MITRE

MTR220199
MITRE TECHNICAL REPORT

Essential Clean-Slate Cyber Recovery Assessment for Time-Critical Processing

Framework and Representative Criteria

Dept. No.: L522
Project No.: GNA019.P810.TEC.FS and OVH010.L520.520.J5

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

Bedford, MA

Deborah Bodeau
Kris Britton
Carolyn Francisco
Richard D. Graubart
Linda K. Jones

June 2022

Abstract

Destructive malware (e.g., ransomware) is an increasing concern for cybersecurity risk management. A variety of products, service offerings, and business processes can be used to mitigate many destructive malware events, usually with some time lag in restoration and with assumptions that certain services are already available. This report provides a starting point for an organization to establish a process for assessing the recoverability – from a “clean slate” – of enterprise services and mission processes that are time-critical and mission-essential. Such essential clean-slate cyber recovery assessment is intended to be part of an organization’s broader assessment of its readiness for cyber events and of its supply chain risk management processes, in support of and consistent with its cybersecurity risk management strategy.

Executive Summary

This document presents a framework and a representative set of criteria for assessing essential clean-slate cyber recovery (ECCR), for large organizations with time-critical functions or high volumes of time-sensitive transaction processing. ECCR is a narrowly-scoped capability, which must be understood in the context of an organization’s overall contingency and continuity of operations planning. *Essential* limits the scope to recovery of mission-essential or business-critical functions or services (including the data needed to perform those functions or provide those services) to a minimally viable (as contrasted with a fully functional) state. *Clean-slate* limits the scope to recovering, restoring, or reconstituting functions from “bare metal,” and explicitly excludes failover to a hot standby system as well as partial recovery efforts such as restoring selected files or applications. *Cyber* refers to the focus on recovery from extreme cyber event such as a destructive malware attack. ECCR is an element in a larger incident response process, which includes containing the effects of an attack, preserving evidence, expunging malware, performing post-incident analysis, and coordinating both within the organization and with external organizations. Significant resources are needed to enable ECCR for a set of systems, functions, or applications – for brevity, a target of assessment (TOA).

As illustrated in Figure 1, the framework, criteria, and concept of use are designed to be tailorable and extensible, driven by an organization’s enterprise risk management strategy and translated into terms meaningful to the organization and its critical infrastructure sector.

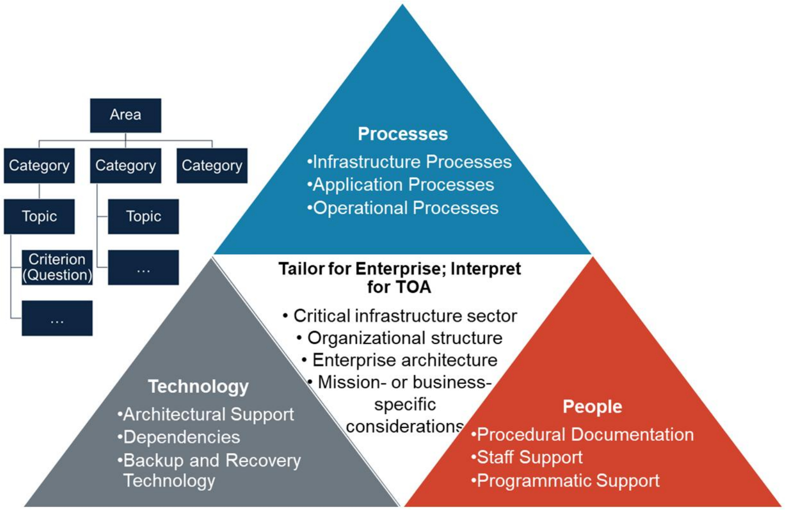

Area
Category
Category
Category
Topic
Topic
Criterion (Question)
…
…
Processes
•Infrastructure Processes
•Application Processes
•Operational Processes
Tailor for Enterprise; Interpret for TOA
• Critical infrastructure sector
• Organizational structure
• Enterprise architecture
• Mission- or business-specific considerations
Technology
•Architectural Support
•Dependencies
•Backup and Recovery Technology
People
•Procedural Documentation
•Staff Support
•Programmatic Support

Figure 1. Structure of the ECCR Assessment Framework

The ECCR assessment framework and criteria are intended to enable an organization to assess its capabilities for ECCR and to identify capability gaps for consideration in its cyber risk management strategy. In addition, an ECCR assessment can help the organization discover disconnects between sub-organizations – inconsistent assumptions about capabilities, priorities of and relationships between events in response and recovery efforts, resource availability (e.g., staffing), and how long specific activities can be expected to take.

Acknowledgments

The authors gratefully acknowledge the insightful comments of Mick Costa and Don Faatz at MITRE, and all who contributed to the development of the ECCRA framework and criteria.

Table of Contents

List of Figures

List of Tables

1 Introduction

Cyber attacks which disrupt essential services are an increasing concern, particularly when they involve destructive malware (e.g., ransomware). The potential for destructive malware raises such questions as: Can data be recovered or restored? Can functioning be restored? How quickly? How completely? These questions are particularly acute for systems, mission or business functions, and business areas which handle large volumes of transactions, which may be time-sensitive.[1] The assumption of a deliberate attacker goes beyond what is typically addressed by conventional contingency planning or continuity of operations (COOP) planning.

Guidance exists, and continues to evolve, on how to recover from (and prepare for recovery from) destructive malware, particularly ransomware. However, no standard criteria have yet been established to enable an organization, mission, or business unit to assess its preparedness to recover from extreme cyber events – those in which cyber resources are destroyed or rendered untrustworthy. Because a cyber attack can compromise undestroyed components as well as destroying others, recovery from extreme cyber events can involve recreating or rebuilding capabilities "from the ground up," "starting with a clean slate," or "from bare metal" rather than simply recovering specific files, application, or databases.

Similarly, a growing number of commercial providers offer ransomware readiness or ransomware resilience services. Frequently, these offerings assume the use of a cloud computing infrastructure (either part of the offering, or to which the offering is an add-on). Common themes in the offerings include immutable backups, multiple point-in-time images of data and software, air gaps, and automated malware analysis and remediation of software. These offerings focus on operational resilience against destructive malware. They typically do not facilitate *assessment* of the capacity for or speed of *clean-slate cyber recovery* – i.e., for recovering, restoring, or reconstituting mission, business, or supporting functions from "bare metal" to a minimally viable state after an extreme cyber event such as a destructive malware attack.[2]

Clean-slate cyber recovery sets a high bar, since it entails (i) an understanding of what constitutes a minimum viable state for a function, including what systems, services, and data that function depends on and what security services or capabilities are required as part of that state, as well as (ii) planning, resourcing, and testing or exercising recovery plans. Thus, clean-slate cyber recovery is limited to *essential* mission, business, or supporting functions, systems, or services. These functions are typically time-critical (e.g., business-essential transaction processing) or security-critical (e.g., identity and authorization management or IdAM services). The identification and prioritization of functions, systems, and services for essential clean-slate cyber recovery will be directed by enterprise risk management.

[1] These include financial systems, air traffic control systems, reservation systems, streaming services, energy providers, and managed security service providers (MSSPs) handling large volumes of log data streamed from many systems. Of these different high-volume transaction processing domains, only the financial services domain is the focus of published guidance on addressing destructive malware.

[2] Planning for Essential Clean-Slate Cyber Recovery (ECCR) can be a component of contingency planning, where the contingency being considered is one in which the entire software stack (and possibly the firmware) needed to perform essential mission or business functions has been compromised, rendered suspect, or rendered useless.

This document presents a framework for defining and evaluating criteria for essential clean-slate cyber recovery, to support assessment of capacity as well as definition and evaluation of metrics. The ability to recover essential functions can be assessed for different scopes, including functions performed by or identified with an application, a system, a service, a mission or business process, a mission or business function, or an organization as a whole. While the Essential Clean-slate Cyber Recovery Assessment (ECCRA) framework and criteria have been defined to be customizable for a variety of environments, the focus in this document is on ECCRA for time-critical services (e.g., enterprise security services, high-volume transaction processing). The process for using ECCRA enables an organization to specify the set of resources under consideration – that is, the application, system, service, mission or business process, or a mission or a business area (for brevity, referred to as a target of assessment or TOA) – and to re-express the criteria in terms meaningful to the TOA, the missions or business functions it supports, and the organization as a whole.

The framework is illustrated in Figure 2. Nine categories of assessment criteria are defined, in the broad areas of people, processes, and technology. The Technology categories relate to technical characteristics of and capabilities used by the TOA for backup and recovery to a minimally viable state[3]. The Processes categories relate to processes and procedures which staff execute as part of recovery to a minimally viable state, or in preparation for such recovery (in particular, recovery exercises and backup). The People categories relate to the staff involved in recovery activities, and the resources – information, training, and financial resources – needed. The criteria are defined using terms and ideas from a conceptual framework of states and transitions to describe essential recoverability.

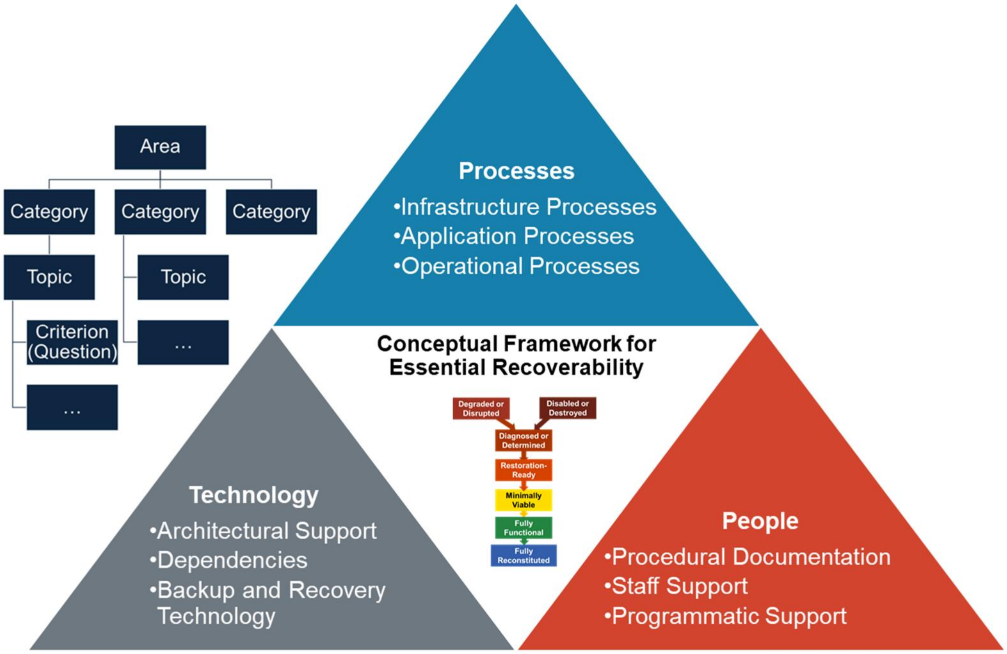


Figure 2. Essential Clean-slate Cyber Recovery Assessment (ECCRA) Framework

[3] See Section 3 for the definition of minimally viable state.

For each *category* (e.g., the infrastructure processes category in the Process area), a set of *topics* is identified based on the literature review. For each topic, one or more *criteria* are identified in the form of a question. Representative answers are provided for each criterion, as are a set of notional assessment levels, based on the alternative responses: unknown, below threshold, threshold, enhanced, and optimum. The evaluation of a criterion (the response to the question) and the assessment level support either an overall assessment of recoverability (can the TOA be recovered to a minimally viable state?) or the ability of the TOA recovery to meet time and performance requirements.

One of the major benefits of performing an ECCRA can be the discovery of disconnects between different parts of the organization – inconsistent assumptions about capabilities, priorities of and relationships between events in response and recovery efforts, resource availability (e.g., staffing), and how long specific activities can be expected to take.

1.1 Overview of This Document

Section 2 provides background on the ECCRA framework and criteria. It identifies assumptions and constraints which guided framework development as well as sources from which the criteria were drawn. Section 3 presents the conceptual framework for essential recoverability which defines key concepts and terms used in the criteria. Section 4 describes the overall concept of use for the ECCRA framework and criteria – how an organization can customize and use it to assess essential recoverability. Section 5 presents the ECCRA framework, populated with a representative set of criteria drawn from sources identified in Section 2 as well as subject matter expert (SME) expertise. A glossary and an acronym list are also provided.

2 Background

The ECCRA framework and criteria focus on a restricted problem domain, and are not intended to be used by small organizations. Section 2.1 identifies assumptions and constraints which inform ECCRA. The criteria draw from multiple sources; these are identified in Section 2.2.

2.1 Assumptions and Constraints

Assumptions and constraints relate to the scope of the ECCRA framework; the size, structure, and maturity of the organization using ECCRA; the scope of the assessment; and the ability to reconstitute. The tailoring of the ECCRA framework for an organization, together with initial assessment efforts, will serve to validate assumptions or will lead to further tailoring.

Framework Scope: The ECCRA framework focuses on essential clean-slate cyber recoverability from destructive malware, a particular type of cyber threat. Essential clean-slate recovery is part of a larger incident response process, which is beyond the scope of the ECCRA framework. The ECCRA framework does not include failover to a hot standby. The ECCRA framework currently does not address operational technology (OT).[4]

- **Essential recoverability** refers to the ability to recover, restore, or reconstitute essential mission or business functions, including application data. For a TOA, essential recoverability involves restoring the TOA to a minimally viable level of service (or a minimally viable state). Essential clean-slate cyber recoverability is essential recoverability of a TOA which includes cyber resources, starting from “bare metal” (i.e., from hardware).[5] ECCRA criteria are intended to be used to evaluate essential recoverability and to assess whether the **time to restore** capabilities to a minimally acceptable level meets requirements. Target and objective values for metrics associated with the criteria will depend on the specific application and on the assumed recovery environment. Recovery can assume the presence of, or can involve dependence on restoration of, the full stack of information and communications technology (ICT) support to an application.
- **Cyber threats** are threats that involve the use of cyberspace, either as a threat vector (i.e., used in the execution of a threat scenario) or as a threat target (i.e., the threat results in harm to cyber resources). The cyber threat landscape continues to evolve, with new alerts being issued in response to changing circumstances beyond an individual organization’s control [1]. The ECCRA framework excludes threats of natural disaster or structural failure, which are typically addressed by contingency planning and continuity of operations planning [2].

[4] Destructive malware threats against OT are of increasing concern [47]. However, in responses to incidents involving OT, consideration must be given to safety as well as rapid restoration of functionality. An ECCRA framework for OT is a topic for future investigation.

[5] More precise definitions are presented in Section 3 below.

- The ECCRA framework focuses on the threat of **destructive malware** – malware that makes cyber resources unusable.[6] Ransomware is one form of destructive malware; it makes data (which can include software) unusable via encryption. A ransomware attack can be part of a larger cyber campaign against an organization, where that campaign includes exfiltration of sensitive information and the threat that the exfiltrated information will be published unless the ransom is paid. Threats of exfiltration and extortion related to exfiltrated data are not addressed by the ECCRA framework.
- Essential clean-slate recovery is part of a larger process of **incident response**, which includes detection and initial analysis, evidence-gathering, recovery to a fully functional state, and post-incident activity [3]. The ECCRA framework assumes that the organization has a defined incident response program. Therefore, ECCRA includes only activities or capabilities needed for essential clean-slate recovery.
- Processes and technology for backup and recovery are distinct from those for hot backup and **failover**. The assumption is that failover is adequately addressed in existing contingency planning and relates to the transition from minimally viable to fully functional. It is recognized that an integrity event can be expected to affect hot standby systems, as well as the primary instantiation of the TOA. How the TOA implements – and how it uses infrastructure services for – hot backup and failover are beyond the scope of ECCRA framework and criteria.

Organization: The ECCRA framework and criteria presented in this document are intended to be used by or within a **large** enterprise with time-critical (e.g., high-volume transaction processing) requirements. The enterprise is assumed to include an organizational unit that provides a **minimum set of common services**. The **COOP planning** of the enterprise as a whole or of constituent organizations is assumed to be relatively mature.[7] The enterprise is assumed to have documented ECCR-related and security-related processes and procedures in its enterprise risk management (ERM) strategy and/or its enterprise cybersecurity risk management (CSRM) strategy.

- The enterprise is assumed to be **large** enough that multiple organizational units (organizations or sub-organizations) are responsible for distinct missions or business areas. Therefore, ransomware guidance oriented toward small-to-medium-size enterprises is of limited applicability.
- A **minimum common set of services** is assumed. The enterprise is assumed to include an organizational unit responsible for enterprise information infrastructure services (EIIS), and it is assumed that the TOA depends on EIIS for networking and shared security services (e.g., identity, credential, and access management or ICAM) as well as

[6] Destructive malware threats against OT or cyber-physical systems which could cause damage to physical resources controlled by such systems are out of scope for this document. While destructive malware can also cause physical damage to computing hardware (e.g., by causing overheating), that is typically not a cyber attacker's goal.

[7] For example, the enterprise is assumed to have achieved at least maturity indicator level (MIL) 3 in the Service Continuity Management (SCM) domain of the Cyber Resilience Review [24].

intrusion detection and response.[8] The TOA may also depend on EIIS for backup and recovery services.

  - The ECCRA framework and criteria do not preclude an organization from relying on a managed security services provider (MSSP) for shared security services. If this is the case, representatives of the MSSP will need to participate in the ECCR assessment along with EIIS representatives.
  - EIIS may also provide processing platforms (e.g., servers, virtual machines in a cloud environment) for the TOA. However, it is not assumed that all organizations within the enterprise depend solely on EIIS for security or continuity services. For example, an organization might have contracted with a third party (e.g., a cloud service provider) to provide networking, security, backup, or other services, via infrastructure, platforms, or software as a service (IaaS, PaaS, or SaaS). As noted above, representatives of the service provider will need to participate in the ECCR assessment.
  - The ECCRA framework and criteria are intended to apply to critical (including security-critical) enterprise information infrastructure services. The organization is assumed to have identified functional and assurance dependencies among such services, and to have reflected those dependencies in its contingency and continuity of operations planning (see below).

- The organization is assumed to have at a minimum performed basic **contingency planning** [2] and **continuity of operations planning**. Thus, the organization has determined which missions or business areas are most critical, and which functions within a mission or business area are essential. That is, mission-essential and/or business-critical functions have been identified.[9] For each such function, a maximum tolerable outage (MTO) has been identified, and thus a maximum tolerable downtime (MTD) or recovery time objective (RTO) has been identified for systems, services, or applications which are necessary to the execution of the function. For service providers outside the organizational unit (either EIIS or a third party service provider), the organizational unit has established service level agreements (SLAs) for services needed by each essential function; it is assumed that the SLAs are consistent with the essential function’s MTD or RTO. It is also assumed that contractual agreements with third party service providers include support for tests or exercises of contingency or COOP plans.
  - Minimum performance requirements for a mission-essential or business-critical function are assumed to include **security and safety requirements**. That is, if a function does not meet its security and safety requirements, it has failed to meet its minimum performance requirements.

[8] The concept of essential clean-slate cyber recovery also applies to enterprise services that must meet service level agreements with organizational units. This document includes TOAs within EIIS responsible for time-critical services. ECCRA for EIIS as a whole is a topic for future investigation.

[9] The term “mission-essential function” is commonly used in Government settings, while the term “business-critical function” is used in business or critical infrastructure settings.

