CYBER TOOLKIT EXECUTIVE SUMMARY

We are extremely proud to share the Bay Area UASI Cyber Toolkit, developed in conjunction with the Northern California Regional Intelligence Center (NCRIC).

As the Nation becomes increasingly reliant on information technology, cyber incidents are occurring more frequently and have the potential to cause widespread damage. Malicious cyber actors—including nation states and cyber criminals—grow more sophisticated and difficult to detect by the day. These actors exploit vulnerabilities in information technology (IT) systems and infrastructure to steal data, disrupt essential services, and ransom money.

Cyber incidents can result in significant downtime and prevent organizations from providing critical community services. Moreover, a cyber incident can jeopardize the privacy of your employees, partners, and the public, severely diminishing community trust in your department or agency. Given the potential negative consequences, organizations must be prepared to act swiftly and effectively in response to an actual or suspected cyber incident. The Bay Area UASI seeks to provide entities across the region with the tools and support they need to strengthen their cybersecurity planning and enhance their resilience.

To achieve these goals, the Bay Area UASI has engaged in region-wide cyber planning efforts through its **Cybersecurity Incident Response Framework Planning Project**. The Bay Area UASI and NCRIC have collaborated with the Cyber Resilience Work Group to develop and conduct a region-wide cybersecurity preparedness survey and cyber plan review. These efforts informed the 2020 Bay Area UASI Cybersecurity Preparedness Workshop, where stakeholders in information technology and emergency management roles across government, regional, non-profit, and private sector entities discussed their cyber planning needs. The Cyber Toolkit is designed to address priorities determined throughout this project.

The Cyber Toolkit includes templates and other resources created to assist localities in strengthening their cyber incident response and recovery planning. Having a robust and actionable **Cyber Incident Response Plan** and **Technology Recovery Plan** will help ensure that organizations can effectively manage cyber incidents and limit or eliminate their impacts. Whether a breach is large or small, it is vital that organizations actively engage in cyber planning and have established plans in place. This will enable organizations to successfully respond to and recover from cyber incidents while mitigating the risk of being a victim of a future incident.

The Bay Area UASI and NCRIC are committed to building and sustaining cyber preparedness across the region and will continue to prioritize support to help communities respond to and recover from cyber incidents.

Sincerely,

Mikyung Kim-Molina
Bay Area UASI Regional Project Manager

Alison Yakabe
NCRIC Cyber Security Team Lead Analyst

Purpose

The Bay Area UASI has developed a Cyber Toolkit to assist organizations/jurisdictions with cyber planning, including several resources that can be used to increase cyber incident preparedness and response. The Cyber Toolkit includes this Executive Summary, a Technology Recovery Plan (TRP) template, a Cyber Incident Response Plan (CIRP) template, and a document that outlines all components of the National Institute of Standards and Technology (NIST) Framework Core Structure (**Table 1**).

Your organization/jurisdiction can use these resources to facilitate cyber planning, working with parties to customize with specific information relevant to your entity. These resources are designed to help you develop your own cyber plans that enable your organization/jurisdiction to quickly identify, respond to, and recover from cyber incidents.

Table 1: Contents of the Cyber Toolkit

Resource	Purpose
Cyber Toolkit Executive Summary	Highlights the contents of the Cyber Toolkit and indicates relationships between documents and planning elements
TRP Template	Identifies priorities, strategies, and resources that your organization/jurisdiction can use when recovering from cyber incidents
CIRP Template	Provides the guidance and structure needed to develop a clear and actionable plan for your organization/jurisdiction to implement quickly in response to an actual or suspected cyber incident
NIST Framework Core Structure	Outlines the functions, categories, and subcategories that comprise the NIST Framework Core, which is introduced and described in the Bay Area Regional Cyber Incident Response Framework

Overview of Technology Recovery Plan Template

The TRP serves as the guide to quickly redirect available resources towards information technology systems recovery and restoration. Using the TRP template, your organization/jurisdiction can identify recovery priorities and procedures that should be utilized in the aftermath of a cyber incident and a communication plan for internal and external stakeholders. The TRP also enables the efficient recovery of critical systems and helps your jurisdiction/organization avoid further damage or disruption to critical business functions. Executing this plan will minimize recovery time and possible delays, improve security, and mitigate potentially damaging impacts caused by taking action without a clearly defined and tested plan.

