University of Connecticut

University Information Technology Services

Information Technology Contingency Plan & Planning Guide

Prepared by
Victor Font
UITS Business Continuity / Disaster Recovery Coordinator
December 2012

Table of Contents

Version Control

Date	Author	Version	Notes
12/01/2012	UITS BCP/DR Coordinator	1.0	Rev. 01
01/14/2013	UITS BCP/DR Coordinator	1.0	Rev. 02
01/21/2013	UITS BCP/DR Coordinator	1.0	Rev. 03

Document Change History

DOCUMENT CHANGE HISTORY				
Plan Version No.	**Release Date**	**Summary of Changes**	**Section No./ Paragraph No.**	**Changes Made By**
Ver. 1.0/ Rev. 01	12/28/12	Initial Draft	Entire Document	BCP/DR Coordinator
Ver. 1.0/ Rev. 02	01/14/13	Incorporated feedback from Information Security Office and UITS Leadership Team. Added Figures and refined formatting.	Entire Document	BCP/DR Coordinator
Ver. 1.0/ Rev. 03	01/21/13	Incorporated edits from BCP/DR Working Team. Document baselined in version control.	Pages 8 & 18	BCP/DR Coordinator

Attribution

This document is adapted in part from the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) Special Publication 800-series. The series reports on research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations. The NIST provides the series for use or adoption by any organization without copyright.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe a procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by UITS, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by UITS in accordance with its assigned responsibilities. The information in this publication, including concepts and methodologies, may be used by campus Information Technology organizations even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, IT organizations may wish to closely follow the development of these new publications by UITS.

Business Continuity & Disaster Recovery Policy

This policy is available in the Information Security Policy Manual.

Each University department will maintain a current, written and tested Business Continuity Plan (BCP) that addresses the department's response to unexpected events that disrupt normal business (for example, fire, vandalism, system failure, and natural disaster).

The BCP will be an action-based plan that addresses critical systems and data. Analysis of the criticality of systems, applications, and data will be documented in support of the BCP.

Emergency access procedures will be included in the BCP to address the retrieval of critical data during an emergency.

The BCP will include a Disaster Recovery (DR) Plan that addresses maintaining business processes and services in the event of a disaster and the eventual restoration of normal operations. The BCP and DR Plan will contain a documented process for annual review, testing, and revision. Annual testing of the BCP will include desk audits, and should also include tabletop testing, walkthroughs, live simulations, and data restoration procedures, where appropriate. The BCP will include measures necessary to protect Confidential Data during emergency operations.

Data Administrators are responsible for implementing procedures for critical data backup and recovery in support of the BCP. The data procedures will address the recovery point objective and recovery time objectives determined by the Data Steward and other stakeholders.

Developing A Common Contingency Framework

In developing standards and guidelines required by the University of Connecticut's Business Continuity and Disaster Recovery Policy, UITS consults with local UConn IT organizations and offices as well as other academic institutions and State Agencies to improve information security, avoid unnecessary and costly duplication of effort, and ensure that UITS policies, practices and documentation are complementary with NIST standards and best practice guidelines employed for the protection of information technology systems.

In addition to its comprehensive peer review process, UITS collaborates with the UConn Health Center, UConn Foundation, Connecticut Education Network, UConn School of Engineering, Homer Babbidge Library IT, Student Affairs IT, UConn Research, and UConn Department of Public Safety to establish a common foundation for IT Contingency Planning across the University. A common foundation provides the University and their contractors more uniform and consistent ways to manage the risk to organizational operations (including missions, functions, image, and reputation), organizational assets, individuals, other organizations, and the population that results from the operation and use of information systems. A common foundation also provides a strong basis for reciprocal acceptance of security assessment results and facilitates information sharing.

To this end, UITS has commissioned an Executive Steering Committee and IT Working Team to guide and execute the initiative.