    - As part of COOP or contingency planning, resources have been identified for which a **gold copy** is required, and procedures have been established for creating a gold copy.[10] Resources for which a gold copy may be required include data – application or transaction data, enduring mission, or business data (e.g., key parameters for business processes), and configuration data; software; and firmware.
    - **Testing and exercises** are assumed to be performed to support and validate COOP or contingency planning. The scope of testing is assumed to focus on the technologies and procedures for recovery of critical components or of applications and their associated data. Exercises are assumed to be broader, to include operational recovery as part of a larger incident response process.
    - It is not assumed that contingency plans, COOP plans, or cyber incident response playbooks include RACI (Responsible, Accountable, Consulted, and Informed) matrices. It is assumed, however, that plans and playbooks identify roles and responsibilities, and provide contact information.
- The determination of the TOAs for which ECCR is necessary or desirable, and the practices for and resources allocated to ECCR, is documented. Typically, this is documented in the enterprise CSRM strategy or in CSRM strategies for organizations within the enterprise, consistent with the ERM strategy. The ERM strategy may provide direction for or constraints on supply chain risk management (e.g., restrictions on suppliers; creation, maintenance, and use of war-time reserves). The ERM strategy or the enterprise CSRM strategy can identify circumstances under which cyber insurance is appropriate.
- The ERM strategy or the enterprise CSRM strategy identifies the process by which the TOA receives approval to operate (ATO); establishes minimum, target, and objective levels of assurance[11] for critical supporting services, whether provided as EIIS or by a third party (e.g., backup and restore; security services such as ICAM, audit, and IDR); defines the minimum level of security[12] for a TOA and for critical supporting services; defines processes for periodically validating the integrity of critical supporting services; and identifies processes or controls to determine whether a minimum level of security has been achieved as a precondition to restoring operations. (Note that these identifications or specifications can be indirect, via reference to documented policies, procedures, and requirements.)

[10] Although the phrase “gold copy” is used frequently in the contingency and COOP planning literature, and particularly in the literature related to ransomware, no standard definition exists. In this paper, the term refers to a copy for which the provenance can be established and the quality (correctness, completeness, and/or absence of unauthorized or erroneous modification) of which can be validated.

[11] In contrast with minimum, target, and objective levels of performance, which are established via service level agreements and determined via performance testing and monitoring, levels of assurance are determined via scrutiny, analysis, and penetration testing.

[12] The minimum level of security for a TOA or a supporting service includes the security functionality it provides, the level of performance for that functionality, and the level of assurance in that functionality. A TOA at or above its minimum level of security is in a minimum or acceptably secure state.

Assessment Scope: The ECCRA criteria can be evaluated for TOAs with a wide range of properties, including:

- The TOA architecture, including what components are part of the TOA; what the TOA's location in the enterprise architecture is; what data is needed for the TOA to function (e.g., configuration data, user credentials); and what TOA dependencies are on enterprise information infrastructure services or third party services.
  - The TOA could provide a critical supporting service to the enterprise or to an organization. Examples include networking services, platforms or servers, and those security services that the enterprise has determined to be essential (e.g., IdAM, network segmentation).[13]
  - The TOA could be a mission or business area as a whole, but more often will be a system or a mission or business application – i.e., a collection of software components which collectively provide a specific business function or set of functions. This includes custom applications specific to the mission or business area.
  - The TOA could be a custom application within EIIS. For example, the TOA could be an enterprise-specific ICAM application (e.g., a consistency checker, an application to locate, document, and remove all credentials and permissions associated with a given individual).
  - The TOA could consist of a set of commercial applications or tools, custom configured for EIIS.
  - The TOA could include one or more database applications. Whether the database management system (DBMS) and the database associated with those database applications are part of the TOA, or are provided as infrastructure elements, depends on the TOA's architecture.
- The mission or business criticality of the TOA, the functions it performs or the services it provides, and what constitutes its minimum viable state. The minimum viable state will typically be described in terms of the TOA's capacity for specific functions or services (e.g., how many transactions of a given type it can execute in a given time period), and will be tied to its MTD, RTO, or SLAs.
- Functional dependencies, both of the TOA on enterprise services and infrastructures, third-party services and infrastructures, other systems within the same mission or business area, systems or services managed by other mission or business areas, and systems or data provided by external entities; and vice versa (that is, what systems, services, or customers depend on the TOA performing its essential functions).

Ability to Reconstitute: Finally, it is assumed that the TOA can be restored to a minimally secure and functional state.

[13] The set of security services deemed essential will depend on the enterprise risk management strategy and on the aligned cybersecurity risk management strategy, and will take into account laws, regulations, and contractual obligations.

- It is assumed that the persistent malware associated with the events from which clean-slate recovery is needed can be successfully eliminated prior to beginning restoration, or as part of the recovery process.
- It is assumed that the description of the TOA's minimum viable state includes not only its minimum required functionality and level of performance, but also its minimum required security posture – what security functions or services it performs, what security functions or services it relies on, and the minimum required level of performance for those functions or services.[14]
- It is not assumed that essential clean-slate recovery improves the TOA's security posture. The ECCRA criteria do not involve searching for and expunging malware embedded in commercial products, as in the case in the SolarWinds campaign. While such efforts can improve the organization's overall security posture, they are not part of essential clean-slate cyber recovery.
- If the TOA performs transaction processing, it is assumed that criteria exist for determining whether a transaction that was in-progress when the TOA entered an adverse state[15] remains valid and should be completed or has been invalidated due to the passage of time or the loss or corruption of needed data. It is assumed that transaction processing rules have been defined and implemented for the timing of completing partially-executed transactions.
- It is assumed that restoration is achievable, although possibly not in the desired time frame. In particular, it is assumed that **sufficient documentation exists** about the design, integration, and configuration of system elements, and about sources and recipients of transaction information that, if necessary, the system could be rebuilt from scratch. This could involve acquiring new hardware and software, and possibly even re-implementing some applications.

2.2 Sources of Guidance

The framework draws from multiple sources of different types, as shown in Table 1. These include publications by the National Institute of Standards and Technology (NIST), the Cyber and Infrastructure Security Agency (CISA), and the International Standards Organization (ISO). They also include sources related to different sectors or domains.

Multiple critical infrastructure sectors perform high-volume transaction processing, and ransomware attacks have been documented in those sectors. However, development of guidance related to ransomware or other destructive malware is lagging for most sectors. For example, air traffic management handles, and smart airports can be expected to handle, high volumes of transactions. However, the Compilation of Cyber Security Regulations, Standards and Guidance Applicable to Civil Aviation [4] does not include any guidance related to destructive malware. While references in [4] include the ISO/IEC 27000 series and multiple NIST publications, they do not cite publications related to ransomware or other forms of destructive malware.

Similarly, high volumes of transactions are handled in the energy sector, both by operational technology (OT) and by billing systems. (The billing systems of Colonial Pipeline were affected

[14] This information may be captured in the documentation of the TOA's approval to operate (ATO).

[15] See Section 3 below.

by a ransomware attack in May 2021.) However, specific guidance on recovery from destructive malware has not been developed for the energy sector or its sub-sectors. For example, while the Electricity Information Sharing and Analysis Center (E-ISAC) tracks ransomware attacks in the electrical sector, the reliability and security guidelines developed by the North American Electrical Reliability Corporation (NERC) Reliability and Security Technical Committee (RSTC) [5] do not provide guidance on ransomware or other forms of destructive malware.

Guidance for high-volume transaction processing environments is available for the financial sector, and defines concepts and terminology used in the development of the ECCRA framework and criteria. In addition, a few representative commercial offerings are cited, to illustrate how commercial offerings implement the NIST, CISA, and financial sector guidance.

Table 1. Source Documents

NIST publications related to contingency planning, resilience, and addressing threats of destructive malware	
NIST SP 800-34 Rev. 1 [2]	Guidance on contingency planning for Federal information systems. Does not mention ransomware, but establishes terminology (e.g., Recovery Time Objective, Recovery Point Objective) needed to frame discussions of and defines practices which are used in essential recovery. See also NIST SP 1800-25, 1800-26, and 1800-11, and NIST SP 800-53.
Draft NIST SP 800-40 Rev. 4 [6]	Guidance on enterprise patch management technologies. Keeping systems and applications patched helps to protect against malware.
NIST SP 800-53 Rev. 5 [7]	Defines controls for contingency planning in the CP family: Policy and Procedures (CP-1), Contingency Plan (CP-2), Contingency Training (CP-3), Contingency Plan Testing (CP-4), Alternate Storage Site (CP-6), Alternate Processing Site (CP-7), Telecommunications Services (CP-8), System Backup (CP-9), System Recovery and Reconstitution (CP-10), Alternate Communications Protocols (CP-11), Safe Mode (CP-12), and Alternative Security Mechanisms (CP-13). (CP-5 was withdrawn.)
NIST SP 800-83 Rev. 1 [8]	Guidance on malware prevention and response for laptops and desktops.
NIST SP 800-160 Vol. 2 Rev. 1 [9]	Guidance on engineering applications, systems, and mission or business functions to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Identifies fourteen techniques (groups of technologies and practices) which can be used to address a range of threats; some are highly applicable to destructive malware.
NIST SP 800-184 [10]	Guidance on preparing for and recovering from cyber incidents. Focus is on processes and practices, in contrast with the technology-specific how-to guidance in NIST SP 1800-25, 1800-26, and 1800-11.
NIST SP 800-209 [11]	Recommendations and guidelines for securing storage infrastructure, in twelve areas. The areas are physical storage security (PS), data protection (DP), authentication and data access control (AC), audit logging (AL), network configuration (NC), isolation (IS), restoration assurance (RA), encryption (EN), administrative access (AA), configuration management, and training (TR). Each recommendation is given a unique identifier of the form xx-SS-Ry, where xx indicates the area and y is a sequential numerical identifier.

NIST SP 1800-25 [12] **NIST SP 1800-26 [13]** **NIST SP 1800-11 [14]**	NIST Special Publications 1800-25, 1800-26, and 1800-11 describe practices aligned with the five functions defined in the NIST Cybersecurity Framework (CSF, [15]): Identify, Protect, Detect, Respond, and Recover. Specific CSF categories and sub-categories, and corresponding controls from NIST SP 800-53, are identified. NIST SP 1800-25 [12]: Guidance on *identifying* and *protecting* organizational data assets from ransomware, destructive malware, and other threats to data integrity. High-level capabilities include integrity monitoring, backups, and secure storage. NIST SP 1800-26 [13]: Guidance on *detecting* and *responding* to ransomware and other destructive events. NIST SP 1800-11 [14]: Guidance on *recovering* from ransomware and other destructive events. High-level capabilities include secure storage (e.g., WORM technologies or data encryption), logging, virtualization, corruption testing, and backup. Each publication assumes a high-level architecture and includes detailed how-to guides on installing, configuring, and using commonly-used products to apply the guidance.
NISTIR 8286 [16] **NISTIR 8286A [17]** **NISTIR 8286B [18]** **NISTIR 8286C [19]**	Recommendations and guidelines for integrating cybersecurity risk management (CSRM) and enterprise risk management (ERM). NISTIR 8286A discusses the identification of the cybersecurity risk context, scenarios, and analysis of likelihood and impact. It includes methods to convey risk information, such as cybersecurity risk registers (CSRRs) and risk detail records (RDRs). NISTIR 8286B describes how risk analysis can be used to help prioritize cybersecurity risk, evaluate, and select appropriate risk responses, and communicate risk activities as part of an enterprise CSRM strategy. NISTIR 8286C describes processes for aggregating information from CSRM activities throughout the enterprise. Ransomware is mentioned as an example type of risk.
NISTIR 8374 [20]	Provides a profile, using the NIST Cybersecurity Framework [15], for ransomware risk management. Identifies the central role of business-critical services in incident recovery planning and execution.
CISA publications related to ransomware, destructive malware, and operational resilience	
Ransomware Guide [21]	Describes best practices for reducing the risks of ransomware infection, and provides a response checklist.
ST13-03 [22]	Describes best practices and planning strategies for addressing destructive malware threats, particularly recovery and reconstitution planning informed by a Business Impact Analysis (BIA).
CISA Incident Response Playbook [23]	Presents standard processes for responding to incidents (including but not limited to destructive malware incidents) and responding to discovery of potential vulnerabilities.
Cyber Resilience Review [24]	Provides an assessment process (which can be administered by a third party, or executed as a self-assessment) to determine an organization’s operational resilience to cyber incidents and to manage cyber risk to critical services under operational stress. Assesses organizational capabilities and practices in ten cybersecurity domains.
CISA Tabletop Exercise Package – Ransomware [25]	Provides a tailorable template for an organization to develop a cyber tabletop exercise (TTX) focused on ransomware.
CISA Tabletop Exercise Package – Ransomware – Third Party Vendor [26]	Provides a tailorable template for an organization to develop a cyber tabletop exercise (TTX) focused on ransomware injected from a third-party vendor.
Standards related to cybersecurity and operational resilience	

ISO/IEC 27001 [27] and other publications in the 27000 series	Define standard processes for cybersecurity risk management and standard cybersecurity controls. Do not specifically address destructive malware.
ISO 22301:2019 [28]	Defines requirements for business continuity management systems. Does not specifically address destructive malware.
Guidance for transaction-oriented processes	
FSSCC [29]	Identifies needs to develop operationally resilient systems and business practices. Considers the full range of threat sources, including natural disaster as well as cyber attacks. Includes a definition of "bare metal" restoration.
DTCC [30]	Discusses potential large-scale attacks on financial systems, with the possibility of significant cascading and contagion effects. Recommends development of industry standards, e.g., criteria for safe resumption of operations. Defines a response and recovery lifecycle which includes resumption of critical operations by implementing safe-mode or alternative processes to enable critical operations, allocating surge resource support, and mobilizing partners and third-party service providers.
FSB [31]	Recommends practices for cyber incident response and recovery. Identifies needs for prioritization, "golden source" data, approved restoration procedures, and validation of restored assets. Recommends using ransomware as a motivating incident in tests and exercises.
Industry Working Group [32]	Identifies issues, tool needs, and existing tool availability specific to data integrity compromise, in both impactful and "extreme but plausible" scenarios. Identifies the concern that traditional data replication strategies have the potential to spread corrupted data to backup databases. Identifies four different data types: configuration data, application data, business transaction data, and business reference data. Identifies requirements for and assesses tool availability for recovery, reconciliation, and replay of each data type.
FFIEC [33]	Identifies destructive malware as an increasing concern, including the concern that attacks could simultaneously affect backup data centers or mirrored sites as well as primary systems. Recommends such protections as logical network segmentation, hard backups, air gapping, maintaining an inventory of authorized devices and software, and physical segmentation of critical systems.
Representative offerings from vendors and service providers	
Dell [34] [35]	Describes Dell's offering and solution architecture for backup and recovery from cyber attacks. Key concepts include logical or physical air gaps, immutable restore points, analytics which can examine backups to discover corrupt files, and expunging malware or rebuilding systems from gold-copy images of application and operating system binaries.
IBM [36] [37]	Describes an architecture for cyber incident recovery in a hybrid multi-cloud environment, supported by IBM's offerings. Key elements are immutable or write-once-read-many (WORM) storage, air-gapped protection, anomaly detection, configuration data verification, and automation and orchestration of recovery workflows.
MSP360 [38]	Describes MSP360's offering for backup and recovery, including recovery from malware attacks. Offers system image backup and full or partial system image recovery (including bare-metal restoration).

3 Conceptual Framework for Essential Recoverability

This section presents a conceptual framework, using definitions of states and transitions, for describing those portions of the recovery process relevant to Essential Cyber Recovery Assessment (ECCRA) criteria. The results of an ECCRA enable the owner or operator of an application, a system, a service, a specific mission or business process, or a mission or business area to assess how well – how quickly and how accurately[16] – steps in the recovery process are (or can be) executed. A TOA's owner or operator can also use the evidence assembled to support an ECCRA to determine the TOA's time to recovery.

In the sourced references, the terms "recovery," "restoration," "recover," and "restore" are commonly used, but with no consensus on their meaning. "Recover" is often used to apply to data, while "restore" is often used to apply to functionality. However, "recovery" often refers to functionality, and some sources discuss restoring data to a known good state.

One reason for this lack of consensus is the lack of a generally agreed-upon description of system states. This section characterizes the potential states of a system for purposes of defining ECCRA criteria. (Other efforts – e.g., requirements definition, development of service level agreements – might require definition of a more nuanced set of states.)

The conceptual framework presented below uses "system," since the decision of whether a system will be the target of an assessment depends on how an organization applies the ECCRA concept of use presented in Section 4. In the conceptual framework, "*system*" refers to a separably managed set of resources which collectively perform a set of functions or provide a set of services. While broad use of the term "system"[17] does not require the use of information or telecommunications technologies, the ECCRA framework and criteria apply to systems which consist of or include *cyber resources* – i.e., system elements that exist in or intermittently include a presence in cyberspace [9]. For ECCRA purposes, "system" can refer to (i) an application, together with its associated data; (ii) a set of applications and the platforms[18] on which they run; (iii) a set of shared services or infrastructures offered to other systems, together with the management data needed to provide the offerings; or (iv) a system-of-systems, as identified with a mission or business function or with a business area, as long as all constituent systems are under the same operational authority. In any case, a system is inherently socio-technical; it includes not only information and communications technology, but also the personnel and operational processes involved in performing system functions. "System" can also be identified with "product" in the sense of the information or services provided by the system to users or consumers (systems, mission or business areas, external organizations) who are not part of the system.

[16] Accuracy in this context means getting it right the first time – not needing to repeat a step to get more information or resources.

[17] NIST SP 800-160 Vol. 1 [7], consistent with ISO/IEC/IEEE 15288, defines a system as "a combination of interacting elements organized to achieve one or more stated purposes." The draft Revision 1 of NIST SP 800-160 Vol. 1 [41] defines a system as "an arrangement of parts or elements that together exhibit behavior or meaning that the individual constituents do not."

[18] While a platform (e.g., a server) can be a system, it can also provide supporting infrastructure to one or more other systems.

Figure 3 below identifies six possible recovery-related states of a system. The descriptions of these, and of the transitions between them, are based on the following assumptions (underlined) and *definitions (italicized* terms)[19]:

- Criticality analysis has been performed. This is typically part of contingency planning and COOP planning [2].
  - Critical functions or services have been identified. One or more of the functions the system performs or services the system provides have been designated as critical.[20]
  - Critical resources have been identified. A set of system resources have been determined to be critical, i.e., if the resource is unavailable, some critical function cannot be performed. Those resources may be system components, or may be external to the system.
    - *Resources* are separably managed assets or personnel, and include hardware, firmware, software, data, and communications ("cyber resources" or "information resources"), as well as personnel (with appropriate training and authorities), materiel, and money.
    - System *components* are discretely identifiable resources which include hardware, firmware, and software, either separately or in combination. A component can be maintained or replaced separately from other resources. A *critical component* is a component whose unavailability makes the execution of an essential function or the provision of a critical service impossible.
  - Loss limits have been defined. For data processed by the system, a recovery point objective (RPO) – the maximum acceptable amount of data loss, or the time period beyond which data loss is unacceptable, after a disruption – has been determined. For services offered by the system, a maximum tolerable downtime (MTD) or recovery time objective (RTO) has been determined.
- Performance requirements have been established for at least the critical functions, and possibly for other functions or services as well. These performance requirements include
  - A minimum acceptable level of performance, and
  - An objective or normative level of performance.

  Performance can be described in a variety of ways (e.g., transactions per unit time) and locations (e.g., in requirements or design documentation). Minimum acceptable levels of

[19] Definitions are also provided in Appendix A.

