Service Teams	Service Team Risk/ Issue that only impacts the team itself. The risk/issue is within the team's control to influence. Should be resolved by the end of the sprint.	Available options: • SharePoint List (template provided) • Excel Spreadsheet • Manual Board	• Resource constraints or availability within the service team. • Technology constraints that can be resolved within the team's influence. • Support service team impediments that are active for more than two sprints.
Agile Release Train (ART)	Release Risk/Issue that impacts the digital service teams involved in the current Program Increment (PI) or Release. The risk/issue is within the ART's control to influence. Should be resolved within the construct of the PI (within six sprints).	ART Release Program Board tracks PI risks and issues ⇓ ROAM Board (Manual) tracks potential Project risks and issues	• Environment build delays that impact more than one team. • Technology issues that cannot be resolved within the six sprints.
Information Security Lead (ISL)	Security Risk/Issue dealing with information security and the potential loss or breach of confidential data. The risk/issue is within the ISL's control to influence. Although it may qualify as a project-level risk or issue, it cannot be managed through the global Risk and Issue Log due to security policy and the	Confidential and Secure Risk and Issue Log stored on secured network drive	• Google drive is insecure and opens the project to vulnerabilities. • Firewall allows external access point.

Entity Managing the Risk/Issue	Type of Risk/Issue	Tracking the Risk/Issue	Examples
	confidentiality of the matter.		
Project Management Office (PMO)	Project-Level Risk/ Issue that is global in nature and impacts the entire project.	Clarity (mandatory)	• Technology constraints that require external entities. • Training, OCM or BPR issues with external stakeholders. • Impacts of more than 10% to overall end schedule or budget. • Global resource constraints or delays.

6.2 Escalation Criteria for Risks and Issues

This section provides guidance on when risks managed at lower levels of the organization may need to be escalated to a higher governing body for direction, approval or guidance.

Entity	Escalates Based on Criteria			
	Agile Release Train (ART)	**Project**	**ELT**	**Board of Directors (BOD)**
Service Team	• When a risk/issue no longer impacts only the service team but starts to impact the entities involved in the current or next PI.	• When a risk/issue no longer impacts only the service team but starts to impact the entire project.		
Agile Release Train (ART)		• When a risk/issue no longer impacts only the ART, but starts to impact the multiple digital service teams. • When a risk/issue requires assistance from executive management to resolve.	• When a critical issue becomes an emergency (timing, control agency escalation, media distribution) and needs immediate attention.	
Project			• When a critical issue becomes an emergency (timing, control agency escalation,	

			media distribution) and needs immediate attention.	
ELT				• When SPR or IAPD milestones are delayed by more than 10%.

7 Risk and Issue Management Tools

The project staff shall use the following tools to report, identify, and analyze Risks and Issues as well as to develop and implement comprehensive risk mitigation and issue resolution plans:

7.1 Project Risk Database

All information pertaining to the Risk throughout its lifecycle will be stored in Project Risk Database. The CWS-NS Project will use Clarity for this purpose. Clarity can be accessed by the following URL: https://ondemand.ca.com/web/portal/login.

7.2 Project Issue Database

All information pertaining to the Issue throughout its lifecycle will be stored in Project Issue Database. The CWS-NS Project will use Clarity for this purpose. Clarity can be accessed by the following URL: https://ondemand.ca.com/web/portal/login.

7.3 Candidate Risk Form

Below is an example of the Candidate Risk form. The Candidate Risk Form is a read-only form available on SharePoint:

Risk ID: <<Provided by Risk/Issue Manager**>>**

Reported By: **Date Reported**:

Risk Title:

Risk Statement (Must be less than two sentences**):**

Risk Cause:

Impact Description:

Trigger Event:

Risk Response Strategy: ***(Accept, Avoid, Mitigate, Transfer)***

Probability Scale (<20%, 21-40%, 41-60%, 61-80% or >80%):

Impact Scale (<5% change, 5-10% change, 11-15% change, 16-24% change, <25% change):

Timing Scale *(<6 months, six months to a year, over 1 year from now)**:***

Owner:

Recommended Mitigation Steps:

1.

