[ISP Vendor Name]

CYBERSECURITY RISK MANAGEMENT PLAN

Version: v1.4
Version Date: [DD Month YYYY]

Prepared by: Employee Name, Title, Company Name
Employee Name, Title, Company Name
Employee Name, Title, Company Name

TEMPLATE OVERVIEW

***[INSTRUCTIONS:** The "Template Overview" section is intended to be instructional and can be deleted up on completion of the subgrantees completion of their Cybersecurity Risk Management Plan.]*

Template Revision History

The following table shall be used to track authorship for any changes, modifications, or updates to this document.

Table 0-1: Document Revision History

Version	Date	Description of Change	Author
1.0	11/28/23	Template	Commonwealth of Virginia
1.4	10/21/2024	Revised for NIST 2.0	Commonwealth of Virginia

Template Introduction

The purpose of this template is for the Commonwealth of Virginia to provide an accelerator for Internet Service Providers (ISPs) to help them define, document, and disseminate a Cybersecurity Risk Management Plan in-alignment with the requirements as specified by the NTIA within *Section IV.C.2.c.vi of the BEAD Notice of Funding Opportunity (NOFO)*. Use of this document or the associated checklist are not required. Organizations with existing Cybersecurity Risk Management Plans can continue to use the existing documentation, provided it meets the requirements outlined by the BEAD NOFO and further specified in ***National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)*** and ***Executive Order 14028: Executive Order on Improving the Nation's Cybersecurity***.

Document Components

The following outlines the key elements of this template and how to update the document appropriately.

Instructions

Instructions are included in this document to provide clarity, further guidance, and additional resources for the associated phase of the document. The instructions are not intended for direct use within the final program document and should be removed before the document is finalized.

For the purposes of this document, all instructions are contained within square brackets, and are written in italicized red text. The end of all instructions will include a reminder that this text should be removed from the document. Below is a visual example of the instructions found in this document.

***[INSTRUCTIONS:** This will provide additional clarity on how to compose that section of the document.*

Delete this instruction and all other instructions from your final version of the document.]

Example Text

Examples are included in this document as an initial starting point for the authors of the final program document. These excerpts may be included in the final program document, but should be reviewed,

updated, and customized to the ISP Vendor's specific organization. While example text may be included in the final program document, the example tag at the beginning should be removed.

For purposed of this document, all examples are prefixed by the word "example" in bold, blue, all capital letters contained within square brackets, while the text itself should appear normal. This example tag should be removed throughout the document. Below is a visual example of the example tag found in this document.

[EXAMPLE] This text is an example of the content that may be contained after an example tag.

Update Tags

Update tags are included in this document to provide visual highlights for information that needs to be customized for the ISP Vendor's specific organization or where more information is needed.

For purposed of this document, all update tags are highlighted in yellow. These are the only highlights in the document. Sections that require generation of new content rather than minor revisions will be tagged with the word "update" in bold, black, all capital letters contained within square brackets. Below is a visual example of the update tag found in this document.

[UPDATE]

Implementation Summary Tables

At the beginning of each phase of the NIST Risk Management Framework (RMF) program leveraged in this document, an Implementation Summary table has been included where the authors of this document can report on the overall implementation and operationalization of the associated phase of the program. This table includes four (4) key pieces of information:

- **Implementation Status** – describes the status of the operationalization of the controls.
- **Responsible Role** – the title of the organizational role responsible for ensuring the implementation and operationalization of the plan as well as maintaining and updating this section of the plan. Note: Titles are used in lieu of personnel names as the role should still be responsible with staff turnover.
- **Implementation Plan** – If the controls are not fully implemented and operationalized, a timeline and remediation steps should be clearly defined.
- **Planned Date for Full Implementation** – If the controls are not fully implemented and operationalized, the intended date for full implementation should be listed. If the controls are already implemented, this date should reflect the date the program was successfully established and operationalized as defined.

The following describes the listed implementation statuses:

- **Implemented** – The program has been fully operationalized as documented.
- **Partially Implemented** – Some parts of the program have been operationalized, but work is still in progress for full implementation.
- **Planned** – The plan for the control has been clearly defined and documented in the plan, but the organization has not begun to operationalize the defined program.
- **Alternative Implementation** – The control cannot be implemented as intended or designed, but compensating controls have been established to provide equivalent or better protection. Controls with alternative implementation should have a documented explanation in the Implementation Plan.

- **Not Applicable** – The control does not apply to the specific in scope environment. Controls that are not applicable should have a documented explanation in the Implementation Plan.

For purposed of this document, all implementation summary tables can be found at the beginning of each section as applicable. Below is a visual example of the implementation summary table found in this document.

Table 0-2: EXAMPLE Implementation Summary

EXAMPLE Implementation Summary			
Implementation Status (check all that apply):		**Responsible Role:**	
☐ Implemented ☐ Partially Implemented ☐ Planned	☐ Alternative Implementation ☐ Not Applicable	[Named Role(s)]	
Implementation Plan			**Planned Date for Full Implementation:**
[If applicable, insert text or replace with "N/A"]			DD Month YYYY

Key Terminology Definitions

At the end of this document, there is a table for all key terminology and definitions. Organizations may leverage the NIST, IR 7298, Revision 1, Glossary of Key Information Security Terms or the NIST Computer Security Resource Center (CSRC) Glossary found at https://csrc.nist.gov/glossary.

Document Updates

The Commonwealth of Virginia will store the latest version of the cybersecurity risk management plan template at: [insert link].