[20] Note that a *critical function* can (a) be a function designated by the organization as a mission essential function (MEF) or a business-critical function (BCF, [20]), (b) be a function or provide a service which is necessary to the correct and timely execution of a MEF or BCF, or (c) be designated as critical based on other considerations (e.g., security-critical, safety-critical). Depending on the type of organization, the MEF designation may be driven by policy or regulations. The designation as a critical function is a result of criticality analysis.

performance may be specified in Service Level Agreements (SLAs) with users or consumers of the system (or the system's product).[21]

- Dependencies have been identified. The systems, services, or infrastructures on which the system depends (for brevity, "supporting infrastructures") have been identified, and corresponding performance requirements for those infrastructure elements have also been identified. Those performance requirements may be specified in SLAs (with EIIS or third-party providers).
- Multiple ways to be in some states may be possible.

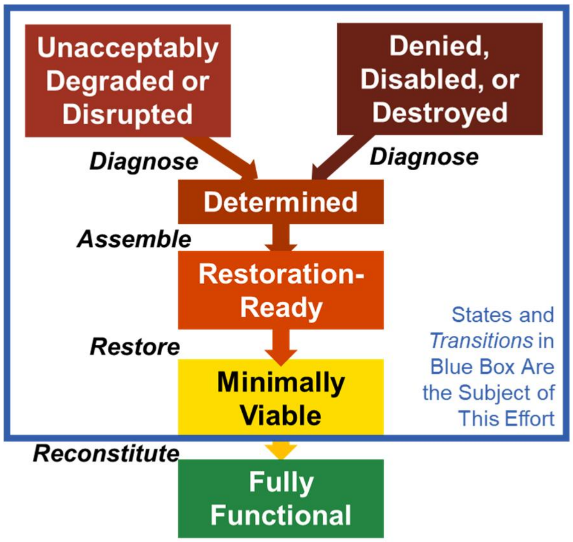

Unacceptably Degraded or Disrupted
Denied, Disabled, or Destroyed
Diagnose
Diagnose
Determined
Assemble
Restoration-Ready
Restore
Minimally Viable
States and *Transitions* in Blue Box Are the Subject of This Effort
Reconstitute
Fully Functional

Figure 3. Recovery-Related States of a System

Table 2 characterizes the states shown in Figure 3. For brevity, the first two states ("Unacceptably Degraded or Disrupted" and "Denied, Disabled, or Destroyed") are referred to as "adverse states." The proximate cause of the system being in an adverse state is referred to as an adverse event.

Table 2. Recovery-Related States of a System

State	Description
Unacceptably Degraded or Disrupted	Some essential functions or data are unavailable or cannot meet their performance requirements *or* SLAs cannot be achieved. *Degradation refers to a decrease in level of service or functioning. Disruption refers to intermittent gaps in a service or function.* *This state may be due to disruption or degradation of a supporting infrastructure, or to a non-critical resource being disabled or destroyed.*

[21] The phrase *minimum viable product* is sometimes used to refer to the outputs the system produces, the functions the system performs, and/or the services which the system provides when operating at its minimum acceptable level of performance.

State	Description
Denied, Disabled, or Destroyed	No functions can be performed. *This state is typically the result of an extreme event (see discussion below).* *This state may be due to a critical resource being disabled, destroyed, or made unreachable.*
Determined	The states of the system, its components (including software and data), and its supporting infrastructures are known *This knowledge is needed to enable the resources needed for restoration-readiness to be identified.* *The cause of the system's adverse state may be known. This knowledge can facilitate determination of the states of resources needed for restoration-readiness, but is not required.*
Restoration-Ready	All resources needed to return the system to a minimally viable state have been identified and put in place. *Note that these include not only resources which are part of the system itself, but also resources which are provided by supporting infrastructures.*
Minimally Viable	The system performs its critical functions to at least the minimal level of performance required for those functions. *In this state, functioning may be degraded or disrupted, but not to an unacceptable level. Security services and functions provided or used by the system operate correctly and at (at least) the minimum level of performance required by the organization.*[22]
Fully Functional	The system performs all its required functions at the objective or normative level. *The functions and resources used to achieve the state may or may not be the same as those employed prior to the disruption.*

Table 3 establishes terms for the transitions between the states.

Table 3. Recovery State Transitions

Starting State	Ending State	Name of Transition
Unacceptably Degraded or Disrupted	Determined	Diagnose
Denied, Disabled, or Destroyed	Determined	Diagnose
Determined	Restoration-Ready	Assemble
Restoration-Ready	Minimally Viable	Restore
Minimally Viable	Fully Functional	Reconstitute

In the ECCRA framework, ***essential cyber recovery relates to capabilities, resources, and processes needed to take a system from any adversely affected state to a Minimally Viable state***.[23] The criteria focus on recovery from an extreme event, from an integrity event, and

[22] The minimum level of security functioning may be specified in the system requirements, the organization's cybersecurity risk management strategy, the organization's contingency plan, or the system's approval to operate (ATO).

[23] The term "partial recovery" can be used to refer to the composite transition from either of the adverse states to a state in which some functioning has been restored, but the requirements for being in a Minimally Viable state have not been met.

especially from an extreme integrity event, with a cyber cause (e.g., not caused by a physical disaster). These terms are discussed in Section 3.1. An extreme integrity event with a cyber cause calls for clean-slate recovery, in order to re-establish the trustworthiness of system functions. Clean-slate recovery is discussed in Section 3.2.

3.1 Events of Concern

An ***integrity event*** is one which reduces the quality of one or more information resources; a user of the information resource cannot have confidence that it has its required properties (e.g., correctness, accuracy, timeliness, internal consistency). An integrity event can cause a system in a Fully Functional state to transition to a Minimally Viable, an Unacceptably Degraded or Disrupted, or a Denied, Disabled, or Destroyed state. An integrity event has the consequence that some information resources cannot reliably be used.

An ***extreme event*** is one which results in the Denied, Disabled, or Destroyed state. Examples of extreme events include, but are not limited to:

- Destructive malware, which can destroy data, disable firmware or software, or (as was the case with Stuxnet) destroy physical system components. Destructive malware includes ransomware, but can also include wipers (e.g., file system wiping, Master Boot Record (MBR) wiping).
- Determination that a critical or security-critical system component has been so compromised as to merit shutting down a system and rebuilding it (e.g., as in the case of SolarWinds).
- Physical destruction of or extended unavailability of power or staff for a facility housing the system's processing and storage. Note that recovery from this type of extreme event can be handled by failover and is covered by contingency planning.

Destructive malware (e.g., ransomware) is intended to cause an ***extreme integrity event***, i.e., an event which destroys the system, or which has the consequence that no part of the system can *a priori* be assumed to be trustworthy. Thus, an extreme integrity event may require that a system be recovered, restored, or reconstructed starting "from bare metal" (where a more precise characterization of the resources used in recovery from an extreme event depends on the system's technical and operational architecture).

3.2 Recovery from "Bare Metal" or a "Clean Slate"

The term "bare-metal recovery" is often used to refer to recovery of a single machine or platform (for example, [39]). By contrast, [29] states that "**Bare Metal** restoration is a process whereby new technology environments ("new normal") need to be created. This would typically take place when the infrastructure and operating data required to deliver business services have been destroyed or rendered unusable." To avoid confusion, the term "bare metal / clean slate recovery (BM/CSR)" is used in this report to encompass the broader sense of recovering a system which may consist of multiple machines (physical or virtual), operating systems (OSs), applications, and supporting software, starting from wiped-clean instances of those machines or from new machines. Thus, BM/CSR can – but does not necessarily – include acquisition (or provision from a war-time reserve[24]) of new hardware or software. BM/CSR contrasts with partial or selective recovery (i.e., recovery of specific applications / files from backups, assuming the OS and supporting services are functioning normally) in its inherent distrust of running software.

BM/CSR also contrasts with failover to a system which mirrors the primary system – and which, in the case of ransomware or other destructive malware, must be assumed to be in the same adverse state as the primary system. At the platform / individual machine level, there are two major approaches to BM/CSR: rapid or system image recovery (using a bootable image) and phased recovery (install OS; recover partitions; recover applications / files). (These can be executed on existing hardware, after restoring BIOS and other firmware, or on a new hardware component.) The recovery assessment criteria do not assume that a TOA can perform rapid recovery of individual machines; the criteria therefore include assessment questions which cover both rapid and phased recovery processes. More importantly, unless the TOA is a single machine, BM/CSR must be orchestrated – components need to be brought online according to some order of precedence, based on their interdependence.

BM/CSR is a response to extreme integrity incidents. As noted above, such incidents can render unusable or untrustworthy all software components of the system. The system needs to be recovered "from bare metal" (i.e., not retaining as active any of its components, but instantiating them from trustworthy copies – which may not be completely current) to a minimally viable state; this includes critical software (properly configured), supporting services, and data files.

In terms of the state-transition model in Figure 3, the Determined state provides the knowledge needed to decide whether BM/CSR is necessary or desirable. (Note that a situation may arise in which the system is in an unacceptably degraded state, from which the recovery process that is quickest and can be performed with the greatest confidence in a quality outcome is BM/CSR.) The ECCRA criteria are intended to enable the enterprise to answer the following questions:

- How quickly, and with how much confidence that the decision is correct, can the TOA's owner determine which type of recovery from an adverse state is needed? That is, how quickly and with how much confidence can the *Diagnose* state transition be executed?[25]
- Assuming the determination is that BM/CSR is needed, how quickly and how completely can the TOA's recovery-responsible staff assemble the resources they need to start the transition to a minimally viable state? That is, how quickly and with how much confidence can the *Assemble* state transition be executed?
- In the case of BM/CSR, how quickly can the TOA's recovery-responsible staff execute the transition to a minimally viable state? That is, how quickly and with how much confidence can the *Restore* state transition be executed?

One of the key resources in BM/CSR is a gold copy of software and configuration data. A gold copy of some business data (i.e., data that is used as a standard reference for the business process, as contrasted with application or transaction data) may also be needed, depending on the

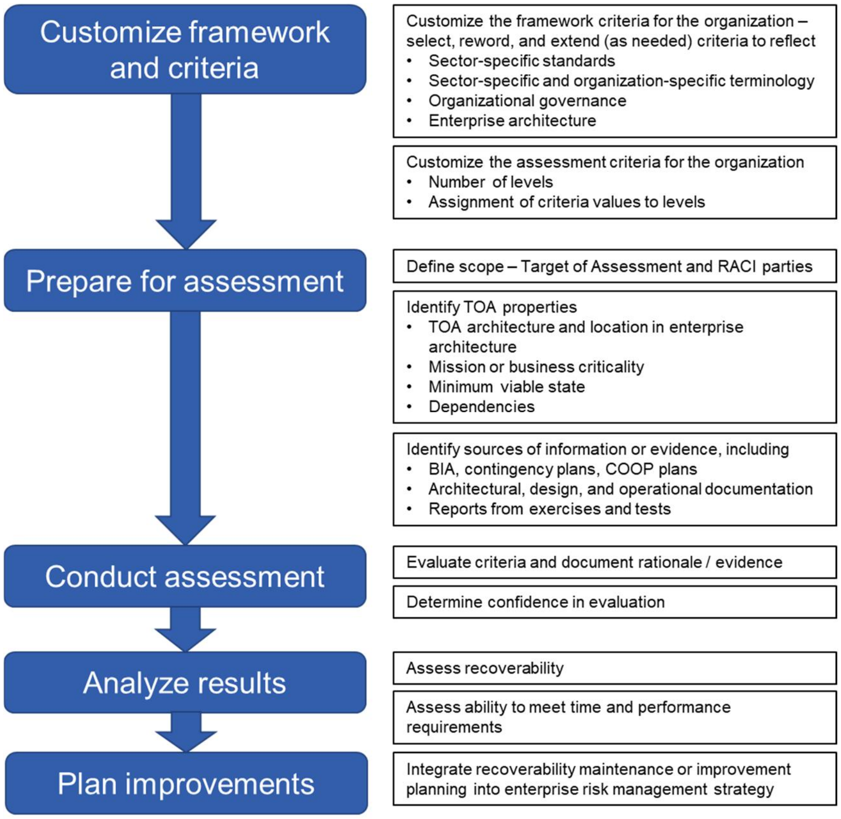
[24] A war-time reserve is "reserve of critical components, both special-purpose and acquired, for use in a crisis situation." [9]

[25] The degree of confidence in the damage assessment needed to determine the course of action – standard recovery vs. BM/CSR – is an expression of the enterprise risk tolerance, as established in the enterprise risk management strategy.

nature and function of the TOA. The maintenance of gold copies in air-gapped, secure storage offline from the operational system is increasingly cited as a standard of good practice. Depending on organizational policies and practices, gold copies of software can include incremental updates and patches or can take the form of a vendor’s original delivery of the software.

4 Concept of Use

The ECCRA framework and criteria are intended to be customized and used by an organization to assess essential clean-slate cyber recoverability from extreme integrity events and to assess whether the time to restore capabilities to a minimally acceptable level meets requirements. The general process for using the ECCRA framework and criteria is illustrated in Figure 4. Five broad phases are identified, with the first phase interpreting the organization's enterprise risk management (ERM) strategy,[26] the middle three being specific to the target of assessment, and the final phase integrating the results into the organization's ERM program.



Customize framework and criteria

Customize the framework criteria for the organization – select, reword, and extend (as needed) criteria to reflect
- Sector-specific standards
- Sector-specific and organization-specific terminology
- Organizational governance
- Enterprise architecture

Customize the assessment criteria for the organization
- Number of levels
- Assignment of criteria values to levels

Prepare for assessment

Define scope – Target of Assessment and RACI parties

Identify TOA properties
- TOA architecture and location in enterprise architecture
- Mission or business criticality
- Minimum viable state
- Dependencies

Identify sources of information or evidence, including
- BIA, contingency plans, COOP plans
- Architectural, design, and operational documentation
- Reports from exercises and tests

Conduct assessment

Evaluate criteria and document rationale / evidence

Determine confidence in evaluation

Analyze results

Assess recoverability

Assess ability to meet time and performance requirements

Plan improvements

Integrate recoverability maintenance or improvement planning into enterprise risk management strategy

Figure 4. General Process for Using ECCRA Framework and Criteria

The selection and prioritization of mission or business areas, and TOAs within (or identified with) those areas, is driven by the organization's ERM strategy. In general, selection and prioritization is consistent with contingency and COOP plans, and is based on criticality to mission-essential or business-critical functions. However, other factors could result in modifications to a criticality-based prioritization. These could include resource availability (both resources to perform the assessment, and resources to improve recoverability), concerns for vulnerability to attack, planned upgrades or modifications, and other programmatic

[26] NISTIR 8286 [16] provides general guidance on integrating cybersecurity into ERM. NISTIR 8286A [17] and NISTIR 8286B [18] provide guidance on identifying, estimating, and prioritizing cybersecurity risks, explicitly including risks due to ransomware.

considerations (e.g., the integration of new systems into the enterprise as the result of an acquisition or merger).

Benefits: One of the major benefits of performing an ECCRA can be the discovery of disconnects between different parts of the organization – inconsistent assumptions about capabilities, priorities, and sequences of events in response and recovery efforts, resource availability (e.g., staffing), and how long specific activities can be expected to take. Thus, ECCR assessment would serve to improve the organization's overall contingency planning and asset management. In addition, the documentation of TOA properties, the assembly of information sources, and the documentation of answers to ECCRA criteria questions enable each new set of participants to consult the elicited information and validate it, correct it, or determine that the information needs to be developed. Thus, another benefit of an ECCRA is improvement of the organization's documentation for the TOA.

4.1 Customize the Framework and Criteria for the Enterprise

In the first phase, the organization customizes the framework and assessment criteria to be meaningful and useful in the context of its ERM strategy. Customization applies to the framework, assessment levels, and confidence levels. The organization also defines procedures for carrying out assessments, building on the descriptions in Sections 4.2 through 4.4.

Framework. The framework can be extended to include additional topics and criteria, based on the organization's critical infrastructure sector and sector-specific standards for cybersecurity, resilience, and COOP. The organization can determine that some topics are not relevant to its operations, in light of its governance structure or enterprise architecture. The wording of topics and criteria can be tailored to reflect sector-, organization-, or architecture-specific terminology. For example, some representative answers identify time intervals (e.g., annually, semi-annually, monthly); the time intervals could be re-specified based on organizational policies and practices. Additional representative values for criteria can be identified (e.g., based on guidance or regulations specific to the sector or domain in which the organization operates).

Assessment Levels. Notional assessment levels are identified in Section 5, based on the alternative responses to a question, as shown in Table 4.

Table 4. Notional Assessment Levels

Assessment Level	Description
Below Threshold	Unknown or not reaching the minimum baseline set by the organization.
Threshold	The minimum baseline set by the organization. If answers fall below the threshold, TOA recoverability from an extreme incident cannot be assured and recovery time cannot be estimated.
Enhanced	An intermediate level between Threshold and Optimum. Answers at this level indicate the potential for TOA recoverability from an extreme incident, with the caveat that the level of effort and time involved to assemble the needed information and resources and to achieve a minimally viable state may be significant.
Optimum	The organizational goal for all TOAs. Answers at this level indicate a high degree of recoverability, and high confidence that the TOA can be restored to a minimally viable state within its required time to recover.

As part of customization, the break points between levels could be adjusted, based on organizational policies and risk management strategies. Additional intermediate levels could be defined if needed to reflect organizational policies. It should be noted that organizational risk management strategies and resulting policies, processes, and practices may need to be defined in order to refine the definition and achievability of the Optimum level.

Confidence Levels. Confidence levels are used with assessment respondents as part of reviewing and discussing the responses and evidence and having a conversation around the quality of the findings. Customization of confidence levels involves scope and values. In terms of scope, the organization can assess confidence levels for individual criteria, for topics, or for each category.

Notional confidence levels, which the organization can tailor to its assessment process, are provided in Table 5.

Table 5. Notional Confidence Levels

Confidence Level	Description
Low	The respondents had difficulty answering most of the questions, and generally struggled even with the ones they could answer. The supporting evidence is very limited or non-existent (e.g., incomplete documentation, no actual or planned testing artifacts, few products/components identified).
Moderate	The respondents provided answers to majority of the questions, most were just partial answers, and/or they struggled with them. There was supporting evidence, but it was not complete (e.g., in some instances documentation was still being developed, testing was planned but had not been carried out, not all products/components had been identified).
High	The respondents provided complete or nearly complete answers to all questions. The answers took into consideration the needed depth and breadth of the question. The supporting evidence was complete (e.g., documentation provided/referenced for all aspects of the question, identification of a specific product/component, testing and response, sample test results).

Confidence levels could apply equally to positive or negative assessment responses; however, evidence will typically only apply to positive assessment responses. For example, it is possible for the respondent to be very confident that the TOA does not have a particular recovery capability.

Once the framework has been tailored and populated for the organization, the assessment criteria can be adjusted consistent with the ERM strategy. The number of assessment levels can be decreased (e.g., unknown, unacceptable, acceptable) or increased. The assignment of possible criteria values to levels can be adjusted.

Assessment Procedures. The organization defines procedures for conducting the assessment of a TOA, consistent with existing organizational processes, to elicit the most accurate information and to minimize the time, effort, and disruption. This can involve creating data collection instruments (e.g., worksheets, Web-based tools) so that criteria can be assessed asynchronously, taking advantage of standing meetings to assess criteria in a facilitated session, holding assessment-specific facilitated scoring meetings, or some combination of these. The procedures for performing an assessment will cover such topics as the order in which different areas are assessed and how inconsistencies between answers to questions will be resolved.