7.4 Candidate Issue Form

Below is an example of the Candidate Issue form. The Candidate Issue Form is a read-only form available on Share-Point:

Issue ID: <<Provided by Issue/Issue Manager>>

Issue Title:

Issue Description:

Impact Description:

Action Taken to Date:

Priority ***(Low, Medium, High)***:

Date Submitted: **Submitted by:**

Owner:

Resolution Plan/Next Steps:

Due Date:

7.5 Service Team Risk Log template

Below is a template for the service teams to use when identifying and managing their Risks. This Risk Log template is a read-only form available on Share-Point and should be copied to the service team SharePoint site.

ID	Owner	Risk Title Risk Description (no more than two sentences)	Risk Impact	Trigger Event	Response Strategy (Mitigate, Accept, Avoid, Transfer)	Probability 1 = <20% 2 = 21-40% 3 = 41-60% 4 = 61-80% 5 = >80%	Impact 1 = <5% change 2 = 5-10% change 3 = 11-15% change 4 = 16-24% change 5 = <25% change	Timing 1 = < 6 months .66 = 6 -12 months .33 = > 12 months	Priority	Status Open or Closed	Created Date	Recommended Mitigation	Status / Comments	Closed Date	Resolution
RSK-699	Sanabria, David	**Lack of 24/7 Production Support** The CWS-NS Project doesn't have 24/7 production support from vendors (developers, DevOps Engineers) or State staff. As a result, production incidents that occur outside of normal business hours may experience delays in resolution or long outage	Project response to system outages outside normal business hours will be delayed or suffer quality resolution.	1. A production event causes an outage or performance degradation outside of business hours (between the hours of 5:00 PM and 08:00 AM). 2. An alert is generated indicating a potential critical condition outside of business hours.	Mitigate	2	3	0.33	2	Open	8/2/2017	1. Due to limited usage of the CWS-NS in production, need an immediate Project Decision to define availability requirement for production environments to be between the hours of 8:00 AM – 5:00 PM for a short-term period. Set expectations with county partners to allow for the system to be unsupported outside of normal business hours for the next six months, to allow time for contract amendments as needed. 2. Amend DevOps 1 contract to include additional budget for on-call response times, to be used for on-call support only 3. Amend development contracts to include additional budget for on-call support outside normal business hours (on-call support only) 4. Hire additional State staff to provide on-call support outside of normal business hours. 5. Alternative: Engage outside support to provide on-call L2 support for infrastructure outside of normal business hours.	08/02/2017: New risk accepted by the Risk Forum.		

7.6 Service Team Issue Log template

Below is a template for the service teams to use when identifying and managing their Issues. This Issue Log template is a read-only form available on Share-Point and should be copied to the service team SharePoint site.

ID	Owner	Issue Title Issue Description (no more than two sentences)	Issue Impact	Action Taken to Date	Priority (Low, Medium, High)	Status Open or Closed	Created Date	Next Steps	Resolution Plan	Status / Comments	Closed Date	Resolution
ISS-734	Jones, Cheryl	**Lack of COunty Funding for Data Cleanup** Lack of matching State funding for county data cleansing activities may impact the counties ability to meet data quality deadlines.	Lack of sufficient resources allocated to support data quality clean-up activities will hinder the ability for counties.	Thru the ACF approval process, CWS/CMS was able to allocate an additional $2.9m in funds to counties to support data duplication clean-up efforts in the CWS/CMS.	Medium	Open	4/30/2017	1. Work with CDSS to move forward on seeking approval to finalize ACL and CFL to provide funding support for counties.	1. ACL 17-60 posted effective June 22, 2017. The ACL provides the funding approval for CWS Legacy Data Clean Up. Subsequent County Funding Letter pending which will prescribe the method in which counties can claim fund.	08/02/2017: Issue owner provided updated response plan. 07/19/2017: As per the issue owner, the ACL is posted. The CFL with instructions on how counties claim the funding is pending posting by CDSS. Once done, this issue can be retired 06/21/2017: Based on conversation with CDSS, the ACL notification is being communicated to counties which will provide funds to support county resources and concerted effort to support the CWS/CWS DQ effort. Once the ACL letter is out, we can close this risk.		