Attached Checklist

When compiling the Plan, the "BEAD Cybersecurity Risk Management Plan Checklist" can be used as guidance for developing a cybersecurity risk management strategy that meets NOFO requirements and incorporates leading practices. This checklist can be used to confirm that all applicable sections have been included in the Plan. The checklist contains:

- Topics included in Cybersecurity Risk Management Plans; these topics correspond to sections in this Plan template.
- Steps to incorporate into the Plan, which specify content that should be detailed in the Plan.
- NOFO requirement verbiage, NOFO source references, and additional reference materials, as applicable, which provide additional context on the requirements.

DOCUMENT MAINTENANCE

[ISP Vendor] shall ensure that this document reviewed and updated at least annually and following any system update that affects the accuracy of the information contained within. If the plan is substantially updated, [ISP Vendor] must resubmit the information to the Commonwealth of Virginia within 30 days of revision.

Document Revision History

The following table shall be used to track authorship for any changes, modifications, or updates to this document.

Table 0-1: Document Revision History

Version	Date	Description of Change	Author
0.0	11/15/23	Template	Commonwealth of Virginia
1.0	##/##/##	Initial Draft	[Named Authors]

Document Approval History

This document shall be reviewed and updated at least annually or upon significant organizational change. [ISP Vendor] designates the [ISP Vendor] [Document Approvers] as the organizationally defined official(s) to manage the development, documentation, and dissemination of this plan. Their review and approval are required for all changes to this document and shall be tracked in the following table.

Table 0-2: Document Approval History

Version	Date	Documented Approver(s)
1.0	##/##/##	[Responsible Role], [Name of Personnel] [Responsible Role], [Name of Personnel]

Document Dissemination

This Cybersecurity Risk Management Plan shall be stored and disseminated to [ISP Vendor] personnel through [insert technology name] under [Folder Name, if applicable]

Questions, comments, or concerns regarding this document should be directed to [Document Approvers (include contact information)].

Table of Contents

List of Tables

List of Figures

1 DOCUMENT OVERVIEW

1.1 Background

***[INSTRUCTIONS:** This section should include a summary of why cybersecurity risk management is important to the organization. In outlining the need for a robust cybersecurity risk management strategy, this section may include:*

- *a high-level summary of processes/systems/datasets that are critical to business, and why protecting these is important to the organization's mission*
- *stakeholder expectations, dependencies, industry, third-party and/or legal, regulatory and/or contractual requirements relevant to cybersecurity risk management*
- *the impact of an adverse cybersecurity event on business processes, sensitive data, critical systems and/or personnel*
- *how cybersecurity risk management supports the organization's business objectives*

This section should state that because of these factors, the organization has established a Cybersecurity Risk Management Plan, which is outlined in the remainder of this document.

Delete this instruction and all other instructions from your final version of the document.]

[EXAMPLE] This Cybersecurity Risk Management Plan provides definitive information on the prescribed measures used to establish and enforce the cybersecurity risk management program for [ISP Vendor].

[ISP Vendor] is committed to protecting its employees, partners, and customers, from damaging acts that are intentional or unintentional. An effective information security is a team effort involving the participation and support of every [ISP Vendor] user who interacts with data and systems. Therefore, it is the responsibility of every user to know these policies and to conduct their activities accordingly.

Protecting company data and the systems that collect, process, and maintain this information is of critical importance. Consequently, the security of systems must include controls and safeguards to offset threats, as well as controls to ensure accountability, availability, integrity, and confidentiality of the data. Risk management is the process of identifying, evaluating, and addressing threats and vulnerabilities within an organization. Included in the process is implementation of controls to minimize the adverse effect of losses to [ISP Vendor]. Implementing a process of risk evaluation and mitigation strategies reduces the likelihood of incident occurrence, thereby protecting [ISP Vendor] from financial and reputational risk.

[UPDATE]

1.2 Purpose

***[INSTRUCTIONS:** This section should outline the purpose of the Cybersecurity Risk Management Plan, which may reference a desire to mature the organization's security posture, implement a repeatable process to identify and address risk, support enterprise risk management initiatives, and/or mitigate risk to critical business processes. The goal of this section is to establish the risk-based foundation upon which the organization operates and safeguards its data and systems.*

This section should also outline how the organization is implementing and supporting this Cybersecurity Risk Management Plan—i.e., by implementing controls aligned to an industry framework (such as the National Institute of Standards and Technology Cybersecurity Framework [NIST CSF]); documenting

supporting policies, procedures, and standards; socializing cybersecurity best practices and educating personnel at all levels; etc.

Delete this instruction and all other instructions from your final version of the document.]

[EXAMPLE] The purpose of this Cybersecurity Risk Management Plan is to improve the overall security posture, outline the cybersecurity risk management requirements and prescribe a comprehensive framework as follows:

- Create an information security management system (ISMS) based on the ***National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)*** and ***Executive Order 14028: Executive Order on Improving the Nation's Cybersecurity***.
- Protect the confidentiality, integrity, and availability of [ISP Vendor] data and systems.
- Protect [ISP Vendor], its employees, and its clients from illicit use of [ISP Vendor] systems and data.
- Ensure the effectiveness of security controls over data and systems that support [ISP Vendor] operations.
- Recognize the highly networked nature of the current computing environment and provide effective companywide management and oversight of those related information security risks.
- Provide for the development, review, and maintenance of the security controls required to protect [ISP Vendor] data and information systems.

This plan, as well as the related policies, standards, procedures, and guidelines, are necessary to support the management of information risks in daily operations. The development of policies provides due care to ensure that [ISP Vendor] users understand their day-to-day security responsibilities and the threats that could impact the company.