Note that the tables in Section 5 identify notional assessment levels, and that the organizational customization of the framework and criteria will define organization-specific levels, based on organization-tailored representative answers. It is recommended that the materials provided to participants in the scoring process exclude the definition of organization-specific levels, to avoid biasing the responses.

4.2 Prepare for the Assessment

In the second phase, the scope of the assessment is determined; properties of the TOA are identified; and sources of information to be used in the evaluation of criteria are designated. Participants in the assessment are also identified, and the organization-specific assessment procedures are defined. As part of determining the scope, responsible, accountable, consulted, and informed (RACI) parties may be identified, so that answers to criteria questions (particularly those related to dependencies) can be validated.

Scope: As noted in Section 2.1, the ECCRA framework and criteria could be applied to a variety of TOAs. Preparation for the assessment involves answering such questions as:

- What is the TOA? What functions does it perform, or what services does it provide?
- Who – what organizational unit, office, or role – is responsible for overseeing its operations? Who is responsible for day-to-day operations? Who is responsible for ensuring that it is maintained consistently with the organization's policies and architectural requirements?
- Who are the stakeholders in the TOA's correct and timely functioning? To whom is TOA management accountable (e.g., via SLAs, in terms of organizational policies)? Who is responsible for determining that the TOA is in a minimum viable state and thus can be allowed to operate? Who is responsible for determining that the TOA is in a fully functional state? Who should be consulted about changes in TOA functioning, or relative priorities for recovery functions? Who should be informed about the TOA's health and status? (These questions apply the RACI – responsible, accountable, consulted, informed – concept to TOA functioning and recovery.)

Properties: Preparation for the assessment includes identifying the TOA's mission-essential or business-critical functions as well as its critical components. Preparation also includes identifying any specific properties that must be validated for the TOA, either for its minimally viable state or for its fully functional state. Such properties will typically be related to security, privacy, safety, or performance; the results of validation inform stakeholders as identified above. Preparation for the assessment involves answering such questions as:

- What constitutes acceptable (minimum) security for the TOA? How is the security of the TOA determined?
- If the TOA performs transaction processing, how is the state of a transaction determined?

Information: Sources of information that participants in the assessment can refer to or draw upon, to support their answers, can include

- Contingency plans, COOP plans, and the analyses supporting that planning, e.g., mission impact analyses or assessments (MIAs) or business impact analyses (BIAs), or crown jewels analyses (CJAs).
- Cyber incident handling procedures or incident response playbooks.
- Cyber resilience assessments such as the Cyber Resilience Review (CRR).
- Operating procedures for the TOA, particularly those which involve backup and recovery.
- Technical documentation for the TOA, which identifies its components, functional dependencies, and information flows. Infrastructure services on which the TOA or its recovery process depends can include backup and recovery services; identity and access management services; audit services; cloud / processing services; storage services; file transfer; messaging and/or email; enterprise network infrastructure; and telecommunications services. Note that maintenance of such documentation can be costly and time-consuming, and is driven by the TOA's criticality to the enterprise.
- Reports from tabletop exercises[27], cyber exercises, COOP exercises, and tests of backup and recovery capabilities.

Participants and Procedures: The set of participants in the assessment will depend on the organization's structure and on the TOA's location in the enterprise architecture. (Roles and expertise are identified for each category; see Section 5 below.) If the TOA is part of the enterprise information infrastructure, then participants will typically be limited to EIIS staff, although representatives of mission or business areas may be consulted. If the TOA falls under (or is identified with) a mission or business area, participants will include representatives from that area, with representatives of EIIS consulted to ensure that responses about how enterprise services are used are correct. Similarly, if the TOA uses third-party services (e.g., a cloud computing infrastructure), representatives of those services may be consulted.

4.3 Conduct the TOA Assessment

The organization conducts the assessment of the identified TOA, following its specific procedures.

Criteria are evaluated (i.e., questions are answered by selecting or specifying answers) by the identified participants, whose roles or knowledge are as identified for each category in the ECCRA framework. The rationale or evidence for the answers is documented, and the confidence in the responses is assessed.

[27] In the context of IT, a tabletop exercise (TTX) is "a discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario." [48] A TTX can focus on cyber attack vectors (i.e., a cyber TTX), on an emergency which involves cyber resources (e.g., fire at an IT facility), or on an emergency which changes the attack surface (e.g., pandemic resulting in reliance on employee home networks). Cyber TTXs are often incorporated into the system development process [49].

Review of the evidence and assessment of confidence levels helps validate the results, identify sources of information for assessment of metrics (e.g., time to recover), and identify categories or areas in which more investigation is needed to support recoverability assessment and recovery planning.

4.4 Analyze the Results

The organization can analyze the results of essential cyber recoverability assessments at the TOA level or across multiple TOAs. At the TOA level, analysis is based on the artifacts generated in the course of the assessment:

- *Criteria responses and assessment levels*: Answers to the questions selected and tailored from those in Section 5, and corresponding assessment levels.
- *Supporting documentation*: Evidence to support the responses, including design documentation, inventory reports, and reports from exercises.
- *Confidence levels*: Assessment of the confidence in each response, based on the availability and quality of supporting documentation and on the respondents' certainty about their answers.

TOA analysis can focus on either or both essential recoverability (*can* essential functions – including the data they require – be restored?) and time to recover (*how quickly* can a minimum viable state be achieved?). As indicated in Table 6, most criteria relate to recoverability. (See Section 5 for details.[28]) The evidence supporting the evaluation of criteria related to time to recover can be expected to include or indicate how long essential recovery takes, particularly at the higher assessment levels.

Table 6. Characterizing Criteria

Category	Recoverability Criteria	Time-to-Recover Criteria
Architectural Support (AS)	AS.1a, AS.1b, AS.2a, AS.2b, AS.3a, AS.3b, AS.4a, AS.5a	AS.2c
Dependencies (DP)	All	
Backup and Recovery Technology (BR)	BR.1a, BR.1b, BR.1c, BR.2a, BR.2b, BR.2c, BR.2d, BR.4a, BR.4b, BR.4c	BR.1d, BR.3a, BR.3b
Infrastructure Processes (IP)	IP.2a, IP.2b, IP.2c, IP.3a, IP.3b, IP.4a, IP.5a, IP.5b	IP.1a, IP.1b
Application Processes (AP)	AP.2a, AP.3a, AP.4a, AP.5a, AP.6a, AP.7a, AP.7b, AP.7c, AP.7d, AP.8a, AP.8b, AP.8c, AP.8d	AP.1a, AP1.b
Operational Processes (OP)	OP.1a, OP.2a, OP.3a, OP.4a, OP.6a	OP.5a, OP.5b, OP.5c
Procedural Documentation (PD)	PD.1a, PD.1b, PD.1c, PD.1d, PD.1e, PD.2a, PD.2b, PD.3a, PD.3b	PD.1f, PD.1g
Staff Support (ST)	All	
Programmatic Support (PS)	All	

[28] As discussed in Section 5 below, for ease of reference, criteria are given identifiers of the form XY.n.l, where XY refers to the category (e.g., AS for Architectural Support), n identifies the topic within the category (e.g., AS.1 refers to the identification of a minimally viable state), and l identifies the question.

Assessing the ability to recover entails analysis of the results of the assessment (i.e., evaluation of the criteria), together with artifacts and evidence provided in support of responses and the level of confidence in the results. The TOA assessment can be presented as a heat map profile based on the criteria associated with recoverability (as contrasted with time to recover), with the results of assessed values rolled up from questions to topics to categories.

Assessing how well the RTO for the TOA can be met involves looking at the evaluation of the time-to-recover criteria and the supporting evidence (e.g., exercise or test results). RTOs are typically developed under the assumption that the cause and scope of the disruption are known. Recovery from a cyber-related event adds the complexity of needing to determine the scope of the incident and the trustworthiness of components of a system (applications, data, etc.) prior to restoration. This can include forensic analysis of artifacts left by an attacker. Time-to-Recover calculations should include an analysis of how the scope will be determine and how component trustworthiness will be determined, how long it will take to identify and get in place known good components, along with how long the actual system restoration will take.

Evidence should be retained and used for reference, but the confidence level should reflect a qualitative assessment of the answers. Analysis of gaps in recovery capabilities should emerge from the results to indicate areas to be included in the improvement plan.

5 Essential Clean-Slate Cyber Recovery Assessment Criteria

This section describes the recovery assessment criteria for the categories illustrated in Figure 2. . Nine categories are defined in Table 7. The first three relate to technical characteristics of and capabilities which can be used by the TOA for backup and recovery to a minimally viable state.

The next three relate to processes and procedures which staff execute as part of recovery to a minimally viable state, or in preparation for such recovery (in particular, recovery exercises and backup). The differences among these categories relate to expertise about the TOA and to roles and responsibilities for executing the processes. Roles include TOA administrators and user representatives, system administrators within the mission or business area, system user representatives within the mission or business area (if different from TOA users), enterprise system administrators, and third-party system administrators. (Additional or different roles may be identified.)

The three process-related categories each include some form of exercise or test, but the assumptions about the scope and the personnel involved in the exercise or test differ. Under infrastructure processes (IP), use of infrastructure in recovery of the TOA's critical components is tested; those involved will typically be primarily enterprise staff, with TOA administrators tracking their efforts. Under application processes (AP), recovery of TOA applications and data or some functionally distinct and separably recoverable subset of TOA resources is tested; those involved will typically be TOA administrators, with knowledge of TOA internals, with EIIS staff tracking and supporting their efforts. Under operational processes (OP), recovery processes are exercised, to ensure that operational staff (TOA administrators, users, and TOA senior management, as well as enterprise staff) have experience.

The last three categories relate to the staff involved in recovery activities, and the resources – information in the form of documentation, training, and financial – needed.

Table 7: Criteria Categories

Category	Description
Technology	
Architectural Support (AS)	This category covers aspects of the technical architecture of the TOA which facilitate more effective and assured recovery – in particular, how the TOA's architecture takes the anticipated need for recovery from extreme integrity events into consideration and whether, how, or to what extent the TOA's architecture provides for damage limitation.
Dependencies (DP)	This category covers identification of the TOA's dependencies on resources not under the control of its responsible office. These include infrastructure services as well as upstream applications (i.e., other applications which create data products which serve as inputs or feeds to the application) and can include resources provided by other critical infrastructures (e.g., power, water). This category can also cover identification of other applications, services, mission or business areas, or external business partners which depend on the TOA.

Category	Description
Backup and Recovery Technology (BR)	This category covers the technical capabilities for backup and recovery that exist, and who is responsible for providing those capabilities to the application. It does not cover how those capabilities are actually used by the TOA.
Processes	
Infrastructure Processes (IP)	This category covers processes and procedures performed by TOA administrators to manage the use of the infrastructure components, systems, or services that need to be in place prior to recovery of mission or business applications. These processes use the technical capabilities identified in the Backup and Recovery Technology area and rely on identification of dependencies (see Dependency area). These processes also use the resources (e.g., spare hardware components) provided by Programmatic Support.
Application Processes (AP)	This category covers processes and procedures for using technical capabilities to determine the health and status (particularly the status during a recovery) of the TOA. These processes and procedures are typically performed by TOA administrators (or system administrators for EIIS custom applications or commercial tools). These processes use the technical capabilities identified in the Backup and Recovery Technology and Architectural Support areas.
Operational Processes (OP)	This category covers operational processes and procedures related to maintenance, backup, recovery, and status evaluation for the TOA or the mission or business area. This category covers processes and procedures performed by system staff (e.g., administrators, users) (or system administrators for EIIS custom applications or commercial tools) to perform recovery. These processes use the technical capabilities identified in the Backup and Recovery Technology area.
People (and Resources They Need)	
Procedural Documentation (PD)	This category covers documentation for processes involved in recovery. Documentation also includes information about Dependencies and uses of technology.
Staff Support (ST)	This category covers the staff resources involved in executing a successful recovery.
Programmatic Support (PS)	This category covers programmatic considerations (e.g., financial resources, contracting, supply chain) needed for recovery.

The recovery assessment criteria are presented in table form. For each category, the ECCRA framework identifies several topics, based on review of the literature as cited in Section 2.2. Topics are given an identifier (e.g., AS.1), a brief identifying phrase (e.g., Defined Minimally Viable State), and a short description of why the topic is important. For each topic, one or more questions are provided. Each question is given an identifier (e.g., AS.1a). A representative set of alternative answers is derived from the literature. Depending on the question, a single answer or multiple answers may be selected. Moreover, depending on the question, the response may involve providing specific information. As discussed in Section 4.1, these tables are intended to serve as a starting point for the development of organization-specific criteria.

The assessment levels (Threshold, Enhanced, Optimum) identified in the tables below are notional rather than normative. They reflect engineering judgment, practical experience, and the current state of the recovery literature – which continues to evolve. Thus, as discussed in Section 4.1, these levels are intended to serve as a starting point for the organization to define its own assessment levels.

5.1 Architectural Support (AS)

This category covers aspects of the technical architecture of the TOA, which facilitate more effective and assured recovery. Topics and criteria address how the TOA's architecture takes the anticipated need for recovery from extreme integrity events into consideration and how the TOA's architecture provides for damage limitation. Therefore, two concepts are central to the AS criteria: minimum viable state (see Section 3) and critical components.

Answers to AS questions about minimum viable state are directed to the office responsible for the TOA (e.g., the mission or business area director, the system manager) or their designee. Answers to questions in the other categories are directed to the TOA systems engineering staff (if such staff are retained for the TOA, as might be the case in a DevOps environment), or by the TOA's owner or operator (e.g., system manager).

Answers to AS questions are expected to be supported by design documentation (including documentation of dependencies) for the TOA or for the mission or business area as a whole, which should be maintained to be current. (See PD.1f.) Unless otherwise indicated, all criteria are used to assess recoverability.

Table 8. Architectural Support

AS.1: Minimum Viable State Defined. Specificity in the definition of "minimally viable state" enables planning and execution of recovery processes to be performed efficiently.		
Question	**Representative Answers**	**Notional Assessment Levels**
AS.1a: To what extent has a minimum viable state of the TOA been defined?	Unknown; Not at all; Informally defined using general service descriptions; Formally defined (e.g., in a requirements document, in an SLA) specifically identifying services, functions and components, with MDT or RTO specified; Formally defined, with the definition and requirements (MDT, RTO, or SLAs) coordinated with requirements for essential functions or other organizational requirements	Threshold: Informally defined Enhanced: Formally defined Optimum: Formally defined, with coordination

AS.1b: How have critical TOA functions or services been identified?	Unknown;
	Not at all;
	Informally identified;
	Formally identified (e.g., through BIA or crown jewel analysis);
	Formally identified with coordination with stakeholders (e.g., users of the services or of the results of the functions)
		Threshold: Informally identified
		Enhanced: Formally identified
		Optimum: Formally identified, with coordination

AS.2: Critical Components Identified. Critical application / system components are identified over time, and a critical component needs to be identified with enough specificity that it is possible to determine whether a restored or replaced version of that component will suffice. This is needed because it may not be possible in a timely manner to recover all components, so critical components may need to be prioritized.

Question	**Representative Answers**	**Notional Assessment Levels**

AS.2a: How have critical components been generally identified (characterized)?	Unknown;
	Not at all;
	Informally;
	Formally (through BIA or crown jewel analysis);
	Formally identified with coordination with stakeholders (e.g., users/owners of components)
		Threshold: Informally identified
		Enhanced: Formally identified
		Optimum: Formally identified with coordination

AS.2b: Which critical components have been specifically identified (e.g., using a software version number)? [29]	Unknown; None; Some, as internal to the application [specify] and updated [specify frequency]; Some as provided by [specify: the TOA's owner or operator, the official responsible for the mission or business area under which the TOA falls, EIIS, 3rd party] and updated [specify frequency]; All and updated whenever the version changes	Threshold: Some (internal) – list provided and updated at least annually Enhanced: Threshold + Some (provided by other entity) – list provided and updated at least every six months Optimum: All, updated whenever the version changes

AS.2c: How frequently is the critical component list reviewed and refreshed?	Unknown;
	Never;
	Annually;
	Quarterly;
	Whenever maintenance, updates, or changes occur;
	Other [specify]
		Threshold: Annually
		Enhanced: Quarterly
		Optimum: Whenever maintenance, updates, or changes occur

[29] Note that for all critical components to be identified specifically, critical components must be identified formally (AS.2a).

AS.3: Architectural Separation of Critical Components[30]**.** By keeping components that have been identified as critical kept separate from non-critical components (as well as each other as feasible) and by applying the principle of least privilege to interactions between components, the TOA's architecture limits the damage from compromise of different components and enables quicker recovery to a minimally viable state (which involves critical but not non-critical components). Separation may be physical, using air gaps, separate physical networks (e.g., separate cables), and separate processing platforms (hardware and firmware). Separation may be logical, using virtual or cryptographic separation between components as they execute in separate applications, processes, execution domains, or communicate over virtual private networks (VPNs).

Question	**Representative Answers**	**Notional Assessment Levels**
AS.3a: To what extent are critical components kept separate from non-critical components?	Unknown; Critical components not identified; No separation; Some critical components are co-resident with non-critical components (specify); Informal process to keep most critical components separate from non-critical components; Formal process to ensure no critical components are co-resident with critical components	Threshold: Some critical components are co-resident with non-critical components Enhanced: An informal process ensures that most critical components are separate from non-critical components Optimum: A formal process ensures that all critical components are separate from non-critical components

AS.3b: What types of separation methods are employed? Identify for each critical component (or class of critical components).	Unknown;
	None – there is no separation between components as they all execute in the same domain;
	Logical separation only;
	Combination of logical and physical separation
		Threshold: Logical
		Enhanced: Combination of logical and physical
		Optimum: Same as Enhanced

AS.4: Component Modularity. Modularity of components facilitates their individual replacement and enables them to be refreshed to a known good state. Containerization, particularly in a cloud environment, is a key form of implementing modularity.

Question	**Representative Answers**	**Notional Assessment Levels**
AS.4a: To what extent does the TOA architecture provide component modularity? Note that the answer should be consistent with AS.3b.	Unknown; No modularity (TOA components are tightly coupled); Limited modularity (e.g., critical components are packaged separately from non-critical components); Strong modularity (e.g., using containerization); Strong modularity with portability across platforms and clouds	Threshold: Limited modularity Enhanced: Strong modularity Optimum: Strong modularity with portability

[30] See [23], Containment.

AS.5: Recovery Role Support. Fine-grained privileges enable roles related to backup, restoration, and monitoring to be defined separately. This facilitates the definition of processes – and supporting training – for different recovery activities.

Note that support for role definition does not guarantee that roles will be defined. See IP.4, AP.8, OP.4, PD.1d, and ST.2b.

Question	**Representative Answers**	**Notional Assessment Levels**
AS.5a: To what extent does the TOA architecture support definition, separation, and administration of privileges specific to different recovery-related roles?	Unknown; Minimal privilege granularity (e.g., user vs. administrator) supported; Limited privilege granularity supported (e.g., separate roles for backup and for restoration); Highly granular privileges supported (e.g., dual authorization for specific actions); Highly granular privileges which enable organizational policies to be enforced	Threshold: Limited privilege granularity supported Enhanced: Highly granular privileges supported Optimum: Highly granular privileges which enable organizational policies to be enforced

5.2 Dependencies (DP)

This area covers identification of the TOA's dependencies on resources not under the control of its responsible office. Dependencies can be either direct or indirect. Examples of direct dependencies – those which are necessary to the TOA's correct and timely operation – include infrastructure services (in particular, security services such as IdAM and auditing, as well as telecommunications services) as well as upstream applications (i.e., other applications which create data products which serve as inputs or feeds to the TOA). These can also include resources provided by other critical infrastructures (e.g., power, water), facilities (e.g., a backup facility), or organizations (e.g., a cloud service provider, a software vendor). This area can also cover identification of other applications, services, mission or business areas, or external business partners which depend on the application.

