Cyber Incident Response (CIR) Planning Checklist

Worked Example of Completing an Item in the CIR Planning Checklist

Addendum Purpose and Use: This addendum provides a general procedure for completing checklist items in the CRL Cyber Incident Response (CIR) Planning Checklist. It describes the example activities of each step in the procedure for a representative checklist item.

Illustrative Guidance Only: The content below is illustrative of the steps to be followed to achieve the selected checklist item. Assumptions are made for the purpose of the example, but these assumptions are not intended to narrow the solution options in an actual case. All of the content in this example is illustrative only, not prescriptive. The selected example is more complex and costly than most checklist items.

Exhibit 1. General Procedure for Addressing Checklist Items

Follow this general procedure for completing checklist items:

1. Determine the scope and specific objectives of the task.
2. Coordinate with other stakeholders in the organization to get buy-in, advice, engagement, partnership, and support.
3. Identify the resources needed to complete the checklist item (e.g., tools, subject matter experts, functional experts, software applications, IT infrastructure, funding).
4. Define a schedule of milestones for completing the checklist item.
5. Design the solution that addresses the requirements of the checklist item.
6. Implement the solution.
7. Complete the documentation of the solution and procedures developed.
8. Train personnel on the solution and its procedures as required.

Because the items of the CRL Cyber Incident Response (CIR) Planning Checklist vary widely, this procedure is designed as a reference that may be modified based on the nature of each item and the specific conditions at the county.

Reference to Exhibit 1: The description below follows the general procedure of Exhibit 1, outlining what should be done to accomplish the checklist item; it does not perform the work itself. That is, the example does not develop the design, write the policy, develop the procedures, nor implement the technical solution – it only provides guidance to implementers by outlining what is needed for each of the steps in Exhibit 1.

Project-Specific Detail Required: In an actual case, each step in Exhibit 1 would require focused effort, as would the overall management of the project. Implementing and IT solution is always very specific to the target environment. In an actual case, more detail would be required than what is contained in the example.

Example: Data Backup Capability

- ○ 6. **PR.DS-11** Create, protect, maintain, and test backups of data, including network and system log data.
    a. Test data and system restoration on a regular basis, adjusting test objectives to cover a broad range of scenarios over time. Include testing of processes for verification of data integrity. (supports **RC-RP-03**)

Scope and objectives

While the checklist item is written as an operational activity, this example is based on the assumption that the capability to create, protect, maintain, and test restoration of backups is not fully implemented and that the capability will first have to be built or improved. The example elaborates on the steps outlined in Exhibit 1 for this particular checklist item. Completion of these steps and operationalizing the capability would be necessary to fully address the checklist item.

1. **Research the Current Backup Environment:** Research the current data backup environment to develop an understanding of:

    - **Enterprise Data Types for Backup**: Determine the types of enterprise data to be included in the backup strategy such as official business data, confidential financial data, Personally Identifiable Information (PII), protected intellectual capital, classified government data.
    - **Current Backup Capabilities**: Evaulate the current backup capability, including the technical architecture, key technical components (e.g., primary and secondary data centers, cloud storage, disaster recovery sites, vendor/partner sites, and archival storage facilities), the deployed technology and infrastructure, as well as backup, test, and restore procedures.
    - **Existing Data Protection Policies**: Examine the existing policy environment for data protection and backup. This includes the enterprise Data Protection Policy, which establishes many data protection requirements (e.g., data classification framework and data labeling, handling, and retention requirements). Other relevant documentation that may exist includes:
        - **Approach and Requirements:** Definition of the top-level data backup approach and requirements (e.g., on-premises, hybrid, hosted, cloud-native solutions), infrastructure-as-a-service (IaaS), managed services across the backup estate, and other features, considering:
            - How the backup approach compares with the basic 3-2-1 strategy given the many options that IaaS and cloud storage open up. The 3-2-1 strategy calls

for three copies of the data (production data plus two more copies), stored on two different types of media, with one copy offsite.

- How the backup strategy supports Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) for different systems and data types.
- Backup frequency and retention (e.g., retain 48 hourly snapshots, 30 daily backups).
- Backup types (e.g., full, incremental, continuous, replication, point-in-time copies, etc.).
- Compliance obligations (e.g., data residency, security and privacy rules)
- Locations where enterprise data assets physically reside (e.g., on-premises, in the cloud, and geographically).
- Types of media to be used (e.g., solid state, disk, tape).
- Encryption requirements for data in transit and in storage, as well as encryption key retention and key rotation.
- Other protection requirements – e.g., digital signing, archiving, location, facility security (fire, explosion, magnetic interference protection).