Implementing consistent security controls across the company will help [ISP Vendor] comply with current and future legal obligations to ensure long-term due diligence in protecting the confidentiality, integrity, and availability of [ISP Vendor] data.

[UPDATE]

1.3 Scope

[INSTRUCTIONS: *This section should define the scope of cybersecurity risk management practices across the organization. When drafting this section, consider what would fall under the purview of centralized cybersecurity risk management, including, but not limited to:*

- *Are all datasets in the organization's environment in scope? Or do in-scope datasets only include those created by and/or used by and/or handled by and/or owned by the organization?*
- *Are all systems/resources—both physical and virtual, both organization-owned and personal devices—that touch the organization's network or handle the organization's data in scope?*
- *Do all personnel who perform work for the organization—including any contractors, consultants, and temporary workers—fall under this policy?*
- *Are all locations and entities associated with or managed by the organization subject to these cybersecurity risk management practices?*

*Alternatively, scope can be defined more broadly as **all** personnel, data, systems, activities, assets, resources, and locations that (1) are within the organization's environment; and/or (2) are used for business purposes; and/or (3) are owned or managed by the organization.*

Consider how exceptions or out-of-scope items are handled. Are there any notable out-of-scope exceptions worth calling out in this section—such as sister organizations, subsidiaries, locations, etc.—that are not subject to cybersecurity risk management practices? Alternatively, this section can (1) direct readers to an exceptions policy that outline a process for reviewing and approving items that are not within scope of cybersecurity risk management, and/or (2) allow supporting security policies to carve out exceptions or specify further requirements, as appropriate, and/or (3) allow certain groups/departments to create more restrictive policies/procedures/standards that apply to a subset of the organization, as long as they comply with the general requirements of this Cybersecurity Risk Management Plan.

Delete this instruction and all other instructions from your final version of the document.]

[EXAMPLE] This document applies to all ISP Vendor] data, systems, activities, and assets owned, leased, controlled, or used by [ISP Vendor], its agents, contractors or other business partners on behalf of [ISP Vendor]. This plan further applies to all personnel, consultants, contractors, temporary workers, and any users of internal systems who access, store, process, or transmit non-public information. Systems include physical and virtual technology and services such as computing devices, servers, network devices, and applications.

Some requirements apply specifically to persons with a specific job function (e.g., a system administrator); otherwise, all personnel supporting [ISP Vendor] business functions shall comply with the policies. Cybersecurity Risk Management Plan departments shall use these requirements or may create a more restrictive policy, but none that are less restrictive, less comprehensive, or less compliant than these requirements.

This plan does not supersede any other applicable law or higher-level company directive or existing labor management agreement in effect.

A range of security training measures must be undertaken to achieve widespread compliance with various information security obligations. The details of specific requirements may vary from this policy based on various security and compliance obligations that pertain specifically to [ISP Vendor]. All corporate standards are considered baseline requirements and may be superseded by any system-specific standards as needed so long as the corporate requirements are met.

[UPDATE]

1.4 Roles & Responsibilities

***[INSTRUCTIONS**: This section should define roles (either titles, individuals, teams, or groups) related to responsibilities outlined in this document to ensure adequate resources are allocated in alignment with the cybersecurity risk strategy. This should include:*

- *Ownership of the Cybersecurity Risk Management program*
- *Implementation/deployment of controls related to Cybersecurity Risk Management*
- *Assessment of the Cybersecurity Risk Management program*
- *Reporting/tracking of the Cybersecurity Risk Management program*
- *Lines of communication across the organization for tracking risks, including risks from suppliers and/or other third-parties*

- *Executive oversight of the Cybersecurity Risk Management program*
- *Training and educating users on the Cybersecurity Risk Management program*

Delete this instruction and all other instructions from your final version of the document.]

[EXAMPLE]

ISP Vendor Position	Responsibilities
Named Owner, Chief Information Security Officer OR Position Title	Ownership of the Cybersecurity Risk Management program (defining, documenting, managing, updating, and disseminating a Cybersecurity Risk Management program)
IT Director OR Position Title	Implementation/deployment of controls related to Cybersecurity Risk Management
Audit Committee OR Position Title	Assessment of the Cybersecurity Risk Management program
Security Director OR Position Title	Reporting/tracking of the Cybersecurity Risk Management program
Executive Team OR Position Title	Executive oversight of the Cybersecurity Risk Management program
Security Manager OR Position Title	Training and educating users on the Cybersecurity Risk Management program

1.5 Management Commitment & Program Status

***[INSTRUCTIONS:** This section should outline leadership's commitment to cybersecurity risk management to establish accountability at the executive level.*

Delete this instruction and all other instructions from your final version of the document.]

[EXAMPLE] The [ISP Vendor] **Executive Team** recognizes the importance of Cybersecurity Risk Management and has authorized [Document Approvers] to define, document, and disseminate a Cybersecurity Risk Management program that accomplishes this mission.

[UPDATE]

[EXAMPLE] [ISP Vendor] is committed to the importance of operationalizing the defined Cybersecurity Risk Management Plan. As such, [ISP Vendor] [has/has not] fully implemented the Cybersecurity Risk Management Plan as defined in this document. **[If ISP Vendor has not fully implemented the plan, add]** The following areas are pending operationalization and are schedule for full implementation by the timelines listed:

- **[UPDATE]**

1.6 Coordination Among Organizational Entities

***[INSTRUCTIONS**: This section should demonstrate that this Cybersecurity Risk Management Plan is supported and deployed consistently at all levels of the organization. As the organization works to achieve the Cybersecurity Risk Management Plan's objectives, effective coordination fosters consistency and helps avoid duplication of efforts. This can be exhibited by the formation of committees with representation from various departments/teams; coordination of risk management efforts between key stakeholders; and/or alignment between various policies, procedures, and standards.*

Delete this instruction and all other instructions from your final version of the document.]