Indirect, or second-order dependencies, are generally at greater distances from the TOA's internal functions and their impact on operations often take considerable time to manifest themselves. The importance of identifying second-order or indirect dependencies depends on the concept of operations (CONOPS) for BM/CSR recovery. An organization can create criteria for indirect dependencies by tailoring the DP.3 criteria.

Knowledge of direct and indirect dependencies enables the *Diagnose* transition to be made more efficiently.

Answers to DP questions are expected to be supported by SLAs and the Recovery Playbook (see PD below).

Table 9. Dependencies

<table>
<tr><td colspan="3"><b>DP.1: Dependency Level of Depth.</b> A TOA’s dependencies, when represented using a tree structure or other dependency mapping method, can be identified at varying levels of depth – i.e., distances from the TOA’s internal functions. Increased levels of depth provide context for recovery planning, particularly in case of widespread cyber attacks or outages.</td></tr>
<tr><td><b>Question</b></td><td><b>Representative Answers</b></td><td><b>Notional Assessment Levels</b></td></tr>
<tr><td>DP.1a: To what level of depth have dependencies been identified for the TOA? Select all that apply.</td><td>Unknown;
Direct dependencies within the mission or business area;
Direct dependencies on other mission or business areas;
Direct dependencies on infrastructure or other shared services or components;
Indirect or second-order dependencies on IT;
Indirect or second-order dependencies on other critical infrastructures</td><td>Threshold: Direct dependencies within the mission or business area + Direct dependencies on infrastructure or other shared services or components
Enhanced: Threshold + Direct dependencies on other mission or business areas
Optimum: Enhanced + Indirect or second-order dependencies on IT; Indirect or second-order dependencies on other critical infrastructures</td></tr>
<tr><td colspan="3"><b>DP.2: Current Dependency Identification.</b> Knowledge of dependencies helps a TOA owner plan recovery process. More complete and current information reduces the time and effort needed to assemble resources for recovery.</td></tr>
<tr><td><b>Question</b></td><td><b>Representative Answers</b></td><td><b>Notional Assessment Levels</b></td></tr>
<tr><td>DP.2a: How <i>current</i> is the information about dependencies?</td><td>Unknown;
Very outdated (e.g., application design documentation);
Outdated (e.g., final documentation of application at initial operational capability);
Recent (e.g., based on testing or exercise);
Refreshed at regular intervals (specify);
Includes Point of Contact (POC) information, refreshed at regular intervals (specify)</td><td>Threshold: Outdated (e.g., final documentation of application at initial operational capability)
Enhanced: Recent (e.g., based on testing or exercise)
Optimum: Enhanced + Refreshed at regular intervals (specify); Includes Point of Contact (POC) information, refreshed at regular intervals (specify)</td></tr>
</table>

DP.2b: How *complete* is the information about dependencies?
Note that dependency information is often revealed by exercises and experimentation (e.g., unplugging devices or cables, changing configurations).
	Unknown;
	Dependencies within the mission or business area [select: partially, fully] specified;
	Dependencies on shared [select: services, components] provided by [select: EIIS, 3rd party (specify)] [select: partially, fully] specified;
	Dependencies on upstream services [select: partially, fully] specified
		Threshold: Dependencies within the mission or business area and on shared services or component **partially** specified
		Enhanced: Dependencies within the mission or business area and on shared services or component **fully** specified; Dependencies on upstream services **partially** specified
		Optimum: Enhanced + Dependencies on upstream services **fully** specified

DP.2c: How are the *infrastructure* services or components on which the TOA directly depends identified?
Dependencies on such services will be reflected in the contents of the Playbook or Checklist (see PD.1). Note that the answer to this will need to be cross-checked with the answers to BR and IP.
	Unknown;
	Identified in general terms, including the provider (e.g., mission or business area, EIIS, 3rd party);
	Identified by name;
	Identified by name and minimum level of service
		Threshold: Infrastructure services are identified in general terms, but not specified by name
		Enhanced: Infrastructure services are specified by name
		Optimum: Infrastructure services are specified by name and minimum level of service

DP.2d: How are the *upstream applications* on which the TOA directly depends identified?
Responses to this question should be consistent with answers to PD.1.
	Unknown;
	Not applicable;
	Identified by name;
	Identified by name and by data products or data feeds
		Threshold: Not applicable or Identified by name
		Enhanced: Not applicable or Identified by name and data products or data feeds
		Optimum: Same as Enhanced

DP.2e: Where are dependencies *documented*? Identify all that apply.
Responses to this question should be consistent with responses to PD.1.
	Unknown;
	Design documentation;
	Documentation at initial operational capability (IOC);
	Recovery Playbook;
	Recovery Checklist;
	Other [specify]
		Threshold: Documentation at IOC
		Enhanced: Recovery Playbook or Recovery Checklist
		Optimum: Same as Enhanced

DP.3: Direct Dependents. Knowledge of applications, services, or systems which directly depend on the TOA helps the TOA owner plan communications during recovery (e.g., who to notify first). *Note that the communications plan – which will be covered under PD.1 – is expected to be different for external dependencies.*		

DP.3a: How are applications, services, or systems which depend on the TOA identified? Identify all that apply.	No identification of dependents; Unknown (may be included in Recovery Playbook for other applications, but if so, this is not known by the TOA owner); Identified as part of requirements definition for the TOA; Identified via SLAs to which the TOA is committed; Identified via cyber TTXs during TOA development; Identified via cyber TTXs, business continuity TTXs, or testing during operations	Threshold: Identified as part of requirements definition for the TOA Enhanced: Identified via SLAs to which the TOA is committed and/or Identified via cyber TTXs during TOA development Optimum: Enhanced + Identified via TTXs or testing during operations
DP.3b: How current is the information about direct dependencies? Identify all that apply.	Unknown; Very outdated (e.g., application design documentation); Outdated (e.g., final documentation of application at initial operational capability); Recent (e.g., based on testing or exercise); Refreshed at regular intervals (specify); Includes Point of Contact (POC) information, refreshed at regular intervals (specify)	Threshold: Outdated (e.g., final documentation of application at initial operational capability) Enhanced: Recent (e.g., based on testing or exercise) Optimum: Enhanced + Refreshed at regular intervals (specify); Includes Point of Contact (POC) information, refreshed at regular intervals (specify)
DP.3c: Which direct dependents, if any, are external? Identify all that apply.	Unknown; None (no external dependents); Some (specified by organization name); Some (specified by organization name and functional business unit within that organization); Some (POC identified)	Threshold: None, or List (specified by organization name) Enhanced: None, or List (specified by organization name and functional business unit within that organization) Optimum: None, or List (POC identified)

5.3 Backup and Recovery Technology (BR)

This category covers the technical capabilities that exist, and who is responsible for providing those capabilities to the TOA. It does not cover how those capabilities are actually used by the TOA. These include capabilities for:

- Backup
- Validation / checking during the backup process
- Protection of backup

- Validation / checking during the recovery process: *Assemble* system elements from backup
- Recovery capabilities: *Restore* the system to a minimally viable state

As a precondition to answering the questions in this category, the TOA owner needs to clarify:

- [BR-EIIS] What backup and recovery technology does the TOA rely on EIIS to provide? (Note that this is typically identified in SLAs.)
- [BR-SYS] What backup and recovery technology does the TOA provide for itself?
- [BR-MBA] What backup and recovery technology does the mission or business area provide to the TOA?
- [BR-3P] What backup and recovery technology does a third-party infrastructure provider (e.g., a cloud service provider) under contract with the TOA owner (or the mission or business area, or the organization as a whole) provide to the TOA?

If the TOA shares backup and recovery capabilities with the mission or business area, or uses an infrastructure component, supporting service, or other application, contention for resources can arise during recovery. Therefore, for backup and recovery capabilities for (i) application data, (ii) software, and (iii) configuration data, several questions arise:

- How are priorities for shared capabilities established?
- How do those priorities affect recovery of the application?

Answers to questions in this category can typically be found in design documentation, administrator and user manuals, or SLAs.

Table 10. Backup and Recovery Technologies

BR.1: Granularity of Backup and Recovery. Granularity refers to the extent to which individual applications or functions and smaller blocks of data / transactions can be recovered. Finer granularity supports recovery from low-to-moderate severity integrity events; for extreme integrity events, finer granularity supports analysis of more subtle attacks on integrity.		
Question	**Representative Answers**	**Notional Assessment Levels**

BR.1a: What types of resources are backed up? (Identify all)
For data, answer BR.1b. For codebase and configuration baseline, answer BR.1c.
	Unknown;
	Codebase;
	Configuration baseline;
	Application data (e.g., transaction state, transaction data)
		Threshold: Application data
		Enhanced: Application data and Codebase
		Optimum: Application data, Codebase, and Configuration baseline

BR.1b: What is the smallest block of critical data / transactions that can be backed up and recovered? For example, does a whole database need to be recovered, or can it be recovered incrementally?	Unknown;
	Entire database;
	Directory;
	File;
	Record;
	Message;
	Other (specify)
		Threshold: Entire database or Directory
		Enhanced: File
		Optimum: Record or message

BR.1c: If individual critical functions / applications (i.e., executables) are corrupted, to what extent can each be recovered separately?	Unknown; Cannot be recovered separately (recovery is monolithic); Some executables can be recovered separately (specify conditions); Each executable can be recovered separately	Threshold: Cannot recover separately Enhanced: Some executables can be recovered separately Optimum: Each executable can be recovered separately
BR.1d: How well specified is the maximum amount (or upper bound) of transactions or other mission or business data that can be lost as a result of existing Recovery Point Objective guidelines?	Unknown; No; Specified in design documentation; Specified in documentation at IOC; Specified in SLAs, Recovery Plan, and/or Recovery Checklist	Threshold: Specified in design documentation Enhanced: Specified in documentation at IOC Optimum: Specified in SLAs, Recovery Plan, and/or Recovery Checklist

BR.2: Unauthorized Change Prevention. Mechanisms should be provided to ensure that backup data and applications are not compromised. Note that questions of whether and how those mechanisms are used fall under IP and AP. [29] [34] [36]

Question	**Representative Answers**	**Notional Assessment Levels**

BR.2a: What methods are provided to ensure that backups of data and applications are not themselves compromised during storage? (Identify all)	Unknown;
	Virtual or logical isolation (e.g., separate virtual machines, subnets separated by firewalls);
	Cryptographically based protection;
	Diversity of backup applications;
	Use of WORM drives;
	Air gapped solutions;
	Other (specify)
		Threshold: Virtual or logical isolation
		Enhanced: Cryptographically based protection and/or Diversity of backup applications
		Optimum: Air gapped solutions and/or Use of WORM drives

BR.2b: How methods are used to create and maintain the backups? Answer separately for each type of resource that can be backed up (application data, software, configuration data).	Unknown;
	Manual process;
	Automated process, via a backup utility or service (specify)
		Threshold: Manual process
		Enhanced: Automated process, via a backup utility or service
		Optimum: Same as Enhanced

BR.2c: How can the quality of the backups be verified? Answer separately for each type of resource that can be backed up (application data, software, configuration data). Select all that apply.
Answers should be consistent with the answers to questions in the IP and AP categories.
	Unknown;
	Malware scanning;
	Polynomial checksums;
	Cryptographic checksums;
	Other quality check (e.g., checking consistency of file metadata with observable properties of the file) (specify);
	Testing of restoration
		Threshold: Malware scanning for software; Polynomial checksums for application data
		Enhanced: Malware scanning for software; Cryptographic checksums for application data
		Optimum: Enhanced + Testing of restoration for software, application data, and configuration data + Other quality check for application data

BR.2d: What is data granularity of verification?
Answers should be consistent with BR.1c.
	Unknown;
	Image;
	Executable;
	Entire database;
	Directory;
	File;
	Record
		Threshold: Image (software and configuration data); Entire database or Directory for data
		Enhanced: Selected executables for software; Individual files for application data
		Optimum: Individual executables for software; Records for application data

BR.3: Time-Bounded Recovery. (Assumes [BR-SYS]) Ensure that recovery from backups for critical services or functions within a defined time limit for the TOA. The periodic evaluation of time-to-restore for critical services or functions supports recovery planning.		
Question	**Representative Answers**	**Notional Assessment Levels**

BR.3a: *How* is the expected time-to-restore evaluated?	Unknown;
	Not evaluated;
	Review / qualitative assessment;
	Simulation / Tabletop Exercise;
	Testing
		Threshold: Qualitative assessment
		Enhanced: Simulation/TTX
		Optimum: Testing

BR.3b: How *frequently* is the ability to meet the TOA's time-to-restore requirements evaluated?	Unknown;
	Not at all;
	Annually;
	Semi-annually;
	Monthly;
	At a shorter interval than monthly, set by organizational policy
		Threshold: Annually
		Enhanced: Semi-annually
		Optimum: Monthly or at shorter interval set by organizational policy

BR.4: Monitoring of Recovery Process and Backup Integrity. Ensure that recovery status and integrity checks can be monitored throughout the recovery process and reported to responsible staff.		
Question	**Representative Answers**	**Notional Assessment Levels**

BR.4a: How is the progress of steps in the recovery process, or the recovery of specific components, monitored? Identify all that apply. If supporting services are monitored separately (e.g., by EIIS or a third party provider), identify separately.
Answers should be consistent with PS.2c.
	Unknown;
	No monitoring possible;
	Manual process;
	Automated process;
	Via an application or tool (specify)
		Threshold: Manual
		Enhanced: Automated
		Optimum: Via application or tool

BR.4b: At what granularity can the recovery be monitored? Identify all that apply.	Unknown;
	Function or service;
	TOA as a whole;
	Entire database;
	Directory;
	File;
	Record;
	Message;
	Other (specify)
		Threshold: TOA, Entire DB
		Enhanced: Directory or File; Function or service
		Optimum: Record, Message; Function or service

BR.4c: During the course of the recovery process, what integrity checks of recovered components can be observed? Identify all that apply.	Unknown; No observable checks; Data quality checks of recovered data (specify); Integrity (non-corruption / non-falsification) checks of recovered data (specify); Anti-virus / anti-malware scans of recovered software	Threshold: Data quality checks of recovered data Enhanced: Threshold + Integrity checks of recovered data Optimum: Enhanced + Anti-malware scans

5.4 Infrastructure Processes (IP)

This category covers processes and procedures performed by TOA administrators to manage the use of the infrastructure components, systems, or services that need to be in place prior to recovery of business applications. These processes use the technical capabilities identified in the Backup and Recovery Technology area and rely on identification of dependencies (see Dependency area).

Infrastructure elements can include:

a. Backup and recovery systems or services which backup and perform recovery of

    i. Application data

    ii. Software (e.g., application image, system image)

    iii. Configuration data (including definition of privileges)

  As noted under BR, these services can be provided by the system itself, by the mission or business area, by EIIS, or by a third party under contract with the mission or business area.

b. Communications (network) services (assumed to be provided by EIIS)

Infrastructure elements could also include shadowing or replication systems or services, to support failover to a hot or warm backup. However, failover to a hot or warm backup is out of scope for the ECCRA framework, since destructive malware can replicate to such backups; ransomware typically looks for data backups.

Support for answers to IP questions is expected to be found in operational concept documentation, procedures, or recovery handbooks / playbooks.

Table 11. Infrastructure Processes

<table>
<tr><td colspan="3"><b>IP.1: Critical Component Recovery Tested Regularly.</b> Check that the ability to recover or restore critical components is working properly before an incident necessitates its use. This is both a validation on the mechanisms and processes themselves, and on the users / administrators to ensure that they know what to do in case of an actual recovery. Recovery of a critical component does not include recovery of application data but does include recovery of configuration data as well as software.</td></tr>
<tr><td><b>Question</b></td><td><b>Representative Answers</b></td><td><b>Notional Assessment Levels</b></td></tr>
<tr><td>IP.1a: What is the <i>frequency</i> of testing the recovery of critical components?</td><td>Not tested;
Annually;
Quarterly;
Monthly;
At a frequency defined in terms of a multiple of the temporal RPO (specify)</td><td>Threshold: Annually
Enhanced: Quarterly or Monthly
Optimum: At a frequency defined in terms of a multiple of the RPO</td></tr>
<tr><td>IP.1b: What is the <i>method</i> for testing critical component recovery? Select all that apply. If different methods apply to different types of critical components, specify.</td><td>Not tested;
Manual (i.e., administrator-executed) steps;
Semi-automated (i.e., automated scripts which require administrator interaction);
Fully automated scripts to execute recovery, confirm that the recovered component executes correctly, and measure the time to recover;
Automated scripts to make comparisons between recovered configuration data and determine whether the temporal RPO was achieved</td><td>Threshold: Manual or Semi-automated
Enhanced: Fully automated
Optimum: Fully automated, with comparisons to check against temporal RPO</td></tr>
</table>

IP.1c: How is the ability to recover or replace damaged hardware or firmware tested? Select all that apply. If different methods apply to different types of critical components, specify. *Answers should be consistent with PS.2c.*	Not tested; Procedures to restore firmware executed (specify frequency); Time to execute firmware restoration measured; Procedures to swap in duplicate or alternate hardware executed (specify frequency); Time to swap in duplicate or alternate hardware measured	Threshold: Procedures to restore firmware executed at least annually; Enhanced: Time to execute firmware restoration measured at least every six months + Procedures to swap in duplicate or alternate hardware executed at least annually Optimum: Time to swap in duplicate or alternate hardware measured at least every six months
IP.2: System Changes Captured. Ensure that the backup image is kept consistent and up to date with primary image.		
Question	**Representative Answers**	**Notional Assessment Levels**
IP.2a: How does a change to the system (i.e., a change to firmware, software, or configuration data) trigger an update to the backup?	Unknown; Updates do not drive backups (e.g., backups are performed only on a scheduled or administrator-driven basis); Administrator-driven with automated prompt; Automatically with administrator notification and option for intervention	Threshold: Backups performed on a scheduled or administrator-driven basis Enhanced: Administrator-driven with automated prompt Optimum: Automatically with administrator notification and option for intervention

IP.2b: How are changes backed up?	Unknown;
	Incrementally;
	Entire image
		Threshold: Entire image
		Enhanced: Threshold + Incrementally
		Optimum: Same as Enhanced

IP.2c: How long or for how many change events are backups kept?	Unknown;
	Period of time [specify];
	Number of updates [specify]
		Threshold: Period of time or number of updates, as specified by TOA owner
		Enhanced: Period of time or number of updates, as specified by organization
		Optimum: Same as Enhanced

IP.3: Quality Validated During Backup. Safeguard against intentional or accidental compromise of backup systems (compromise refers in this instance to both integrity compromises of the data and insertion of malware via the backups/recovery system). *Answers should be consistent with answers to questions under BR.2 and PD.1.*		
Question	**Representative Answers**	**Notional Assessment Levels**

IP.3a: What mechanisms and/or processes provided by infrastructure BR services are used to search for the presence of malware in the data and software as they are backed up?	Unknown; No mechanisms are used; Malware scans of software are made as part of the backup process; Quality scans of data are made as part of the backup process; Periodic scans or forensic analysis of backups	Threshold: Quality scans as part of backup Enhanced: Malware scans and quality scans as part of backup Optimum: Quality scans and malware scans as part of backup; Periodic scans or forensic analysis of backups

IP.3b: Where are processes and procedures to respond to detected quality violations documented?	Unknown;
	None defined;
	Ad-hoc set of processes or procedures;
	Documented in (specify, e.g., administrator handbook, incident response playbook)
		Threshold: Ad-hoc
		Enhanced: Documented
		Optimum: Same as Enhanced

IP.4: Well-Defined Backup Deletion Process. Safeguard against intentional or accidental destruction of backup information, whether by deletion or by over-writing. A two-person rule or other defined policy enforcement mechanism helps ensure that the needed backup components are available during recovery.