— **Enterprise IT Resilience Strategy**: An enterprise IT resilience strategy may not be formally or comprehensively specified, but may exist through documentation such as:

- The Enterprise Risk Management Framework and Enterprise Risk Register, identifying specific risks and associated mitigations.
- Strategies on backup systems, data replication, and failover mechanisms designed to ensure availability.
- Business Continuity Plan (BCP) and IT Disaster Recovery Plan (IT DRP).
- The Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of all critical IT systems, which are typically articulated within the BCP and/or IT DRP.
- Records of resilience tests and exercises along with gaps identified, mitigations, and lessons learned.

2. **Scope Definition Considerations:** Consider the following items to define the scope. Some of these items may already be in place and completing the checklist item may involve refining existing capability. Understanding the as-is environment as suggested in Step 1 in this *Scope and objectives section* will inform the scope definition as well as the level of effort required for:

- **Backup Strategy Development**: Defining and implementing a backup strategy.
- **Data Identification and Storage Mapping**: Identifying what data is to be included, where it is currently being stored for normal operations and for intermediate and archival backup.
- **Requirements Definition**: Defining the functional and non-functional requirements of the backup and restore solution.
- **Architecture Implementation**: Implementing the technical architecture and building the backup and restore solution.
- **Policy and Procedure Development**: Developing and promulgating backup, testing, and restoration policies and procedures.
- **Solution Documentation**: Documenting the solution and associated procedures.
- **Resilience Plan Adjustment**: Adjusting existing enterprise resilience concepts and documents to reflect the new solution.
- **Personnel Training**: Training personnel to manage and operate the backup solution.

3. **Task Objectives Overview:** The following objectives define the essential outcomes of this task, guiding the development, implementation, and operational readiness of the backup solution:
   - **Strategy and Policy Development**: Develop or validate the mutually supportive strategies and policies for backup, testing of backups, and restoration of data from backups.
   - **Technical Solution Implementation**: Design and implement a technical solution corresponding to the strategy, including the transition from the existing backup solution and methods.
   - **Procedure Documentation**: Develop and document backup, test, and restoration procedures to carry out the strategy.
   - **Personnel Training**: Train IT personnel and others as appropriate in the required operations and procedures.

Coordination with stakeholders

1. **Stakeholder Engagement Overview:** Building an enterprise data backup, testing, and restoration solution can be a large and challenging undertaking, whether the implementation is new or an evolution of an existing solution. In-depth planning and coordination with internal and external stakeholders are essential to success. Stakeholders include:
   - **Internal IT and Cybersecurity Teams**: In-house IT, cybersecurity, and Business Continuity Planning personnel, owners of business systems, and representatives of the county's legal and compliance organizations.

- **External Technology Providers**: Representatives of cloud providers, external IT managed service providers, software and IT hardware vendors.
- **County Financial and Administrative Personnel**: County personnel who have roles in programming, budgeting, and financial management.

Resource requirements

1. **Resource and Budget Planning Overview**: Identify the skills needed and estimate the level of effort required of each for the duration of the project. Determine the sources for personnel with the required skills.
2. **Skills and Effort Estimation**: Develop a budget in accordance with county practices. Estimate costs using county-approved estimation tools and/or methods. Identify capital expenditures, non-capital expenditures, operations and maintenance costs, personnel costs for implementation as well as for operations and maintenance.
3. **Budget Development**: Identify post-implementation operations and management resource requirements and ensure out-year budgets are sufficient to address them.

Schedule of milestones

1. **Milestone Scheduling and Management Overview**: Develop a schedule of milestones that will serve as a "living" document and project management tool for the full execution of the project.
2. **Activity and Milestone Definition**: Define the specific activities such as those outlined above, along with major milestones and the approximate start and end dates for each activity.
3. **Gantt Chart Visualization**: Depict the activities and major milestones with an initial Gantt Chart to highlight interdependencies.
4. **Ongoing Schedule Management**: Actively manage the schedule of milestones through the duration of the project.

Design, implement, and document the solution

1. **Design the solution.** Applying the insight developed in *Scope and objectives* above, work collaboratively with stakeholders to design and document the solution.
    - **Define Technical Requirements:** Define the technical requirements for the backup system, including overall approach (e.g., 3-2-1 strategy or variation), reliability, availability, Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) for

different systems and data types, backup frequency, allowable latency, and other functional requirements.