[EXAMPLE] [ISP Vendor] recognizes the importance of organizational coordination. This document contains references and coordination with the following policies, standards, procedures, departments, committees, and teams.

- [ISP Vendor] Cybersecurity Governance Committee
- List of Named [ISP Vendor] Departments/Teams
- [ISP Vendor] Supporting Policies
- [ISP Vendor] Supporting Standards
- [ISP Vendor] Supporting Procedures

[UPDATE]

1.7 Compliance

***[INSTRUCTIONS**: This section should affirm the expectation of compliance with this Plan, along with any disciplinary action that may be pursued due to noncompliance. It is recommended to have HR/legal teams review this section to ensure it aligns with relevant HR policies.*

This section can also contain a reference to (or a summary of) the exceptions process. This process would provide a structure for handling any system, activity, process, entity, or control that does not comply with the requirements of this Plan. The exceptions process should include steps for documenting, submitting, reviewing, and approving exceptions, along with plans for mitigating risks associated with the exception.

Delete this instruction and all other instructions from your final version of the document.]

[EXAMPLE] Any [ISP Vendor] user found to have violated any policy, standard or procedure may be subject to disciplinary action, up to and including termination of employment. Violators of local, state, federal and/or international law may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

1.7.1 Exceptions

While every exception to a standard potentially weakens protection mechanisms for [ISP Vendor] information systems and underlying data, occasionally exceptions will exist. Information security considerations such as regulatory, compliance, confidentiality, integrity, and availability requirements are most easily met when all users employ centrally supported or recommended standards. [ISP Vendor] understands that centrally supported or recommended technologies are not always feasible for a specific system or team. Deviation from centrally supported or recommended technologies is discouraged. However, it may be considered provided that the alternative presents a reasonable, justifiable business, or research case for an information security policy exception; resources are sufficient to properly

implement and maintain the alternative technology; the process outlined in this document and other related documents is followed and other policies and standards are upheld.

An exception may be granted by the [Authorized Persons], or their designee, for non-compliance with a policy or standard resulting from:

- Temporary exception, where immediate compliance would disrupt critical operations.
- Implementation of a solution with equivalent or superior protection to the requirements in the policy or standard.
- Impending retirement of a system.
- Inability to implement the policy or standard due to some limitations (i.e., technical constraint, business limitation or statutory requirement).
- Compliance would cause a major adverse financial impact that would not be offset by the reduced risk occasioned by compliance (i.e., the cost to comply offsets the risk of non-compliance)

Exceptions are reviewed for validity on a case-by-case basis and their approval is not automatic. Exceptions that are granted will be for a specific time-period, not to exceed one year. Upon expiration of the exception, an extension of the exception may be requested, if it is still required.

2 CYBERSECURITY RISK MANAGEMENT OVERVIEW

***[INSTRUCTIONS**: This section should summarize the organization's understanding of Cybersecurity Risk Management, along with a high-level overview of the primary components of the organization's Cybersecurity Risk Management strategy (further details of each component of the strategy can be described in Section 3: Standards). If applicable, this section should also reference the framework by which the organization structures and aligns its Cybersecurity Risk Management strategy and why this framework was chosen. The example text used in this template includes references to the NIST Risk Management Framework (RMF) defined within NIST 800-37 as a mechanism to help guide organizations with a structured identification, prioritization, response, and monitoring of risks. However, it is not required that these steps be explicitly followed, and these can be tailored to meet the needs of each organization.*

Delete this instruction and all other instructions from your final version of the document.]

[EXAMPLE] Cybersecurity risk management is the program and supporting processes to manage risk to business operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time. A cybersecurity risk management strategy addresses how organizations intend to assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions.

[ISP Vendor] leverages key components of the ***(optional)*** ***NIST Special Publication 800-37 (Rev. 2): Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*** to define, document, disseminate a risk management program that meets compliance requirements for ***NIST Cybersecurity Framework (CSF)*** and ***Executive Order 14028: Executive Order on Improving the Nation's Cybersecurity***.

*[**INSTRUCTIONS**: More information on these documents, additional guidance can be found here:*

- *NIST RMF: https://csrc.nist.gov/projects/risk-management/about-rmf*
- *NIST CSF: https://www.nist.gov/cyberframework*
- *Executive Order 14028: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/*

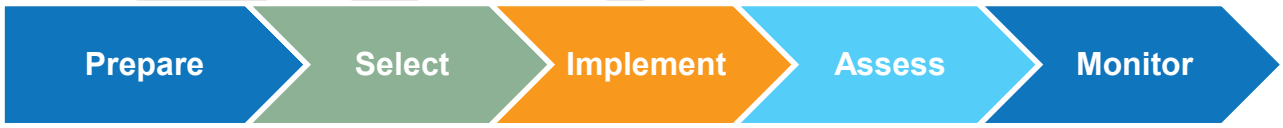
Delete this instruction and all other instructions from your final version of the document.]

[**Update based on framework chosen, as applicable**] As defined by NIST, there are seven steps in the RMF: a preparatory step to ensure that organizations are ready to execute the process and six main steps. While all seven steps are essential for the successful execution of the RMF, this plan focuses on five selected components of these steps which include:

- **Prepare** to execute the RMF from an organization- and a system-level perspective by establishing a context and priorities for managing security and privacy risk.
- **Select** an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk.
- **Implement** the controls and describe how the controls are employed within the system and its environment of operation.
- **Assess** the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.
- **Monitor** the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting standards.