The answer should be consistent with the answers to questions under BR.2 and AS.5.

Question	**Representative Answers**	**Notional Assessment Levels**
IP.4a: How is the process for destruction of backups defined?	Unknown; No backup destruction rule; Informal or ad-hoc backup destruction rule enforced by TOA administration; Formal rule (e.g., based on role initiating backup destruction) enforced by backup service provider; Two-person rule enforced by backup service provider, consistent with organizational policy	Threshold: Informal or ad-hoc rule enforced by TOA administration Enhanced: Formal rule enforced by backup service provider Optimum: Two-person rule enforced by backup service provider, consistent with organizational policy

IP.5: Quality of Backups Verified. Verification of backups helps ensure that the data and applications have not been modified since the backup occurred and thus can be used during recovery.

The answers should be consistent with the answers to BR.2.

Question	**Representative Answers**	**Notional Assessment Levels**
IP.5a: When is the quality of backups verified? Answer separately for each type of resource that is backed up (application data, software, configuration data). Select all that apply.	Periodic validation of stored information (specify period); Randomly timed validation of stored information; Validation of information as it is stored (e.g., checking consistency of file metadata with observable properties of the file); Other (specify)	Threshold: Periodic validation of stored information Enhanced: Randomly timed validation of stored information Optimum: Enhanced + Validation of information as it is stored (e.g., checking consistency of file metadata with observable properties of the file)

IP.5b: Where are processes and procedures to respond to detected quality violations documented?	Unknown; No processes or procedures defined; Ad-hoc set of processes or procedures; Documented in (specify, e.g., administrator handbook, incident response playbook)	Threshold: Ad-hoc Enhanced: Documented Optimum: Same as Enhanced

5.5 Application Processes (AP)

This category covers processes and procedures for using technical capabilities to determine the health and status (particularly the status during a recovery) of the TOA or some subset of the TOA. (The term “application” in the questions is intended to cover both the TOA as a whole and some functionally distinct and separably recoverable subset of TOA resources.) These processes and procedures are typically performed by TOA system administrators (including system administrators for EIIS custom applications or commercial tools, if the TOA is an EIIS custom application or tool). These processes use the technical capabilities identified in the Backup and Recovery Technology area. These processes can include:

- [BR-SYS or BR-MBA] Backup and validation services (including protection of backups) for
    - Business/mission data, including
        - Transaction data: “transactional information that is accessed, used or modified as part of a business process” [32];
        - Application data: databases or files created or maintained by business applications or by commodity applications used in the context of the defined business processes;
        - Reference data: information or data that is not transactional in nature and that is required for the organization to conduct its business (derived from [32]);
    - Software (e.g., application image, system image) (referred to as application data in [32]); and
    - Configuration data (including definition of privileges): “Information that is required to operate technology including system settings, indexes and user configurations” [32].
- [BR-EIIS or BR-3P] System-internal validation of recovered data (in addition to any validation done by EIIS or the third party)

Support for answers to AP questions is expected to be found in operational concept documentation, procedures, or recovery handbooks / playbooks.

Table 12. Application Processes

AP.1: Application Recovery Tests Run Regularly. Carry out practice recovery operations / tests to help provide realistic time estimates for achieving a successful recovery. Criteria for this topic look at the comprehensiveness of recovery tests (what types of responses – e.g., failover vs. BM/CSR; what types of triggering events), and whether they are run on a regular basis.

Question	**Representative Answers**	**Notional Assessment Levels**

AP.1a: How frequently are recovery tests run?	Unknown;
	Annually;
	Semi-annually;
	Monthly;
	Other time period [specify; indicate whether this is consistent with organizational policy];
	In response to [specify triggering situation or event]
		Threshold: Annually
		Enhanced: Semi-annually
		Optimum: Monthly or Other time period consistent with organizational policy + In response to triggering event

AP.1b: How comprehensively are recovery tests defined?	Unknown; Failover / business recovery test, assuming failure of a component or supporting infrastructure; Recovery test, assuming a non-extreme cyber incident; Recovery test, assuming multiple interacting failures, errors, or cyber incidents; BM/CSR test	Threshold: Failover / business recovery test, assuming failure of a component or supporting infrastructure and/or Recovery test, assuming a non-extreme cyber incident Enhanced: Recovery test, assuming multiple interacting failures, errors, or cyber incidents Optimum: Enhanced + BM/CSR test

AP.2: Applications Identified and Located. Identify applications needed for recovery of the TOA and locate the versions to be restored.

Question	**Representative Answers**	**Notional Assessment Levels**

AP.2a: How are all applications (including specific versions) needed for recovery identified and located?
The answer should be consistent with ST.1b.
	Unknown;
	Not identified;
	Ad-hoc process;
	Formal (processes listed in playbook);
	Automated support for location
		Threshold: Ad-hoc
		Enhanced: Formal
		Optimum: Enhanced + Automated support for location

AP.2b: How are the completeness and correctness of the identification verified?	Unknown; No process or mechanism; Ad-hoc verification as part of recovery testing; Checked against design documentation; Checked against asset inventories	Threshold: Ad-hoc Enhanced: Checked against design documentation Optimum: Checked against asset inventories

AP.3: Protection of Application Software Components. Ensure that application software – i.e., software specific to the TOA, in contrast to commodity software such as an OS – is securely stored.

The answer should be consistent with those for BR.2a.

Question	Representative Answers	Notional Assessment Levels
AP.3a: How is the gold copy of each critical application software component stored?	Unknown; No gold copy; Stored on a WORM drive and placed in a secured container; Stored on a WORM drive on an air-gapped system; Stored on an air-gapped system; Stored on a logically separate system	Threshold: Stored on logically separate system Enhanced: Stored on an air-gapped system or Stored on a WORM drive and placed in a secured container Optimum: Enhanced + Stored on WORM drive on an air-gapped system
AP.3b: How is the gold copy of each critical application software component kept current? *Note that the organization's configuration management process will determine how updates, patches, and new versions are deployed.*	Unknown; Fresh gold copy made each time a new version is deployed; Deployed updates and patches captured as increments, to be applied to gold copy during recovery; Fresh gold copy made each time an update or patch is deployed	Threshold: Each time a new version is distributed Enhanced: Deployed updates and patches captured Optimum: Fresh gold copy made upon deployment of an update or patch

AP.3c: How many historical gold copies of each critical application software component are retained?	Unknown;
	One (the most recent);
	Two or more, including the most recent and at least one previous version
		Threshold: One
		Enhanced: Two or more
		Optimum: Same as enhanced

AP.4: Data Location. Ensure that data needed for recovery are identified and can be located.

The answer should be consistent with ST.1b.

Question	Representative Answers	Notional Assessment Levels

AP.4a: What is the process for identifying and locating all data processed (e.g., transaction data) or used (e.g., configuration data) and backed up by the TOA needed for its recovery?	Unknown;
	No defined process;
	Manual process;
	Automated process
		Threshold: Manual
		Enhanced: Automated
		Optimum: Same as Enhanced

AP.5: Mission or Business Area Data Secured. Take measures to secure (protect from unauthorized modification) backup data for the mission or business area.

Answers should be consistent with answers to questions under BR.2.

Question	**Representative Answers**	**Notional Assessment Levels**

AP.5a: How is the backup data protected from unauthorized modification?	Unknown;
	Logical or virtual isolations;
	Air gapped solutions;
	Use of WORM drives;
	Other (specify)
		Threshold: Logical or virtual isolation
		Enhanced: Air gapped solutions
		Optimum: WORM drives

AP.6: Application Integrity Validated. Take measures for application backups to demonstrate that they have not been corrupted. This contributes to recovery confidence.

The answer should be consistent with answers to questions under BR.2.

Question	**Representative Answers**	**Notional Assessment Levels**

AP.6a: How is the integrity of the application backups validated? Identify all that apply.	Unknown;
	No mechanisms;
	Malware scanning;
	Polynomial checksums;
	Cryptographic checksums
		Threshold: Malware scanning
		Enhanced: Threshold + Polynomial checksums
		Optimum: Malware scanning + Cryptographic checksums

AP.7: Data Integrity Validated. Measures are applied to mission or business data to prove that it has not been corrupted. This contributes to recovery confidence.

Question	**Representative Answers**	**Notional Assessment Levels**

AP.7a: How is the integrity of backup data validated?	Unknown;
	No integrity checks;
	Polynomial checksum;
	Cryptographic checksum;
	Other (specify)
		Threshold: Polynomial checksum
		Enhanced: Cryptographic checksum
		Optimum: Same as Enhanced

AP.7b: At what granularity are checksums or other integrity checks associated with data?	Unknown;
	No integrity checks;
	Integrity checks for [select all that apply: record or message, file, directory]
		Threshold: Integrity checks applied to directory or file
		Enhanced: Integrity checks applied to record or message
		Optimum: Same as Enhanced

AP.7c: At what point in the recovery process is data integrity checked?	Unknown; No check performed; Procedural check when data is located; Automatically checked when data is located; Automatically checked prior to placing data on the restored system	Threshold: Procedural check Enhanced: Automatic check when data is located Optimum: Automatic check prior to placing data on restored system

AP.7d: How are failures of data integrity checks handled? *The answer should be consistent with the answer to PD.1.*	Unknown; Visible in automatically generated report; Application administrator notified automatically	Threshold: Visible in report Enhanced: Administrator automatically notified Optimum: Same as Enhanced
AP.8: Least Privilege for Recovery Tools. Privileges assigned to TOA tools used in recovery processes are minimized, thereby reducing potential harm from misuse or erroneous use of such tools. (Note that privilege assignments for tools used by EIIS or a third-party provider are outside the scope of this assessment. However, the least privilege principle should be applied to such tools as well.) *The answer should be consistent with AS.5.*		
Question	**Representative Answers**	**Notional Assessment Levels**
AP.8a: How are privileges assigned to TOA tools used in recovery processes?	Unknown; No TOA tools for recovery (e.g., all tools involved in recovery are provided by EIIS or by a third-party provider); No system privileges assigned to TOA recovery tools; System privileges are assigned to TOA recovery tools but not documented; System privileges assigned to TOA recovery tools specified and documented (identify where)	Threshold: No TOA tools for recovery or No system privileges assigned to TOA recovery tools *or* System privileges are assigned to TOA tools but not documented Enhanced: System privileges assigned to TOA recovery tools specified and documented Optimum: Same as Enhanced

5.6 Operational Processes (OP)

This category covers operational processes and procedures related to maintenance, backup, recovery, and status evaluation for the TOA. This category covers processes and procedures performed by TOA system staff (e.g., administrators, users) (or staff assigned to the mission or business area, or system administrators for EIIS custom applications or commercial tools) to perform recovery. These processes use the technical capabilities identified in the Backup and Recovery Technology area, for which responsibilities are typically as follows:

- [BR-SYS or BR-MBA] Backup and recovery services (including validation) for
    - Application data;
    - Software (e.g., application image, system image); and
    - Configuration data (including definition of privileges)
- [BR-EIIS or BR-3P] Validation of recovered data (in addition to any validation done by EIIS)

Support for answers to OP questions is expected to be found in operational concept documentation, procedures, or recovery handbooks / playbooks.

Table 13. Operational Processes

OP.1: Track and Maintain Critical Components. Ensure that the set of critical components are tracked and maintained for recovery.		
Question	**Representative Answers**	**Notional Assessment Levels**

OP.1a: What operational processes are used to track critical components?	Unknown;
	None;
	Inventory updated upon initial delivery of hardware and/or software;
	Inventory updated when software is updated or patched
		Threshold: Inventory updated upon initial delivery of hardware and/or software
		Enhanced: Inventory updated when software is updated or patched
		Optimum: Same as Enhanced

OP.1b: What operational processes are used to capture and maintain the critical components and their configurations?	Unknown; None; Process to capture gold copy of original (as-delivered, as initially installed) software; Process to capture gold copy of original software plus scheduled updates and configuration changes; Process to capture gold copy of software, including all updates, patches, and configuration changes; Other (specify)	Threshold: Process to capture gold copy of original software Enhanced: Process to capture gold copy of original software plus scheduled updates and configuration changes Optimum: Process to capture gold copy, including all updates, patches, and configuration changes
OP.2: Validate Critical Components. Ensure that critical components have not been corrupted and thus can be used in recovery.		
Question	**Representative Answers**	**Notional Assessment Levels**
OP.2a: What operational processes are used to validate critical components? Identify all that apply.	Unknown; None; Specialized malware scan used prior to installation of software; Standard anti-virus/ anti-malware scan run as part of maintenance prior to installing software; Forensic analysis used prior to installation of software	Threshold: Standard anti-virus/ anti-malware scan run as part of maintenance prior to installing software Enhanced: Specialized malware scan used prior to installation of software Optimum: Forensic analysis used prior to installation of software

OP.3: Validate Provenance of Critical Components. Intended to ensure the ability to track / confirm the source of the critical components.		
Question	**Representative Answers**	**Notional Assessment Levels**
OP.3a: What is the means of ensuring the authenticity of the source of the components? Identify all that apply.	Unknown; None; Procedural (e.g., visual examination of shrink-wrap or other physical delivery material, manual checking of URLs for software patches or updates); Automated review of URLs and software patching; Automated using some form of non-repudiation (e.g., digital signature) to verify receipt of software; Other (specify)	Threshold: Procedural (e.g., visual examination of shrink-wrap or other physical delivery material; Manual checking of URLs for software patches or updates Enhanced: Automated review of URLs and software patching Optimum: Automated using some form of non-repudiation (e.g., digital signature) to verify receipt of software
OP.4: Authorization of Installation of Critical Components. Ensure that the action to install a critical component is authorized before that action is taken.		
Question	**Representative Answers**	**Notional Assessment Levels**

OP.4a: What measures are taken to ensure that installation of the critical component is not done in error or without proper authorization?	Unknown;
	None;
	Procedural;
	Digital signature;
	Two-person process;
	Other (specify)
		Threshold: Procedural
		Enhanced: Digital signature
		Optimum: Two-person process

OP.5: Operational Recovery Exercises. Ensure that recovery exercises provide enough experience for operational staff, and enough detail to inform updates to SLAs or RPOs.		
Question	**Representative Answers**	**Notional Assessment Levels**

OP.5a: How frequently are recovery exercises performed?	Unknown;
	Not performed;
	Performed on an ad-hoc basis;
	Performed regularly (specify frequency);
	Performed regularly (specify frequency) and on an ad-hoc basis (e.g., based on recent threat events or intelligence)
		Threshold: Performed on an ad-hoc basis
		Enhanced: Performed regularly
		Optimum: Performed regularly and on an ad-hoc basis

OP.5b: How does the scope of the recovery exercises compare with that specified in SLAs or RPOs?	Unknown; Not compared; Procedures are in place to note differences between recovery exercises and what is in SLA; Automated processes are employed to identify and track differences between recovery exercises and what is in SLAs; Differences are reflected in updated SLAs or RPOs; Other (specify)	Threshold: Procedures are in place to note differences between recovery exercises and what is in SLAs Enhanced: Automated processes are employed to identify and track differences between recovery exercises and what is in SLAs Optimum: Differences are reflected in updated SLAs or RPOs
OP.5c: How does the recovery time from exercises compare to those specified in the SLAs?	Unknown; Not compared; Procedures are in place to note recovery time differences from exercises to those in SLA; Automated means are used to identify and track recovery time differences between exercises and those in SLA SLA is updated to reflect time differences; Other (specify)	Threshold: Procedures are in place to note recovery time differences from exercises to those in SLA Enhanced: Automated means are used to identify and track recovery time differences between exercises and those in SLA Optimum: SLA is updated to reflect time differences
OP.6: Dependence or Precedence Ordering of Recovery. Order of recovery of some components is not interchangeable. Known recovery dependency relationships enables automated recovery support.		
Question	**Representative Answers**	**Notional Assessment Levels**
OP.6a: How is the correct order for recovering components specified?	Unknown; Not specified; Captured in an informal or ad-hoc process; Captured in some formal process (e.g., in checklist, recovery handbook); Captured in some periodically (e.g., annually) updated formal process (e.g., in checklist, recovery handbook)	Threshold: Captured in an informal or ad-hoc process Enhanced: Captured in some formal process (e.g., in checklist, recovery handbook) Optimum: Captured in some periodically (e.g., annually) updated formal process (e.g., in checklist, recovery handbook)

5.7 Procedural Documentation (PD)

This area covers documentation for processes involved in recovery.

Topics to be covered in procedural documentation may include:

- How to determine the extent or severity of the TOA’s adverse state – in particular, how to determine whether bare-metal recovery is necessary.
- How to assemble the resources needed for recovery – in particular, resources needed for bare-metal recovery.

- How to restore the TOA to a minimally viable state.
- How to completely recover the TOA to a fully functional state – that is, how to reconstruct the TOA and the supporting infrastructures and upstream systems or applications on which it depends.
- Communication with downstream TOA owners, particularly those that directly depend on the TOA.
- How advanced cyber defense services, processes, and activities could interact with the TOA's recovery from an extreme or integrity event. (For example, forensic analysts could require sequestering resources, rather than allowing them to be wiped clean.)

Support for answers to PD questions is expected to be found in administrator and user manuals, handbooks, and checklists. For purposes of defining questions in the other categories, it is assumed that procedural documentation includes a Recovery Handbook. As the questions in the PD category indicate, this handbook can be non-existent or notional.