Steering Committee

De Facto Members:	Mun Choi, Provost	
	Nancy Bull, Vice Provost and Chief Information Officer	
Chair:	Victor Font, Business Continuity/Disaster Recovery Coordinator	
Members:	John Saddlemire, VP Student Affairs	Barbara O'Connor, Chief of Public Safety
	Suman Singha, VP Research	Jason Pufahl, Chief Information Security Officer
	Rich Gray, Chief Financial Officer	Rachel Krinsky Rudnick, Assistant Director of Compliance/Privacy
	Deb Cunningham, VP UConn Foundation	

Working Team

Chair:	Victor Font, Business Continuity/Disaster Recovery Coordinator	
	Stephanie Kernozicky, Student Affairs IT	Andy Rittner, Research
Members:	Dan Nevelos, UConn Foundation	Tom Hine, Public Safety
	George Assard, School of Engineering	Carrie Gray, IT Internal Audit
	Ryan Kocsondy, UITS Regional Campuses	John Gwinnell, Team Lead SSG Unix
	Robert Swanson, Unix System Administrator, HBL Library	Tim Ruggieri, CLAS
	Jonathan Gill, UITS	Dan Capetta, SAIT

Executive Summary

Information systems are vital elements in most University mission/business functions. Because information system resources are so essential to UConn's success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough policies, plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption.

Information systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire). Much vulnerability may be minimized or eliminated through management, operational, or technical controls as part of the University's resiliency effort; however, it is virtually impossible to completely eliminate all risks.[1] Contingency planning is designed to mitigate the risk of system and service unavailability by providing effective and efficient solutions to enhance system availability.

Information system contingency planning is a coordinated strategy involving policies, plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption. Contingency planning is unique to each system, providing preventive measures, recovery strategies, and technical considerations appropriate to the system's information confidentiality, integrity, and availability requirements and the system impact level. 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.

This document discusses essential contingency plan elements and processes, highlights specific considerations and concerns associated with contingency planning for various types of information system platforms, and assists local IT organizations in preparing and maintaining their own information system contingency plans (ISCPs).

This plan defines the following six-step contingency planning process utilized by UITS that local IT organizations may apply to develop and maintain a viable contingency planning program for their information systems. These six progressive steps are integrated into each stage of the UITS system development life cycle (SDLC).

[1] For example, in many cases, critical resources (such as electric power or telecommunications) may reside outside the organization's control, and the organization may be unable to ensure their availability.

1. **Conduct the business impact analysis (BIA).** The BIA helps identify and prioritize information systems and components critical to supporting the organization's mission/business functions. A template for developing the BIA is available to assist the user.

2. **Identify preventive controls.** Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.

3. **Create contingency strategies.** Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.

4. **Develop an information system contingency plan.** The contingency plan contains detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements.

5. **Ensure plan testing, training, and exercises.** Testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps; combined, the activities improve plan effectiveness and overall organization preparedness.

6. **Ensure plan maintenance.** The plan is a living document that is updated regularly to remain current with system enhancements and organizational changes.

In addition to this guide, UITS has prepared three templates for documenting an information system contingency plan based on low, moderate, or high availability impact level, as defined by the Categorization of University Information and Information Systems in Appendix A. Each template defines three essential contingency plan phases that govern actions to be taken following a system disruption:

1. **Activation/Notification Phase:** the process of activating the plan based on outage impacts and notifying recovery personnel;

2. **Recovery Phase:** a suggested course of action for recovery teams to restore system operations at an alternate site or using contingency capabilities;

3. **Reconstitution**: activities to test and validate system capability and functionality and outlines actions that can be taken to return the system to normal operating condition and prepare the system against future outages.

Purpose

The purpose of this document is two-fold. First, it is the foundation for the UITS contingency plan and associated documents and activities. Second, it serves as a planning guide for other local UConn IT organizations so there are consistent, complementary principles; and repeatable processes and practices across the University. While the principles establish a baseline to meet most organizational needs, it is recognized that each organization may have additional requirements specific to its own operating environment. This guidance document provides background information on interrelationships between information system contingency planning and other types of security and emergency management-related contingency plans, organizational resiliency, and the system development life cycle (SDLC). The document provides guidance to help personnel evaluate information systems and operations to determine contingency planning requirements and priorities. Considerations for security impact level objectives and associated security controls for contingency planning are presented to assist planners in developing the appropriate contingency planning strategy.