Appendix A includes a full RMF task list, which can be used as a reference for consideration on necessary steps to support the Cybersecurity Risk Management Plan.

Figure 2-1: Modified NIST RMF Model



3 CYBERSECURITY RISK MANAGEMENT PLAN

The information included in this section outlines the [ISP Vendor]'s plans to establish and operate a cybersecurity risk management program.

*[**INSTRUCTIONS**: This section should detail how the organization has implemented each component of the Cybersecurity Risk Management strategy throughout its environment. As such, this section should expand on Section 2: Cybersecurity Risk Management Overview and provide further detail of how the organization is achieving the objectives of each component of the organization's Cybersecurity Risk Management Strategy. Note: This template uses the NIST Risk Management Framework (RMF) as an example by which to articulate a cybersecurity risk management strategy. Sub-sections on the following pages align with components of the RMF (see Appendix A for specific tasks associated with the RMF).*

Alignment to the RMF is optional; thus, the RMF only serves as a potential framework to structure an organization's cybersecurity risk management strategies.

Delete this instruction and all other instructions from your final version of the document.]

3.1 Prepare

[INSTRUCTIONS: Update the table below with implementation status of controls in this section.]

Table 3-1: Prepare Implementation Summary

Prepare Implementation Summary	
Implementation Status (check all that apply):	**Responsible Role:**
☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative Implementation ☐ Not Applicable	[Named Role(s)] **Instruction:** Ensure this role matches roles defined earlier in the plan
If not implemented, what is the implementation plan?	**Planned Date for Full Implementation:**
[If applicable, insert text or replace with "N/A"]	DD Month YYYY

The purpose of the ***Prepare*** step is to conduct essential activities at the organization, mission and business process, and information system levels of the organization to help prepare the organization to manage its security and privacy risks using the ***Risk Management Framework***.

[INSTRUCTIONS: *This section describes the organization's approach to meeting the objectives of the* ***Prepare*** *step. The activities in the Prepare step are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.*

Sub-sections should detail the control objectives that demonstrate how the organization understands its IT environment (hardware, software, external systems—prioritized based on criticality and business value), how the organization has defined an operating and reporting structure, and how these elements serve as a foundation to Cybersecurity Risk Management. Sub-sections should be used to identify and understand the business requirements, system requirements, and personnel who can support the Plan. This can include how the organization will:

- *Track regulatory, industry and third-party requirements relevant to Cybersecurity Risk Management*
- *Identify, classify, track, and protect critical assets, systems, data, and business processes that support the organization's mission.*
- *Maintain an inventory of data and corresponding metadata for designated data types.*
- *Identify and understand the business requirements, technical requirements, and security/privacy requirements for each system and business process.*
- *Identify and classify strategic opportunities (i.e., positive risks)*
- *Identify stakeholders who design, development, implementation, assessment, operation, maintenance, or disposal of systems.*
- *Maintain cybersecurity risk management policies and procedures that are consistent with applicable laws, executive orders, directives, regulations, policies, standards and guidelines.*

For more information on content that can be included in this section:

- *Specific tasks associated with the Prepare step can be found in Appendix A.*
- *Additional Guidance for the Prepare step can be found here: https://csrc.nist.gov/Projects/risk-management/about-rmf/prepare-step*
- *The RMF Quick Start Guide (QSG): Prepare Step FAQs can be found here: https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/01-Prepare%20Step/NIST%20RMF%20Prepare%20Step-FAQs.pdf*

Delete this instruction and all other instructions from your final version of the document.]

[UPDATE]

3.2 Select

[INSTRUCTIONS: Update the table below with implementation status of controls in this section.]

Table 3-2: Select Implementation Summary

Select Implementation Summary			
Implementation Status (check all that apply):		**Responsible Role:**	
☐ Implemented ☐ Partially Implemented ☐ Planned	☐ Alternative Implementation ☐ Not Applicable	[Named Role(s)] **Instruction:** Ensure this role matches roles defined earlier in the plan	
If not implemented, what is the implementation plan?			**Planned Date for Full Implementation:**
[If applicable, insert text or replace with "N/A"]			DD Month YYYY

The purpose of the ***Select*** step is to select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the Nation.

Control baselines are predefined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. Controls are chosen for baselines to either satisfy mandates imposed by laws, executive orders, directives, regulations, policies, standards, and guidelines or address threats common to all users of the baseline under the assumptions specific to the baseline. Baselines represent a starting point for the protection of individuals' privacy, information, and information systems with subsequent tailoring actions to manage risk in accordance with mission, business, or other constraints.

Once the control baselines are selected and tailored, [ISP Vendor] should develop and implement a system level strategy for monitoring control effectiveness that is consistent with and supplements the organizational continuous monitoring strategy.

***[INSTRUCTIONS:** This section describes the organization's approach to meeting the objectives of the **Select** step. Sub-sections should detail how the organization selects, tailors, and allocates cybersecurity controls that are commensurate with the organization's risk tolerance. Sub-sections should also outline how the organization plans to document controls (such as in security and privacy plans), as well as how those controls will be reviewed and approved.*

The selection of a control baseline is determined by the needs of subgrantee stakeholders. Stakeholder needs consider mission and business requirements as well as mandates imposed by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. For example, the control baselines in SP 800-53B are based on the requirements from FISMA and PRIVACT.