Figure 1: Technology Recovery Plan

Overview of Cyber Incident Response Plan Template

An established and tested CIRP is vital to ensuring that an organization/jurisdiction is able to respond quickly and effectively to a cyber incident. A CIRP provides the guidance and direction required to effectively assess and respond to any type of cyber incident, including malware, ransomware, or a distributed denial of service (DDoS) attack, among many others. When a cyber incident occurs, it is critical to have a plan in place that describes the specific actions and procedures the organization/jurisdiction should perform. This can be the difference between a minor incident with limited to no damage and an incident that severely impacts your organization/jurisdiction's ability to operate. The

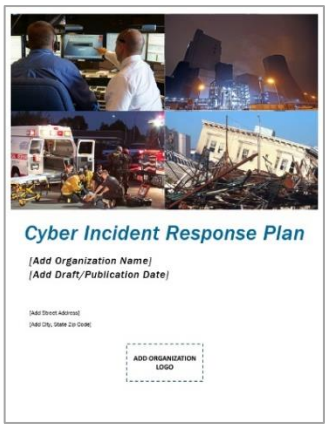

Figure 2: Cyber Incident Response Plan

CIRP template will provide the guidance and structure needed to develop an actionable plan to implement during a cyber incident, including a clear strategy for information sharing. This will help minimize damage, reduce disaster response times, and mitigate breach-related expenses.

Relationship Between the CIRP and TRP

While the CIRP and the TRP are both cyber plans, they serve different purposes. The purpose of a CIRP is to protect sensitive data and systems during an incident. A TRP helps to ensure that an organization/jurisdiction's information technology systems can be restored following an incident to allow it to perform its critical functions.

A CIRP describes the range of actions that must be taken during an incident. It defines an incident response team's roles and responsibilities to ensure that the incident response processes are executed effectively and quickly. A TRP, however, focuses on bringing an organization's information technology systems and infrastructure back to an operational state and successfully recovering from any impacts caused by the incident. Moreover, while the CIRP primarily contains the tactical-level actions that must be taken for a specific incident to address the immediate threat, the TRP contains more strategic-level guidance on the priorities, policies, and procedures required to recovery effectively and prevent a similar event from happening in the future.

The CIRP and TRP are two essential components of a cyber incident preparedness strategy**. Ideally, the two plans will be developed, deployed, and tested together.**

Relationships Between COOP and Cyber Planning

There is a direct relationship between cyber planning through the TRP/CIRP and Continuity of Operations (COOP) planning. COOP planning consists of three main components: the **business process analysis (BPA)**, **business impact analysis (BIA)**, and the final **COOP Plan**.

Through a BPA, an organization identifies the functional processes, activities, personnel expertise, systems, data, interdependencies, alternate locations, and other Essential Assets (EAs) needed to perform their Essential Functions (EFs). An organization then uses a BIA to identify and prioritize those EAs/EFs and determine impacts if those EAs/EFs are disrupted. The data collected and analyzed in the BPA and BIA allows for the application of organization-wide risk analysis to contribute to sound decision making and strengthens operations through effective risk management. The COOP Plan then builds on the BIA, outlining in more detail how an organization will restore its EFs at an alternate site and perform those until they are able to return to normal operations.

A TRP may support a COOP Plan by recovering supporting systems for mission/business processes or EFs. The EAs and EFs identified through COOP planning will directly influence your organization/jurisdiction's

recovery priorities and overall recovery strategy (Error! Reference source not found.) If your organization/jurisdiction has a COOP Plan (or a BIA/BPA) already developed, you should ensure that it informs TRP development. If you do not have a COOP Plan, you can still begin cyber planning with the TRP/CIRP templates using the prompts throughout the documents. For more information on COOP planning and associated tools and templates, please see the Bay Area UASI's COOP/Continuity of Government (COG) Toolkit.