Table 14. Procedural Documentation

<table>
<tr><td colspan="3"><b>PD.1: Define and Document Recovery Processes.</b> This topic identifies expectations for Checklist and Playbook contents to measure completeness of recovery process definitions. Process areas (PAs) are based on [23], with some modifications to align with the recovery process model presented in Section 3.</td></tr>
<tr><td><b>Question</b></td><td><b>Representative Answers</b></td><td><b>Notional Assessment Levels</b></td></tr>
<tr><td>PD.1a: Which <i>process areas</i> are covered in the recovery process documentation for the TOA? Identify all that apply.</td><td>Unknown;
PA1: Preparation for Major Incidents (including processes for maintaining the currency and correctness of TOA recovery processes);
PA2: Detection, Initial Analysis, and Data Preservation;
PA3: Determination of the Incident's Extent or Severity (in particular, determination of whether the incident merits bare-metal recovery);
PA4: Containment;
PA5: Eradication;
PA6: Resource Marshalling;
PA7: Restoration to Minimally Viable State;
PA8: Reconstruction of Fully Functional State;
PA9: Post-Incident Analysis;
PA10: Coordination</td><td>Threshold: PA3, PA4, PA5, PA7, and PA8
Enhanced: Threshold + PA1, PA2, and PA10
Optimum: PA1-PA10</td></tr>
</table>

PD.1b: Which *components, functions, services, and data assets* are described in the TOA's recovery process documentation? Identify all that apply. *The level of detail for this identification will need to be consistent with the answers to DP.2.*	Unknown; TOA software components, functions, services, and data assets; Infrastructure services on which the TOA or its recovery process depends; Infrastructure functions and software components on which the TOA or its recovery process depends; Services, functions, and data flows provided by upstream systems / applications	Threshold: TOA software components, functions, services, and data assets Enhanced: Threshold + Infrastructure services Optimum: Enhanced + Infrastructure functions and software components; and Services, functions, and data flows provided by upstream systems / applications
PD.1c: How *specifically* are components, functions, and services identified in the TOA's recovery process documentation? Select all that apply. *Responses to this question should be consistent with the answers to DP.2.*	Unknown; Software identified by [specify all that apply: name, version, patch]; Functions described [in general terms, via an interface description]; Services described [in general terms, via an SLA or RTO]	Threshold: Software identified by name; Functions defined in general terms; Services described in general terms Enhanced: Threshold + at least one of the following: Software identified by name, version, and patch; Functions defined via an interface description; and Services described in terms of an SLA or RTO Optimum: Software identified by name, version, and patch; Functions defined via an interface description; and Services described in terms of an SLA or RTO
PD.1d: How specifically are roles and responsibilities for activities in the TOA's recovery process defined? *The answer should be consistent with ST.2 and ST.3.*	Unknown; Roles and responsibilities identified in general terms; Roles, responsibilities, and privileges for specific tasks are identified; Roles, responsibilities, and privileges for specific tasks are defined, consistent with organizational policy	Threshold: Roles and responsibilities identified in general terms Threshold: Roles, responsibilities, and privileges for specific tasks are identified Optimum: Roles, responsibilities, and privileges for specific tasks are defined, consistent with organizational policy

PD.1e: How is the TOA's recovery process documentation *packaged*? Select all that apply.	Unknown; Architectural / design documentation of TOA; SLAs for supporting infrastructure; SLAs for upstream systems / applications; SLAs for downstream systems / applications; Fragmented recovery process documentation (e.g., separate documentation for processes related to different threats, separate documentation for processes related to different TOA components) [specify]; Documentation of as-deployed and as-used architecture, components, and dependencies; Recovery Checklists; Unified Recovery Handbook (may include multiple checklists)	Threshold: Architectural / design documentation of TOA; SLAs for supporting infrastructure; and Fragmented recovery process documentation Enhanced: Recovery Checklists; Documentation of as-deployed and as-used architecture, components, and dependencies Optimum: Unified Recovery Handbook
PD.1f: How is the TOA's recovery process documentation kept *up-to-date*? Select all that apply.	Unknown; Updated on an ad-hoc basis; Updated in conjunction with critical component recovery testing (see IP.1); Updated in conjunction with application recovery testing (see AP.1); Updated in conjunction with recovery exercises (see OP.5); Updated at set intervals [select: quarterly, semi-annually, annually, other (specify)]	Threshold: Updated on an ad-hoc basis Enhanced: Updated at set intervals Optimum: Enhanced + Updated in conjunction with testing or exercises
PD.1g: How is the TOA's recovery process documentation kept *consistent* with recovery process documentation for supporting infrastructures and services?	Unknown; Consistency checked on an ad-hoc basis; Consistency checked as part of critical component recovery testing (see IP.1); Consistency checked as part of recovery exercises (see OP.5); Other (specify)	Threshold: Consistency checked on an ad-hoc basis Enhanced: Consistency checked as part of critical component recovery testing Optimal: Consistency checked as part of recovery exercises

PD.2: Ensure Availability and Accessibility of Recovery Documentation. Documentation – about recovery activities and about communications – can be made available to staff with recovery-related responsibilities via hardcopy, softcopy, or both.

Question	**Representative Answers**	**Notional Assessment Levels**

PD.2a: How is the TOA's recovery process documentation made available to staff who will be engaged in recovery processes? Identify all that apply.	Unknown;
	Softcopy available via (specify system – other than TOA – where documentation is stored);
	Hardcopy available at (specify location(s));
	Softcopy available via air-gapped systems (specify)
		Threshold: Softcopy available via non-TOA system
		Enhanced: Threshold + Hardcopy available
		Optimum: Enhanced + Softcopy available via air-gapped systems

PD.3: Provide Communications Plans. Ensure that there is a means of communication among staff in the event of unavailable or compromised internal communications. Call trees and contact lists can be documented (e.g., in a hardcopy handbook); they can also be pre-populated in organizational directories (e.g., via email lists or text message recipient lists, pushed to staff mobile devices) or external directories if authorized by the organization. Note that it may not be feasible to impose enterprise security controls on alternative lines of communication. Staff therefore need guidance on what types of information may be communicated using a given communications method.

Question	**Representative Answers**	**Notional Assessment Levels**

PD.3a: What communications *resources* are available to staff who will be engaged in recovery processes? Identify all that apply.	Unknown;
	Enterprise-internal communications (voice, email, Teams, etc.);
	Enterprise-external communications (e.g., cell phones, cloud-based email and/or file sharing services [specify])
		Threshold: Either enterprise-internal or enterprise-external
		Enhanced: Both enterprise-internal and enterprise-external
		Optimum: Same as Enhanced

PD.3b: What *assistance* on use of alternative lines of communications is given to staff who will be engaged in recovery processes? Identify all that apply.	Unknown;
	Documented (hardcopy) call trees;
	Documented (hardcopy) contact lists;
	Pre-populated (softcopy) call trees;
	Pre-populated contact lists
		Threshold: Documented (hardcopy) call trees or contact lists
		Enhanced: Threshold + Pre-populated (softcopy) call trees and contact lists
		Optimum: Same as Enhanced

PD.3c: What *guidance* on use of alternative lines of communications is given to staff who will be engaged in recovery processes? Identify all that apply.	Unknown;
	Informal guidance;
	Documented restrictions on what is allowed to be communicated using a given method
		Threshold: Informal
		Enhanced: Documented restrictions on what is allowed to be communicated with a given method

5.9 Staff Support (ST)

This category covers the staff resources and training involved in executing a successful recovery.

Table 15. Staff Support

<table>
<tr><td colspan="3"><b>ST.1: Support to Staff During Recovery.</b> This topic involves automated support to staff involved in recovery. Automation can ensure that actions taken by staff to recover the TOA to a minimally viable state are complete and consistent. As described in Section 3, staff actions can be characterized in terms of their purpose: Diagnose (understand the state of the TOA and the resources on which it directly depends); Assemble (identify and gather the resources needed for recovery); and Restore (recover TOA data, functions, and services to a minimally viable state).</td></tr>
<tr><td><b>Question</b></td><td><b>Representative Answers</b></td><td><b>Notional Assessment Levels</b></td></tr>
<tr><td>ST.1a: How completely are the actions involved in recovery to a Minimally Viable State specified?
<i>The answer should be consistent with answers to PD.1.</i></td><td>Unknown;
Incomplete – some actions are known for Diagnose, Assemble, and/or Restore;
Very Partial – many actions are known for Diagnose, Assemble, and/or Restore;
Partial – all of the actions are known for one or more of Diagnose, Assemble, and Restore;
Comprehensive – all actions for Diagnose, Assemble, and Restore are fully defined</td><td>Threshold: Incomplete
Enhanced: Very Partial or Partial
Optimum: Comprehensive</td></tr>
<tr><td>ST.1b: How much automated support is provided for the specified actions?
<i>The answer should be consistent with AP.2 and AP.4.</i></td><td>Unknown;
Minimal, requiring staff knowledge of and expertise in using TOA-internal tools and capabilities which are not specifically oriented toward recovery;
Partial, requiring staff expertise in using tools identified as recovery-supportive;
Extensive, requiring staff familiarity with tools identified as recovery-supportive</td><td>Threshold: Minimal
Enhanced: Partial
Optimum: Extensive</td></tr>
<tr><td>ST.1c: For actions which are not automated, how are manual processes, procedures, and instructions documented?
<i>The answer should be consistent with answers to PD.1.</i></td><td>Unknown;
Not documented;
Documented informally;
Documented in a handbook or checklist</td><td>Threshold: Documented informally
Enhanced: Documented in a handbook or checklist
Optimum: Same as Enhanced</td></tr>
</table>

ST.2: Recovery Roles. Ensure that definition of separate or distinct roles and responsibilities related to backup and recovery is consistent with the principle of least privilege, and reduces risk of misuse or erroneous use of backup and recovery functions. Staff must be able to assume recovery roles quickly in the case of time sensitive recovery. A policy, supported by mechanisms and procedures that allow for privileges to be granted quickly or functions to be carried out quickly, enables staff to assume roles in an emergency.

Question	**Representative Answers**	**Notional Assessment Levels**
ST.2a: How are roles and responsibilities related to backup and recovery specified?	Unknown; No separate backup or recovery roles (backup and recovery responsibilities are part of TOA administration); Specific roles identified for backup and recovery but functions are not specified; Specific roles are affiliated with backup and recovery functions (specify roles and functions)	Threshold: Specific roles identified but functions not known Enhanced: Specific roles are identified for backup and recovery but functions are not specified Optimum: Specific roles are affiliated with specific backup and recovery functions
ST.2b: How do policies and procedures ensure that each recovery role can be filled during an emergency situation?	Unknown; No separate recovery roles; No policies/procedures exist; Policies / procedures exist to ensure that recovery roles can always be filled and there are mechanisms to quickly reassign privileges to ensure that recovery functions can be executed by a person temporarily filling the recovery role; Policies / procedures exist to assign multiple people to recovery roles and ensure that one of them is available all the time	Threshold: Policies / procedures exist to ensure that recovery roles can always be filled and there are mechanisms to quickly reassign privileges to ensure that recovery functions can be executed by a person temporarily filling the recovery role Enhanced: Policies / procedures exist to assign multiple people to recovery roles and ensure that one of them is available all the time Optimum: Same as Enhanced

ST.3: Training. Role-specific training for staff filling recovery roles enables them to execute the recovery actions and use recovery functions.

Question	**Representative Answers**	**Notional Assessment Levels**
ST.3a: How is recovery training provided to personnel filling roles in the recovery process?	Unknown; Ad-hoc on-the-job training; Review of documents and briefings; Training in a lab environment; Other (specify)	Threshold: Ad-hoc on-the-job training Enhanced: Review of documents and briefings Optimum: Training in a lab environment

ST.3b: What is the frequency of the training?	Unknown;
	No required frequency;
	When changes are made to the recovery process;
	Periodically (specify frequency: annually, semiannually, quarterly, monthly, other)
		Threshold: When changes are made to the recovery process and Annually
		Enhanced: When changes are made to the recovery process and Semi-annually
		Optimum: When changes are made to the recovery process and Quarterly or monthly

ST.3c: What training is given to all staff who could fill a given recovery role?	Unknown; Minimum training for staff who serve as backup to primary recovery staff; Common training for all staff who might fill a given recovery role	Threshold: Other roles are cross trained with “lesser” training to fill the recovery role Enhanced: Common training for all staff who might fill a given recovery role Optimum: Same as Enhanced

5.10 Programmatic Support (PS)

This area covers programmatic considerations (e.g., financial resources, supply chain) needed for recovery.

Table 16. Programmatic Support

<table>
<tr><td colspan="3"><b>PS.1: Ability to Estimate Recovery Cost.</b> Recovery cost typically includes level of effort (LOE) for staff performing recovery tasks and dollar costs for acquiring replacement components.[31]</td></tr>
<tr><td><b>Question</b></td><td><b>Representative Answers</b></td><td><b>Notional Assessment Levels</b></td></tr>
<tr><td>PS.1a: How are recovery costs from an extreme cyber event estimated?</td><td>No estimate;
Estimated based on general cybersecurity literature;
Estimated based on domain or sector literature;
Estimated based on recovery exercises / drills;
Estimated using a standardized calculator developed for the organization</td><td>Threshold: Estimated based on general cybersecurity literature
Enhanced: Estimated based on domain or sector literature
Optimum: Estimated based on recovery exercises / drills or Estimated using a standardized calculator developed for the organization</td></tr>
<tr><td colspan="3"><b>PS.2: Ability to Resource Recovery.</b> Ensure that budgeting and resource planning include ensuring resources for recovery from cyber events.[32]</td></tr>
<tr><td><b>Question</b></td><td><b>Representative Answers</b></td><td><b>Notional Assessment Levels</b></td></tr>
</table>

[31] For a commercial institution, recovery cost can also include lost revenue during the recovery period. Recovery cost can be offset by insurance; the estimate of expected recovery cost drives the amount of insurance.

[32] See the discussion of risk reserves in Section 3.5 of NISTIR 8286 [16]. Note that staffing of recovery roles can involve employing a qualified third party. Note also that budgeting can incorporate expected pay-outs from cyber insurance.

PS.2a: How are recovery costs from an extreme cyber event represented in budgeting?	Not included in budget; Implicitly included in operating budget via stated assumptions; Explicitly represented in operating budget as a line item	Threshold: Implicitly included in operating budget via stated assumptions Enhanced: Explicitly represented in operating budget as a line item Optimum: Same as Enhanced
PS.2b: How do policies and procedures ensure that each recovery role can be filled during an emergency situation?	Unknown; No separate recovery roles; No policies/procedures exist; Policies / procedures exist to ensure that recovery roles can always be filled and there are mechanisms to quickly reassign privileges to ensure that recovery functions can be executed by a person temporarily filling the recovery role; Policies / procedures exist to assign multiple people to recovery roles and ensure that one of them is available all the time	Threshold: Policies / procedures exist to ensure that recovery roles can always be filled and there are mechanisms to quickly reassign privileges to ensure that recovery functions can be executed by a person temporarily filling the recovery role Enhanced: Policies / procedures exist to assign multiple people to recovery roles and ensure that one of them is available all the time Optimum: Same as Enhanced
PS.2c: How do contracts with external service providers ensure that they provide adequate support to recovery? Select all that apply. If answers depend on the service provider, specify separately.	Unknown; Contracts specify service level agreements related to recovery from incidents; Contracts specify service provider's participation in or support for testing or exercise of recovery; Contracts specify the organization's relative priority among service provider's customers for restoration	Threshold: Contracts specify service level agreements related to recovery from incidents Enhanced: Threshold + Contracts specify service provider's participation in or support for testing or exercise of recovery Optimum: Enhanced + Contracts specify the organization's relative priority among service provider's customers for restoration
PS.3: Supply Chain Assurance. Reduce supply chain risk for critical components. Recovery may involve utilizing components in the supply chain to rebuild/replace those that have been compromised. Being able to assess the integrity of the supply chain components helps in the determination of how much of the system can be trusted.		
Question	**Representative Answers**	**Notional Assessment Levels**

PS.3a: What processes are in place to ensure the integrity of the supply chain of critical components?	Unknown; No processes in place; Procedural spot checks of supply chain; Require suppliers to validate integrity of application (e.g., via digital signature); Require suppliers to provide a Software Bill of Materials (SBOM) or Hardware Bill of Materials (HBOM); Other (specify)	Threshold: Procedural spot checks of supply chain Enhanced: Require suppliers to validate integrity of application (e.g., via digital signature) Optimum: Require suppliers to provide an SBOM or HBOM
PS.3b: How far down the supply chain do the integrity assurance measures apply? If a TOA owner or system administrator needs a clean copy of a software component, how far into the supply chain can they reach?	Unknown; Just to primary supplier; Down one level to sub-contractor; Down all the way (e.g., via a Software Bill of Materials or SBOM); Other (specify)	Threshold: Primary supplier Enhanced: Primary supplier and direct sub-contractors Optimum: Entire supply chain (e.g., via an SBOM)
PS.3c: What processes are in place to ensure the availability of critical components?	Unknown; Ongoing relationships with primary suppliers; Established relationships with secondary suppliers; War-time reserve of spare components; War-time reserve of alternate components; Other (specify)	Threshold: Ongoing relationships with primary suppliers Enhanced: Threshold + Established relationships with secondary suppliers Optimum: Enhanced + War-time reserve of spare components

6 Conclusion

A review of the literature on recovery from ransomware and other forms of destructive malware revealed that:

- Concern for ransomware and other forms of destructive malware is elevated, and the expectation is that this concern will be high for the foreseeable future.
- Guidance on ransomware recovery continues to evolve, particularly as concepts for using third-party service providers are evolving.
- Gaps in existing guidance on ransomware recovery include:
    - Lack of a well-defined model of recovery-related states and state transitions.
    - Lack of specific consideration for “bare-metal” or clean-slate recovery, which can include retrieval of components from a reserve or even acquisition of fresh components from suppliers.
    - Lack of a sector-neutral framework for recovery of high-volume time-sensitive transaction processing.

This document presents a framework and a representative set of criteria for assessing essential clean-slate cyber recovery (ECCR), for large organizations with time-critical functions or high volumes of time-sensitive transaction processing. ECCR is a narrowly-scoped capability, which must be understood in the context of an organization’s overall contingency and continuity of operations planning. *Essential* limits the scope to recovery of mission-essential or business-critical functions or services (including the data needed to perform those functions or provide those services) to a minimally viable (as contrasted with a fully functional) state. *Clean-slate* limits the scope to recovering, restoring, or reconstituting functions from “bare metal,” and explicitly excludes failover to a hot standby system as well as partial recovery efforts such as restoring selected files or applications. *Cyber* refers to the focus on recovery from extreme cyber event such as a destructive malware attack. ECCR is an element in a larger incident response process, which includes containing the effects of an attack, preserving evidence, expunging malware, performing post-incident analysis, and coordinating both within the organization and with external organizations.

The framework, criteria, and concept of use are designed to be tailorable and extensible, driven by an organization’s enterprise risk management strategy and translated into terms meaningful to the organization and its critical infrastructure sector. They are intended to enable an organization to assess its capabilities for ECCR and to identify capability gaps for consideration in its cyber risk management strategy. In addition, an ECCR assessment can help the organization discover disconnects between sub-organizations – inconsistent assumptions about capabilities, priorities of and relationships between events in response and recovery efforts, resource availability (e.g., staffing), and how long specific activities can be expected to take. Future evolution could include extending the concept of ECCR to general enterprise information technology environments and to architectures which include operational technology (OT) or Internet of Things (IoT) devices as well as information technology (IT). Extensions to industrial control systems (ICS) or IoT applications would include safety implications of ECCR practices and technologies.

Appendix A Glossary

Term	**Definition**
Adverse State	A state (of a TOA) in which a TOA is unacceptably degraded, unacceptably disrupted, or denied, disabled, or destroyed.
Assemble	(In the context of recovery) Locate resources necessary to reconstruct the system or to bring the system from an unacceptably degraded or disrupted state; obtain those resources or make them accessible. *Resources to be assembled include not only information resources which are or can be made part of the system, but also infrastructure elements (e.g., servers) and services, and staff with the requisite knowledge and authorities to perform recovery tasks.*
Application	A collection of software components which collectively provide a specific function or set of functions. *Note that FIPS 201-3 defines application as "a hardware/software system implemented to satisfy a particular set of requirements"* [40].
Bare Metal / Clean Slate Recovery	Recovery of a TOA, which may consist of multiple machines (physical or virtual), operating systems, applications, and supporting software, starting from wiped-clean instances of those machines, as well as recovery of necessary data, to a minimally viable state.
Business Application	An application designed to perform a business function. *A business application is specific to a business function, as contrasted with an application which performs a function or provides a service used by multiple business or mission areas (e.g., word processing).*
Business-Critical Function *or* Business-Critical Service	An organizational function or service that must be performed, or an organizational responsibility that must be fulfilled, in order for the organization to be considered operational. *Identification of business-critical functions or services is crucial to contingency planning.* [20]
Component	A discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware. [7] *Also referred to as a system element, i.e., "a discrete part of a system that can be implemented to fulfill specified requirements"* [41].
Constituent Element	A system element or component, viewed from the perspective of the system or TOA of which it is a part. *The term is used to emphasize the relationship between the component and the system or TOA as a whole. The use in this document is intended to be consistent with usage in NIST SP 800-160 Vol. 1* [42] [41].