For more information on content that can be included in this section:

- *Specific tasks associated with the Select step can be found in Appendix A.*
- *Additional Guidance for the Select step can be found here: https://csrc.nist.gov/Projects/risk-management/about-rmf/select-step*
- *The RMF Quick Start Guide (QSG): Select Step FAQs can be found here: https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/03-Select%20Step/NIST%20RMF%20Select%20Step-FAQs.pdf*
- *When selecting controls, BEAD requests alignment with the following control frameworks:*
  - *NIST 800-161: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*
  - *Key practices discussed in NISTIR 8276, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*
  - *NIST CSF (additional Guidance on NIST CSF can be found here: https://www.nist.gov/cyberframework*
  - *Standards set forth in Executive Order 14028*
- *The following control baselines may be used in addition to NIST CSF to tailor the controls to the organizational needs:*

Table 3-3: Additional Control Baselines for Tailoring

Source	Baseline	Link
Federal	*NIST SP 800-53B*	*https://csrc.nist.gov/pubs/sp/800/53/b/upd1/final*
Department of Defense	*NIST SP 800-171*	*https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final*
Payment Card Industry Data Security Standard (PCI DSS)	*PCI-DSS*	*https://www.pcisecuritystandards.org/document_library/*
International Standards	*ISO 27001*	*https://www.iso.org/standard/27001*

Delete this instruction and all other instructions from your final version of the document.]

[Update]

3.3 Implement

[INSTRUCTIONS: Update the table below with implementation status of controls in this section.]

Table 3-4: Implement Implementation Summary

Implement Implementation Summary		
Implementation Status (check all that apply):		**Responsible Role:**
☐ Implemented	☐ Alternative Implementation	[Named Role(s)]

☐ Partially Implemented ☐ Not Applicable ☐ Planned	**Instruction:** Ensure this role matches roles defined earlier in the plan
If not implemented, what is the implementation plan?	**Planned Date for Full Implementation:**
[If applicable, insert text or replace with "N/A"]	DD Month YYYY

The purpose of the ***Implement*** step is to implement the controls in the security and privacy plans for the system and for the organization and to document in a baseline configuration, the specific details of the control implementation.

[INSTRUCTIONS: *This section describes the organization's approach to meeting the objectives of the* ***Implement*** *step. The focus of this step is to show how the organization will:*

- *Deploy controls that support Cybersecurity Risk Management, including implementing the security and privacy plans and documenting changes to planned control implementations based on "as-implemented" state of controls.*
- *Document changes to the security/privacy plan and planned implementation of controls.*
- *Empower the workforce to implement, manage, and comply with controls.*

For more information on content that can be included in this section:

- *Specific tasks associated with the Implement step can be found in Appendix A.*
- *Additional Guidance for the Implement step can be found here:* https://csrc.nist.gov/Projects/risk-management/about-rmf/implement-step
- *The RMF Quick Start Guide (QSG): Implement Step FAQs can be found here:* https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/04-Implement%20Step/NIST%20RMF%20Implement%20Step-FAQs.pdf

Delete this instruction and all other instructions from your final version of the document.]

[Update]

3.4 Assess

[INSTRUCTIONS: Update the table below with implementation status of controls in this section.]

Table 3-5: Assess Implementation Summary

Assess Implementation Summary	
Implementation Status (check all that apply):	**Responsible Role:**
☐ Implemented ☐ Alternative Implementation ☐ Partially Implemented ☐ Not Applicable ☐ Planned	[Named Role(s)] **Instruction:** Ensure this role matches roles defined earlier in the plan
If not implemented, what is the implementation plan?	**Planned Date for Full Implementation:**
[If applicable, insert text or replace with "N/A"]	DD Month YYYY

The purpose of the ***Assess*** step is to determine if the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization.

Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation. Risk assessments also consider risk from external parties, including contractors who operate systems on behalf of the organization, individuals who access organizational systems, service providers, and outsourcing entities.

***[INSTRUCTIONS:** This section describes the organization's approach to meeting the objectives of the **Assess** step. Key elements of the Assess step include explaining how the organization will:*

- *Determine if cybersecurity controls have been implemented correctly, are operating as intended, and producing desired outcomes.*
- *Establish a risk management strategy and risk tolerance/appetite.*
- *Assess risk and define the frequency of risk assessments.*
- *Identify vulnerabilities within the environment.*
- *Identify, track, and document threats to the organization.*
- *The Plan outlines how the organization will determine the impact and likelihood of threats, vulnerabilities, risks, and adverse events.*
- *Select a team (which can maintain an appropriate level of independence) to conduct controls assessments and risk assessments.*
- *Track risks, including risk severity, risk owner, risk status, risk response, and mitigation plans (e.g., risk register).*
- *Document results from assessments of controls.*
- *Update cybersecurity controls to reflect recommendations.*
- *Develop a plan of action and milestones detailing remediation plans for unacceptable risks.*

For more information on content that can be included in this section:

- *Specific tasks associated with the Assess step can be found in Appendix A.*
- *Additional Guidance for the Assess step can be found here:* https://csrc.nist.gov/Projects/risk-management/about-rmf/assess-step
- *The RMF Quick Start Guide (QSG): Assess Step FAQs can be found here:* https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/05-Assess%20Step/NIST%20RMF%20Assess%20Step-FAQs.pdf

Delete this instruction and all other instructions from your final version of the document.]

[Update]

3.5 Monitor

[INSTRUCTIONS: Update the table below with implementation status of controls in this section.]