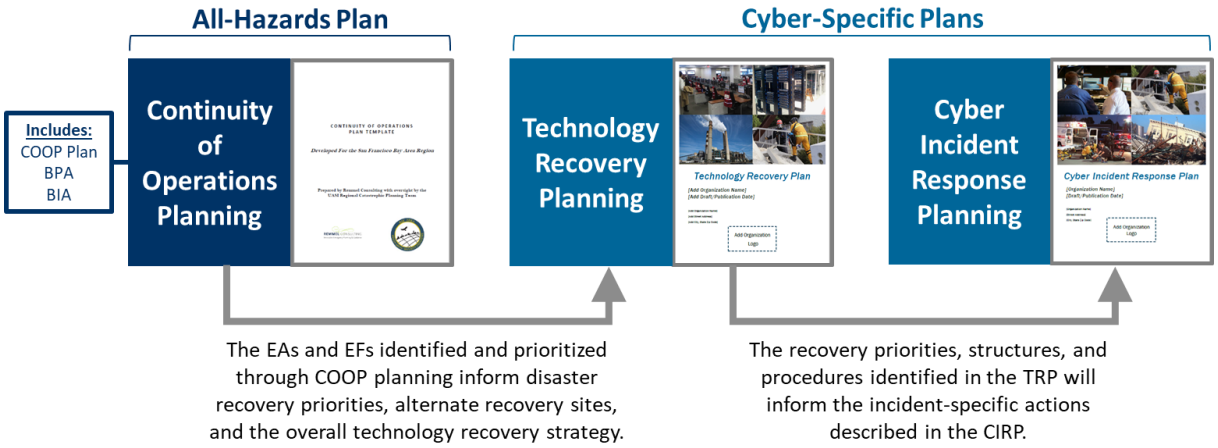

Figure 3: Relationship Between COOP and Cyber Planning

How to Use the Templates

The plan templates empower your organization/jurisdiction to develop a TRP and/or a CIRP tailored to your specific operational capacity and available resources. To aid in the development of these plans, the templates include a variety of guidance language throughout. This language is designed to provide additional context to help your organization/jurisdiction develop actionable plans and falls into three categories: development guidance, best practices, and additional resources. Throughout the templates, this language is included in call out boxes indicated by the icons depicted in **Table 2**.

Table 2: Template Guidance

Icon	Usage
	Development Guidance: Development guidance is included throughout the document to indicate specific instructions to complete the plan. It offers supplemental information that may help organizations fill in placeholders.
	Best Practice: The template will identify best practices for developing the plan (or conducting the assessments that inform the plan). In some cases, following these best practices is not required for plan completion; however, they will help enhance the plan's quality and usefulness.
	Additional Resource: In some cases, this template may reference external resources that provide useful context that will help organizations better understand a concept, collect information as part of plan development, or address other aspects of continuity planning.

The plan templates also include placeholders that prompt the inclusion of agency-specific information into the existing, standard plan content. Filling in each placeholder will allow your organization/jurisdiction to customize the templates to reflect specific requirements, capabilities, priorities, and procedures. Where placeholders are not relevant to your organization/jurisdiction or you would prefer to exclude them for any reason, simply remove the prompt and customize the plan to your preferences.

NIST Framework Core Structure

As described in the Bay Area Regional Cyber Incident Response Framework, the NIST Framework supports a risk-based approach to developing or improving a cyber program. The Framework is a tool that jurisdictions can use within their existing cybersecurity programs to identify opportunities to strengthen their risk management and cybersecurity programs as well as to communicate their programs to partners. The Framework Core reflects cybersecurity industry standards and best practices in a way that enables communication about cybersecurity activities and outcomes across an organization.

The Framework Core is comprised of five functions: Identify, Protect, Detect, Respond, and Recover. The Framework Core also identifies underlying key categories and subcategories for each function and matches them with informative references as shown in **Figure 4**. The NIST Framework Core Structure document included in the Cyber Toolkit lists the categories, subcategories, and informative references for all five functions in an easily readable format.

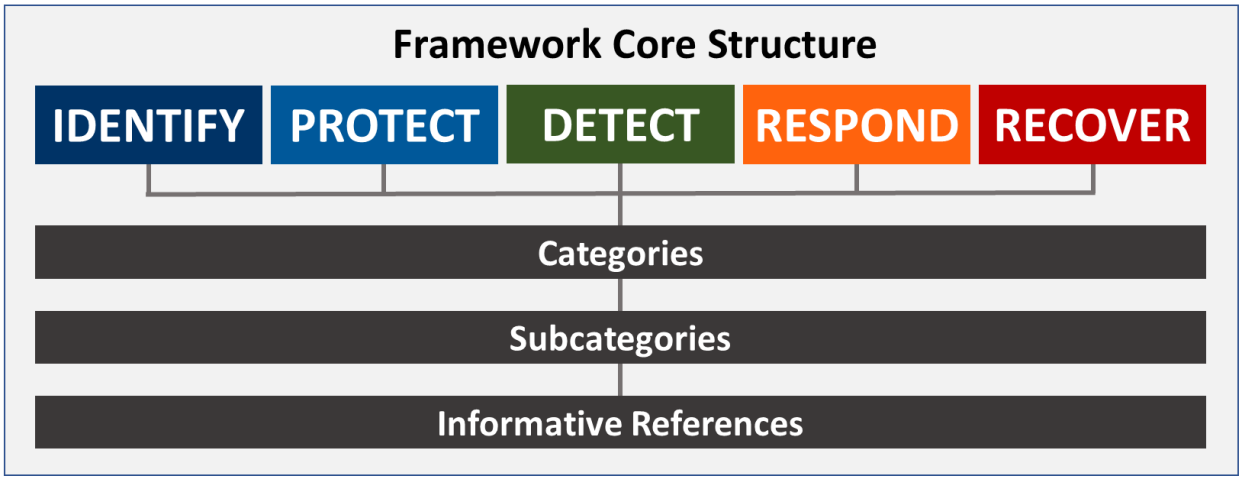

Figure 4: Framework Core Structure