Term **Definition**

Contingency Plan

A coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption. [2]

Contingency planning generally includes one or more of the following approaches to restore disrupted services:

- *Restoring information systems using alternate equipment;*
- *Performing some or all of the affected business processes using alternate processing (manual) means (typically acceptable for only short-term disruptions);*
- *Recovering information systems operations at an alternate location (typically acceptable for only long–term disruptions or those physically impacting the facility); and*
- *Implementing of appropriate contingency planning controls based on the information system's security impact level.* [2]

Critical Component

A system element that, if compromised, damaged, or failed, could cause a mission or business failure. [43]

A critical component is a component the unavailability of which makes the execution of an essential function or the provision of a critical service impossible.

Critical Function or Service

A function or service which performs or supports mission-essential functions or business-critical functions, is necessary to meet security or safety requirements, or which has been determined to be critical to other systems or applications.

A critical function or service is identified via criticality analysis, in contrast to an essential function.

Criticality Analysis

An end-to-end functional decomposition of a system to identify critical functions, services, components, and resources. Includes identification of system missions, decomposition into the functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions. Criticality is assessed in terms of the impact of function or component failure on the ability of the component to complete the system missions(s). ([44], adapted)

"System" here can refer to a socio-technical system, including people and processes as well as technology. Thus, "resources" can include personnel, with associated expertise, roles and responsibilities, and privileges or authorities. "System" can refer to a system-of-systems. In a business context, criticality analysis can be identified with a business impact analysis (BIA) [2].

Cyber Resource

An information resource that creates, stores, processes, manages, transmits, or disposes of information in electronic form, and that can be accessed via a network or using networking methods. [9]

Term	**Definition**
Cyber Threat	A threat that involves the use of cyberspace, either as a vector (i.e., cyberspace is used in the execution of a threat scenario) or as a target (i.e., the threat results in harm to cyber resources). *In general, the term is used to refer to an attacker or adversary, to a threat scenario involving cyberspace initiated by an adversary, or to an adversary's tactics, techniques, and procedures (TTPs).* *Note: A commonly used (or adapted) definition is* *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, modification of information, and/or denial of service.* [44] *However, this definition applies to a threat event or a threat scenario ("circumstance or event"), and is not broad enough to include threat sources – in particular, threat actors.*
Data Asset	Any entity that is comprised of data. For example, a database is a data asset that is comprised of data records. A data asset may be a system or application output file, database, document, or web page. [44], as cited in the NIST Security Glossary.
Degraded	A state (of a resource) in which its functioning, performance, or quality is below its objective or nominal level. *Applicable to data, a system, application, mission or business function, TOA, or constituent element of a TOA.*
Denied	A state (of a resource) in which it is prevented from performing its required functions. *Applicable to a system, application, mission or business function, TOA, or constituent element of a TOA.*
Destroyed	A state (of a resource) in which it cannot be brought to perform any function or cannot be used to support any function. *Applicable to data, a system, application, mission or business function, TOA, or constituent element of a TOA.*
Destructive Malware	Malware that makes cyber resources unusable, and which may also cause damage to physical resources controlled by cyber resources.
Determined	A state (of a system or TOA) in which the states of the constituent elements (including software and data) and of supporting infrastructures are known. *The cause of the adverse state may be known, assumed, or unknown. Knowledge of the states of constituent elements is needed to enable the resources needed for restoration-readiness to be identified.*

Term	**Definition**
Diagnose	Determine the health and status of a system’s information resources, as well as (i) those system-external information resources, infrastructure components, systems, and services on which the system directly depends and (ii) those system-external resources on which the system indirectly depends. *Knowledge of the status of system-external resources is crucial to planning the steps to assemble system resources and restore the system to a minimally viable level of operation.*
Disabled	A state (of a system or of a constituent element of a system) in which it cannot perform any of its required functions.
Disrupted	A state (of a system or of a constituent element of a system) in which its performance of required functions is interrupted intermittently or for an unpredictable period.
Essential Clean-slate Cyber Recovery	Bare metal / clean slate recovery of essential mission or business functions to a minimally viable state. *Essential clean-slate cyber recovery provides essential recoverability from an extreme integrity event to a TOA.*
Essential Function	A function or task an organization must perform, or a responsibility an organization must fulfill, in order to be considered operational. *Essential functions include business-critical functions (functions that are essential from a business perspective) and mission essential functions (functions that are essential from a mission perspective). For Federal Executive Branch organizations, essential functions are those Government functions that have been identified as mission essential functions (MEFs), primary mission essential functions (PMEFs), or national essential functions (NEFs)* [45].
Essential Recoverability	The ability to recover, restore, or reconstitute essential mission or business functions. *Recovery of essential functions includes recovery or reconstitution of application data. The concept of essential recoverability is applicable to critical infrastructure sectors, organizations, missions or business areas, and systems, independent of the disruption from which recovery is needed and of whether any cyber resources are involved.*
Extreme Event	An event which causes a system, a TOA, an infrastructure, or a set of these to be denied, disabled, or destroyed.
Extreme Integrity Event	An event which destroys a system or TOA, or which has the consequence that no part of the system can *a priori* be assumed to be trustworthy. *Destructive malware (e.g., ransomware) is intended to create an extreme integrity event.*
Failover	The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby system upon the failure or abnormal termination of the previously active system. [7]
Fully Functional	A state (of a TOA) in which the TOA performs all its required functions at the objective or normative level. *The functions and resources used to achieve the state may or may not be the same as those employed prior to disruption and recovery.*

Term **Definition**

Gold Copy

A copy for which the provenance can be established and the quality (correctness, completeness, and/or absence of unauthorized or erroneous modification) of which can be validated.

A gold copy can be made of software, firmware, or data. Data for which a gold copy can be made include application data (e.g., files, databases) or transaction data (e.g., transaction records), enduring mission or business data (e.g., key parameters for mission or business processes), and configuration data.

Information Resource

A resource consisting of one or more of the following: hardware, firmware, software, data, and communications.

A key property of an information resource is its overall quality, which can be expressed in terms of one or more specific properties, such as correctness (e.g., consistency with an authoritative source), completeness (e.g., no temporal gaps), internal consistency, and having been created or modified only by an authorized entity (e.g., provenance).

Integrity Event

An event which reduces the quality of one or more information resources.

Depending on its scope (set of information resources affected) or severity (whether the quality is reduced to such an extent that a resource cannot be used or cannot be relied on), an integrity event can result in a system or system component being unacceptably degraded, denied, disabled, or destroyed.

Minimally Viable State (or Minimum Viable State)

A state (of a TOA) in which the TOA performs its critical functions to at least the minimal level of performance required for those functions.

In this state, functioning may be degraded or disrupted, but not to an unacceptable level. The requirements defining the minimum level of performance include security and safety requirements. Minimum viable state is a technology concept. It can be specified in terms of performance requirements. Depending on the nature of the TOA, it can also be specified via Service Level Agreements.

Minimum Viable Product

The minimum acceptable product of a business line or business function (in terms of data it produces or transactions it handles per unit time), which can be identified with a minimum set of critical functions, operating at a minimum level of performance.

Minimum viable product is a business concept. It can be specified via Service Level Agreements.

Mission Essential Function

A function or task an organization or system must perform, or a responsibility an organization must fulfill, in order to accomplish its mission.

For Federal Executive Branch organizations, MEFs are "essential functions directly related to accomplishing the organization's mission as set forth in statutory or executive charter" [45].

Reconstitute

Return a system to a fully operational state.

Reconstitution includes the deactivation of interim system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored system capabilities, reestablishment of continuous monitoring activities, system reauthorization (if required), and activities to prepare the system and organization for future disruptions, breaches, compromises, or failures. [7]

Term	**Definition**
Recoverability	The ability of an organization, mission or business function, system, resource, or set of resources to be returned to a minimally viable or fully functional state.
Recovery Point Objective (RPO)	The point in time, prior to a disruption or outage, to which mission / business process data must be recovered. [2] *An RPO can be specified for an enterprise, a mission or business area, a mission function or business function, or an application.* *The RPO can also be specified in terms of the maximum amount of data (e.g., number of transactions, number of records) which can be lost. The specification of the point of time is then computed using a nominal or objective level of functioning.* *The RPO is used to determine the frequency of incremental backups.*
Resource	(noun) A separably identifiable and manageable asset which can be used to perform or support a function. *Resources include hardware, firmware, software, data, and communications ("cyber resources" or "information resources"), as well as personnel (with appropriate training and authorities), materiel, and money.* (verb) Provide (a person, mission or business function, or organization) with materials, money, staff, and other assets necessary for effective operation.
Restoration-Ready	A state (of a TOA) in which all resources needed to return the TOA to a minimally viable state have been identified and put in place. *Note that these include not only resources which are part of the system itself, but also resources which are provided by supporting infrastructures.*
System	A separably managed set of resources which collectively perform a set of functions or provide a set of services (working definition) Combination of interacting elements organized to achieve one or more stated purposes [42] *A system can be decomposed into constituent system elements.* [42] [41] *A* system *is an arrangement of parts or elements that together exhibit a behavior or meaning that the individual constituents do not.* [41]
Target of Assessment (TOA)	A separably managed resource or set of resources for which recoverability is to be assessed. *A TOA can be, for example, an application, a set of applications, a business function, a system, or a mission or business area. A TOA is made up of constituent elements, including data assets as well as components.*
Unacceptably Degraded or Disrupted	A state (of a TOA) in which some essential functions or data are unavailable or cannot meet their performance requirements *or* the system cannot meet its SLAs. *Degradation refers to a decrease in level of service or functioning. Disruption refers to intermittent gaps in a service or function.* *This may be due to disruption or degradation of a supporting infrastructure, or to a non-critical resource being disabled or destroyed.*
War-Time Reserve	A reserve of critical components, both special-purpose and acquired, for use in a crisis situation. [9]

Appendix B Acronyms

AP	Application Processes (criteria)
AS	Architectural Support (criteria)
ATO	Approval to Operate
BCF	Business Critical Function
BIA	Business Impact Analysis (or Assessment)
BIOS	Basic Input / Output System
BM/CSR	Bare Metal / Clean Slate Recovery
BR	Backup and Recovery Technology (criteria)
CISA	Cybersecurity and Infrastructure Security Agency
CONOPS	Concept of Operations
COOP	Continuity of Operations *or* Continuity of Operations Plan
CRR	(CISA) Cyber Resilience Review
CSRM	Cybersecurity Risk Management
DBMS	Database Management System
DP	Dependencies (criteria)
DTCC	Depository Trust and Clearing Corporation
ECCRA	Essential Clean-slate Cyber Recoverability Assessment
EIIS	Enterprise Information Infrastructure Services
ERM	Enterprise Risk Management
ESB	Enterprise Service Bus
FSSCC	Financial Services Sector Coordinating Council
HBOM	Hardware Bill of Materials
IaaS	Infrastructure as a Service
IATA	International Air Transport Association
ICAM	Identity, Credential, and Access Management
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IOC	Initial Operational Capability
IoT	Internet of Things

IP	Infrastructure Processes (criteria)
ISO	International Standards Organization
ISSA	Information Systems Security Association
IT	Information Technology
LOE	Level of Effort
MBA	Mission or Business Area
MBR	Master Boot Record
MEF	Mission Essential Function
MIA	Mission Impact Analysis or Assessment
MIL	(CRR) Maturity Indicator Level
MSSP	Managed Security Services Provider
MTD	Maximum Tolerable Downtime
MTO	Maximum Tolerable Outage
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NIST SP	NIST Special Publication
OP	Operational Processes (criteria)
OS	Operating System
OT	Operational Technology
PaaS	Platform as a Service
POC	Point of Contact
PS	Programmatic Support (criteria)
RAC	Recovery Assessment Criteria
RACI	Responsible, Accountable, Consulted, and Informed
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RT	Recoverability Time
SaaS	Software as a Service
SBOM	Software Bill of Materials
SCM	(CRR) Service Continuity Management
SLA	Service Level Agreement

ST	Staff Support (criteria)
TOA	Target of Assessment
TTX	Tabletop Exercise
VPN	Virtual Private Network
WORM	Write Once, Read Many

References

[1] CISA, "CISA Insights: Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats," 18 January 2022. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/CISA_Insights-Implement_Cybersecurity_Measures_Now_to_Protect_Against_Critical_Threats_508C.pdf.

[2] NIST, "NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems," 11 November 2010. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf. [Accessed 19 May 2011].

[3] NIST, "NIST SP 800-61, Rev. 2: Computer Incident Handling Guide," August 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

[4] IATA, "Compilation of Cyber Security Regulations, Standards and Guidance Applicable to Civil Aviation, Edition 1.0," August 2020. [Online]. Available: https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/compilation_of_cyber_regulations_standards_and_guidance_1.0.pdf.

[5] NERC, "Reliability Guidelines, Security Guidelines, Technical Reference Documents, and White Papers," NERC Reliability and Security Technical Committee (RSTC), 2022. [Online]. Available: https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx.

[6] NIST, "Draft NIST SP 800-40 Rev. 4, Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology," November 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4-draft.pdf.

[7] Joint Task Force, "NIST SP 800-53R5, Security and Privacy Controls for Information Systems and Organizations," 10 December 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[8] NIST, "NIST SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops," July 2013. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

[9] NIST, "NIST SP 800-160 Vol. 2 Rev. 1, Developing Cyber Resilient Systems: A Systems Security Engineering Approach," December 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf.

[10] NIST, "NIST SP 800-184, Guide for Cybersecurity Event Recovery," December 2016. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf.

[11] NIST, "NIST SP 800-209, Security Guidelines for Storage Infrastructure," 27 October 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-209.pdf.

[12] NIST, "NIST SP 1800-25, Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events," December 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-25.pdf.

[13] NIST, "NISTIR 1800-26, Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events," December 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-26.pdf.

[14] NIST, "NIST SP 1800-11, Data Integrity: Recovering from Ransomware and Other Destructive Events," September 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-11.pdf.

[15] NIST, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," 16 April 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[16] NIST, "NISTIR 8286, Integrating Cybersecurity and Enterprise Risk Management (ERM)," 13 October 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf.

[17] NIST, "NISTIR 8286A, Identifying and Estimating Risk for Enterprise Risk Management," November 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8286A.pdf.

[18] NIST, "NISTIR 8286B, Prioritizing Cybersecurity Risk for Enterprise Risk Management," February 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8286B.pdf.

[19] NIST, "NISTIR 8286C, Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight (DRAFT)," 26 January 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8286C-draft.pdf.

[20] NIST, "NISTIR 8374, Cybersecurity Framework Profile for Ransomware Risk Management," 23 February 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8374.pdf.

[21] CISA and MS-ISAC, "Ransomware Guide," September 2020. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf.

[22] CISA, "Handling Destructive Malware - Security Tip ST13-03," 1 February 2021. [Online]. Available: https://www.cisa.gov/tips/st13-003.

[23] CISA, "Cybersecurity Incident & Vulnerability Response Playbooks: Cybersecurity Incident Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems," November 2021. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.

[24] CISA, "Assessments: Cyber Resilience Review (CRR)," [Online]. Available: https://us-cert.cisa.gov/resources/assessments.

[25] CISA, "CISA Tabletop Exercise Package – Ransomware," 9 September 2020. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/CISA%20Tabletop%20Exercise%20Package_Ransomware%2020200909%20v00_508_0.docx.

[26] CISA, "CISA Tabletop Exercise Package - Ransomware - Third Party Vendor," 9 September 2020. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/CISA%20Tabletop%20Exericse%20Package_Ransomware%20Third%20Party%20Vendor%2020200909_508.docx.

[27] ISO/IEC, "ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements," 2013.

[28] ISO, "ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements," 2019. [Online]. Available: https://www.iso.org/obp/ui#iso:std:iso:22301:ed-2:v1:en.

[29] Financial Services Sector Coordinating Council (FSSCC), "Business Services Resilience and Restoration: Building Operationally Resilient Business Services in the Financial Sector," 8 April 2019. [Online]. Available: https://fsscc.org/wp-content/uploads/2021/02/FSSCC_Operational_Resilience_White_Paper_08April2019.pdf.

[30] DTCC and Oliver Wyman, "Large-Scale Cyber Attacks on the Financial System: A Case for Better Coordinated Response and Recovery Strategies," March 2018. [Online]. Available: https://www.dtcc.com/~/media/Files/Downloads/WhitePapers/Cyber-White-Paper-DTCC-OW.pdf.

[31] Financial Stability Board, "Effective Practices for Cyber Incident Response and Recovery," 19 October 2020. [Online]. Available: https://www.fsb.org/wp-content/uploads/P191020-1.pdf.

[32] Industry Working Group, "Cyber Threats and Data Recovery Challenges for FMIS," September 2021. [Online]. Available: https://www.dtcc.com/-/media/Files/PDFs/White-Paper/Cyber-Threats-and-Data-Recovery-Challenges-for-FMIs.pdf.

[33] FFIEC, "Joint Statement: Destructive Malware," March 2015. [Online]. Available: https://www.ffiec.gov/press/PDF/2121759_FINAL_FFIEC%20Malware.pdf.

[34] Dell, "Dell EMC PowerProtect Cyber Recovery Solution Guide," September 2021. [Online]. Available: https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.

[35] Dell, "White Paper: Recovering from a Destructive Cyber Attack," March 2020. [Online]. Available: https://www.delltechnologies.com/asset/nl-be/products/storage/industry-market/recovering-business-destructive-cyber-attack.pdf.

[36] IBM, "IBM Resiliency Orchestration with Cyber Incident Recovery," 20 November 2020. [Online]. Available: https://www.ibm.com/downloads/cas/40ZB5OEV.

[37] IBM, "Learn about the Bare Metal Restore plug-in," 1 August 2019. [Online]. Available: https://cloud.ibm.com/docs/Backup?topic=Backup-BMRplugin.

[38] MSP360, "Full System Backup and Recovery," 14 September 2021. [Online]. Available: https://www.msp360.com/download/whitepapers/full-system-backup-and-recovery.pdf.

[39] Microsoft, "Bare Metal Recovery," 25 October 2021. [Online]. Available: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/bare-metal-recovery?view=windows-11.

[40] NIST, "FIPS 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors," January 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-3.pdf.

[41] NIST, "Draft NIST SP 800-160 Vol. 1 Rev. 1, Engineering Trustworthy Secure Systems," January 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1-draft.pdf.

[42] NIST, "NIST SP 800-160 Vol. 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems (including updates as of 3-21-2018)," 15 November 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf.

[43] NIST, "NIST SP 800-161, Supply Chain Risk Management Practices for Federal Systems and Organizations," 8 April 2015. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

[44] CNSS, "Committe on National Security Systems (CNSS) Glossary (CNSS Instruction No. 4009)," 26 April 2015. [Online]. Available: https://www.cnss.gov/CNSS/openDoc.cfm?hldYMe6UHW4ISXb8GFGURw==.

[45] FEMA, "Federal Continuity Directive 2: Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process," 13 June 2017. [Online]. Available: https://www.fema.gov/sites/default/files/2020-07/Federal_Continuity_Directive-2_June132017.pdf.

[46] Microsoft, "Human-operated ransomware," Microsoft Security Best Practices, 27 October 2021. [Online]. Available: https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware.

[47] CISA, "CISA Fact Sheet: Rising Ransomware Threat to OT Assets," 9 June 2021. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf.

[48] NIST, "NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities," September 2006. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf.

[49] Director of Defense Research and Engineering (Advanced Capabilities), "Department of Defense Cyber Table Top Guide," 16 September 2021. [Online]. Available: https://ac.cto.mil/wp-content/uploads/2021/09/DoD-Cyber-Table-Top-Guide-v2.pdf.