Table 3-6: Monitor Implementation Summary

Monitor Implementation Summary			
Implementation Status (check all that apply):		**Responsible Role:**	
☐ Implemented ☐ Partially Implemented ☐ Planned	☐ Alternative Implementation ☐ Not Applicable	[Named Role(s)] **Instruction:** Ensure this role matches roles defined earlier in the plan	
If not implemented, what is the implementation plan?			**Planned Date for Full Implementation:**
[If applicable, insert text or replace with "N/A"]			DD Month YYYY

The purpose of the ***Monitor*** step is to maintain an ongoing situational awareness about the security and privacy posture of the information system and the organization in support of risk management decisions. Cybersecurity risk management strategy outcomes should be reviewed to inform and adjust strategy and direction, as needed to ensure coverage of organizational requirements and risks. Organizational cybersecurity risk management performance should be evaluated, reviewed and adjusted as needed.

[INSTRUCTIONS: *This section describes the organization's approach to meeting the objectives of the* ***Monitor*** *step. The Monitor step may include a description of how the organization will:*

- *Monitor information systems and the organization's operational environment in accordance with a continuous monitoring strategy.*
- *Assess control effectiveness on an ongoing basis.*
- *Analyze and responds to the output of continuous monitoring activities.*
- *Update cybersecurity risk management documents based on output from continuous monitoring activities.*
- *Evaluate organizational cybersecurity risk management performance.*
- *Report the organization's security and privacy posture to the authorizing official, senior leaders, and executives.*
- *Maintain a process for authorizing officials to conduct ongoing authorizations (using the results of continuous monitoring activities) and communicate changes in risk determination and acceptance decisions.*
- *Develop and implement an asset management strategy that monitors assets throughout their lifecycle.*

For more information on content that can be included in this section:

- *Specific tasks associated with the Monitor step can be found in Appendix A.*
- *Additional Guidance for the Monitor step can be found here: https://csrc.nist.gov/Projects/risk-management/about-rmf/monitor-step*
- *The RMF Quick Start Guide (QSG): Monitor Step FAQs can be found here:* https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/07-Monitor%20Step/NIST%20RMF%20Monitor%20Step-FAQs.pdf

Delete this instruction and all other instructions from your final version of the document.]

[Update]

.

4 KEY TERMINOLOGY

***[Instructions:** This section includes definitions for key terminology that are referenced in previous sections of this document. Review and adjust terms and definitions, as necessary.]*

In the realm of IT security terminology, the NIST, IR 7298, Revision 1, "Glossary of Key Information Security Terms" and NIST SP 800-30 Revision 1, "Guide for Conducting Risk Assessments", are the primary reference documents that [ISP Vendor] uses to define common IT security terms. The key terminology to be aware of includes the following:

Table 4-1: Key Terminology Definitions

Term	Definition
Control	This is a term describing any management, operational or technical method that is used to manage risk. Controls are designed to monitor and measure specific aspects of standards to help [ISP Vendor] accomplish stated goals or objectives. All controls map to standards, but not all standards map to controls.
Control Assessment	The testing and/or evaluation of the management, operational, and technical security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.
Control Objective	This is a term describing targets or desired conditions to be met that are designed to ensure that policy intent is met. Where applicable, control objectives are linked to an industry-recognized leading practice to align [ISP Vendor] with accepted due care requirements.
Data	This is a term describing an information resource that is maintained in electronic or digital format. Data may be accessed, searched, or retrieved via electronic networks or other electronic data processing technologies provides guidance on data classification and handling restrictions.
Data Owner	This is a term describing a person or entity that has been given formal responsibility for the security of an asset, asset category or the data hosted on the asset. It does not mean that the asset belongs to the owner in a legal sense. Asset owners are formally responsible for making sure that assets are secure while they are being developed, produced, maintained, and used.
Guidelines	This is a term describing recommended practices that are based on industry-recognized leading practices. Unlike standards, guidelines allow users to apply discretion or leeway in their interpretation, implementation, or use.

Term	Definition
Impact	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability
Information Security	This is a term that covers the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. The focus is on the confidentiality, integrity, and availability (CIA) of data.
Likelihood	A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.
Policy	This is a term describing a formally established requirement to guide decisions and achieve rational outcomes. A policy is a statement of expectation that is enforced by standards and further implemented by procedures.
Procedure	This is a term describing an established or official way of doing something, based on a series of actions conducted in a certain order or manner. Procedures are the responsibility of the asset custodian to build and maintain, in support of standards and policies.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Assessment	The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.
Risk Management	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time

Term	Definition
Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.
Risk Response	Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.
Sensitive Data	This is a term that covers categories of data that must be kept secure. Examples of sensitive data includes PII, electronic protected health information (ePHI) and all other forms of data classified as restricted or confidential in nature.
Sensitive Personally Identifiable Information (sPII):	This is a term that is commonly defined as the first name or first initial and last name, in combination with any one or more of the following data elements: • Social Security number (SSN)/Taxpayer Identification Number (TIN)/National Identification Number (NIN) • Driver license (DL) or other government-issued identification number (e.g., passport, permanent resident card) • Financial account number • Payment card number (e.g., credit or debit card)
Standard	This is a term describing formally established requirements regarding processes, actions, and configurations.
System	This is a term describing an asset; an information system or network that can be defined, scoped, and managed. These include, but are not limited to, computers, workstations, laptops, servers, routers, switches, firewalls, and mobile devices.
Target Audience	This is a term describing the intended group for which a control or standard is directed.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Term	Definition
Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

APPENDIX A: COMPLETE RMF TASK LIST

The following table is the complete RMF task list as published by NIST. This can be used as a reference for consideration on necessary steps to support the Cybersecurity Risk Management Plan. The full text of NIST SP 800-37 Rev. 2 can be found here: https://csrc.nist.gov/projects/risk-management , https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