- **Define Backup Architecture:** Define the backup architecture by establishing the arrangement of backup servers, storage nodes, Storage Area Networks (SANs), node replication, and other devices for hot, cold, and warm storage, their general siting, required network connectivity, routers and other network devices, system and network monitoring and other security devices, Hardware Security Modules for cryptographic key storage, and other hardware.

- **Identify Required IT Capabilities:** Identify the required IT operational capabilities, specifying the network requirements (e.g., bandwidth, protocols, routing, segmentation) and facilities required based on the technical architecture.

- **Select Technology Products:** Identify the specific technology products that will comprise the technical solution. Some components of the existing backup architecture may meet the new requirements and can be reused.

- **Complete Bill of Materials and Procurement:** Complete the Bill of Materials through collaboration between the technical team and the county's IT procurement personnel. Acquire the necessary materials in accordance with the required timeline. The procurement schedule may overlap the build schedule; optimize for efficiency.

- **Preserve Design Artifacts:** Preserve all artifacts developed during the design phase, such as interim or draft documents, partial architectural drawings or sketches, whiteboard diagrams, or other works-in-progress for reference and possible incorporation into final documentation in the Implement and Document phase below.

2. **Implement and document the solution.** Depending on its complexity, building the solution may involve a combination of in-house personnel and external contractor or vendor support. The work should be apportioned and scheduled accordingly.

    - **Ensure Operational Staffing:** Ensure that sufficient numbers of skilled IT and cybersecurity staff are available to carry out daily operations while the implementation proceeds.

    - **Maintain Backup Continuity**: Establish a plan to ensure continuity of backup and restoration capability, keeping the existing backup system in operation until cut-over to the new system is achieved.

    - **Expand Implementation Schedule**: Expand the schedule of milestones with more detail for the implementation schedule. Define activities and add milestones for:

        — Building out the network configuration, data center resources, and cloud services as applicable.

- Transitioning the new solution to full operation.
- Decommissioning the previous system.

- **Establish Data Integrity Verification**: Develop clear processes and procedures for verification of data integrity.
- **Refine System Documentation**: Refine the system documentation as the deployment proceeds to reflect the as-built environment.

Communicate with Leadership: Keep senior managers and county leaders informed of the status and outlook of the new capability.

3. **Document the solution:** Complete documentation of the solution and procedures developed.

- **Assemble Project Records**: Assemble and organize all records and artifacts collected in the design and implementation phases, capturing:
- **Capture Conceptual and Design Artifacts**: Include initial conceptual outlines, meeting notes, tradeoff analyses, alternatives considered, and final design..
- **Include Written Procedures**: Document all written procedures developed throughout the project.
- **Track Milestone Schedules**: Record both planned and actual milestone schedules to reflect project progress and adjustments.
- **Document Labor Hours**: Track labor hours required by in-house and contractor staff to support resource planning and accountability.
- **Preserve Informal Project Materials**: Include informal documents such as notes, screenshots, whiteboard photos, and brainstorming notes that contributed to the project. This reference material should be saved as archival references.
- **Develop Final Documentation**: Building on the collected documentation, develop a final set of formal documents in accordance with county standards.
- **Revise and Finalize Project Documents**: Revise and finalize documentation, including data protection policy, backup strategy, architecture documents, component lists, procedures, points of contact references, service level agreements (as applicable), and all other relevant documents. Follow county procedures for review, approval, and promulgation.
- **Update Contingency Planning Documents**: Revise the Business Continuity Plan (BCP), IT Disaster Recovery Plan (IT DRP), crisis management plans, emergency response plans, or other contingency planning documents as necessary to reflect the new system.

- **Document Backup and Restoration Procedures**: Document the data backup, test, and restoration processes and procedures developed in accordance with county standards.

- **Update System Inventories**: Update software and system inventories as necessary with the identifying information of the hardware and software components of the backup system.

Train personnel

1. **Training Requirements Overview**: To ensure effective operations and maintenance of the backup system, it is essential to define and deliver targeted training for IT personnel. Training should address both procedural execution and policy compliance. Key training components include:

    - **Operations and Maintenance Training**: Define training requirements for IT operations personnel for the operations and maintenance of the backup system. In addition to procedures training, the training should also specifically address the requirements expressed in the policy and documented in process and procedures descriptions.

    - **Initial and Ongoing Training**: Define both initial and periodic training requirements for IT and cybersecurity operations staff.