Table A-1: Complete NIST RMF Task List

NIST RMF Prepare Tasks		
Task ID	**Task Name**	**Task Description**
P-1	Risk Management Roles	Identify and assign individuals to specific roles associated with security and privacy risk management.
P-2	Risk Management Strategy	Establish a risk management strategy for the organization that includes a determination of risk tolerance.
P-3	Risk Assessment—Organization	Assess organization-wide security and privacy risk and update the risk assessment results on an ongoing basis.
P-4	Organizationally Tailored Control Baselines and Cybersecurity Framework Profiles (Optional)	Establish, document, and publish organizationally tailored control baselines and/or Cybersecurity Framework Profiles
P-5	Common Control Identification	Identify, document, and publish organization-wide common controls that are available for inheritance by organizational systems.
P-6	Impact-Level Prioritization (Optional)	Prioritize organizational systems with the same impact level
P-7	Continuous Monitoring Strategy—Organization	Develop and implement an organization-wide strategy for continuously monitoring control effectiveness.
P-8	Mission or Business Focus	Identify the missions, business functions, and mission/business processes that the system is intended to support.
P-9	System Stakeholders	Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system.
P-10	Asset Identification	Identify assets that require protection.
P-11	Authorization Boundary	Determine the authorization boundary of the system.
P-12	Information Types	Identify the types of information to be processed, stored, and transmitted by the system.
P-13	Information Life Cycle	Identify and understand all stages of the information life cycle for each information type processed, stored, or transmitted by the system.
P-13	Information Life Cycle	Identify and understand all stages of the information life cycle for each information type processed, stored, or transmitted by the system.
P-14	Risk Assessment—System	Conduct a system-level risk assessment and update the risk assessment results on an ongoing basis.

NIST RMF Prepare Tasks		
Task ID	**Task Name**	**Task Description**
P-15	Requirements Definition	Define the security and privacy requirements for the system and the environment of operation.
P-16	Enterprise Architecture	Determine the placement of the system within the enterprise architecture.
P-17	Requirements Allocation	Allocate security and privacy requirements to the system and to the environment of operation.
P-18	System Registration	Register the system with organizational program or management offices.

NIST RMF Categorize Tasks		
Task ID	**Task Name**	**Task Description**
C-1	System Description	Document the characteristics of the system.
C-2	Security Categorization	Categorize the system and document the security categorization results.
C-3	Security Categorization Review and Approval	Review and approve the security categorization results and decision.

NIST RMF Select Tasks		
Task ID	**Task Name**	**Task Description**
S-1	Control Selection	Select the controls for the system and the environment of operation.
S-2	Control Tailoring	Tailor the controls selected for the system and the environment of operation.
S-3	Control Allocation	Allocate security and privacy controls to the system and to the environment of operation.
S-4	Documentation of Planned Control Implementations	Document the controls for the system and environment of operation in security and privacy plans.
S-5	Continuous Monitoring Strategy— System	Develop and implement a system-level strategy for monitoring control effectiveness that is consistent with and supplements the organizational continuous monitoring strategy.
S-6	Plan Review and Approval	Review and approve the security and privacy plans for the system and the environment of operation.

NIST RMF Implement Tasks		
Task ID	**Task Name**	**Task Description**
I-1	Control Implementation	Implement the controls in the security and privacy plans.

NIST RMF Implement Tasks		
Task ID	**Task Name**	**Task Description**
I-2	Update Control Implementation Information	Document changes to planned control implementations based on the “as-implemented” state of controls.

NIST RMF Assess Tasks		
Task ID	**Task Name**	**Task Description**
A-1	Assessor Selection	Select the appropriate assessor or assessment team for the type of control assessment to be conducted.
A-2	Assessment Plan	Develop, review, and approve plans to assess implemented controls.
A-3	Control Assessments	Assess the controls in accordance with the assessment procedures described in assessment plans.
A-4	Assessment Reports	Prepare the assessment reports documenting the findings and recommendations from the control assessments.
A-5	Remediation Actions	Conduct initial remediation actions on the controls and reassess remediated controls
A-6	Plan of Action and Milestones	Prepare the plan of action and milestones based on the findings and recommendations of the assessment reports.

NIST RMF Authorize Tasks		
Task ID	**Task Name**	**Task Description**
R-1	Authorization Package	Assemble the authorization package and submit the package to the authorizing official for an authorization decision.
R-2	Risk Analysis and Determination	Analyze and determine the risk from the operation or use of the system or the provision of common controls.
R-3	Risk Response	Identify and implement a preferred course of action in response to the risk determined.
R-4	Authorization Decision	Determine if the risk from the operation or use of the information system or the provision or use of common controls is acceptable
R-5	Authorization Reporting	Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk.
R-1	Authorization Package	Assemble the authorization package and submit the package to the authorizing official for an authorization decision.

NIST RMF Monitor Tasks		
Task ID	**Task Name**	**Task Description**
M-1	*System and Environment Changes*	*Monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system.*
M-2	*Ongoing Assessments*	*Assess the controls implemented within and inherited by the system in accordance with the continuous monitoring strategy.*
M-3	*Ongoing Risk Response*	*Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones*
M-4	*Authorization Package Updates*	*Update plans, assessment reports, and plans of action and milestones based on the results of the continuous monitoring process.*
M-5	*Security and Privacy Reporting*	*Report the security and privacy posture of the system to the authorizing official and other organizational officials on an ongoing basis in accordance with the organizational continuous monitoring strategy.*
M-6	*Ongoing Authorization*	*Review the security and privacy posture of the system on an ongoing basis to determine whether the risk remains acceptable.*
M-7	*System Disposal*	*Implement a system disposal strategy and execute required actions when a system is removed from operation.*