Scope

The scope of this document is limited to information systems. An information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information system components include, but are not limited to, mainframes, servers, workstations, network components, operating systems, middleware, and applications. Network components can include, for example, such devices as firewalls, sensors (local or remote), switches, guards, routers, gateways, wireless access points, and network appliances. Servers can include, for example, database servers, authentication servers, electronic mail and Web servers, proxy servers, domain name servers, and network time servers. Information system components are either purchased commercially off-the-shelf or are custom-developed.

The document outlines planning principles for a wide variety of incidents that can affect information system operations. These range from minor incidents causing short-term disruptions to disasters that affect normal operations for an extended period. Because information systems vary in design and purpose, specific incident types and associated contingency measures are not addressed in this guide. Instead, a defined process is provided for identifying planning requirements needed to develop an effective contingency plan for any information system.

This document does not address organizational mission continuity (commonly referred to as a continuity of operations [COOP] plan) except where it is required to restore information systems and their processing capabilities. Nor does this document address continuity of mission/business functions. Although information systems typically support

mission/business functions, the functions also depend on a variety of other resources and capabilities not associated with information systems. Recovery of mission-essential functions is addressed by COOP plans or business continuity plans developed by the individual University organizations.

Audience

This document is for University leadership and those individuals responsible for information systems or security at system and operational levels. It is also written to assist emergency management personnel who coordinate facility-level contingencies with supporting information system contingency planning activities. The audience includes the following types of personnel:

- The **Provost** and **Chief Information Officer** (CIO) with overall responsibility for the organization's information systems;
- **IT Leadership Teams** and **Managers** responsible for overseeing information system operations or mission/business functions that rely on information systems;
- **Chief Information Security Officer** (CISO) responsible for developing and maintaining the security of information systems at the organizational level;
- **Information System Security Officers** (ISSOs)/**Information System Security Managers** (ISSMs) and other staff responsible for developing, implementing, and maintaining an information system's security activities;
- **System engineers** and **architects** responsible for designing, implementing, or modifying information systems;
- **System administrators** responsible for maintaining daily information system operations;
- **Users** who employ desktop and portable systems to perform their assigned job functions; and
- **Other personnel** responsible for designing, managing, operating, maintaining, or using information systems.

Contingency Planning and Resilience

The University of Connecticut must have the ability to withstand all hazards and sustain its mission through environmental changes. These changes can be gradual, such as economic or mission changes, or sudden, as in a disaster event. Rather than just working to identify and mitigate threats, vulnerabilities, and risks, UITS is working toward building a resilient enterprise infrastructure, minimizing the impact of any disruption on mission-essential functions.

Resilience[2] is the ability to quickly adapt and recover from any known or unknown changes to the environment. Resiliency is not a process, but rather an end-state for UITS. The goal of a resilient organization is to continue mission essential functions at all times during any type of disruption. Resilient organizations continually work to adapt to changes and risks that can affect their ability to continue critical functions. Risk management, contingency, and continuity planning are individual security and emergency management activities that can also be implemented in a holistic manner across the University as components of a resiliency program.

Effective contingency planning begins with the University's contingency planning policy and subjection of each information system to a business impact analysis (BIA). This facilitates prioritizing the systems and processes based on the risk impact level and develops priority recovery strategies for minimizing loss. Appendix A—Categorization of University Information and Information Systems provides guidelines on determining information and information system impact to University operations and assets through a formula that examines three security objectives: confidentiality, integrity, and availability.

1. **Confidentiality:** A loss of *confidentiality* is the unauthorized disclosure of information.
2. **Integrity:** A loss of *integrity* is the unauthorized modification or destruction of information.
3. **Availability:** A loss of *availability* is the disruption of access to or use of information or an information system.

The impact for each security objective is determined to be high, moderate, or low, based on definitions provided in Appendix A. The highest of the individual security objective impact levels are used to determine the overall information system security impact level.

Contingency planning considerations and strategies address the impact level of the availability security objective of information systems. Strategies for high-impact information systems consider high-availability and redundancy options in their design. Options may include fully redundant load balanced systems at alternate sites, data mirroring, and offsite database replication. High-availability options are normally expensive to set up, operate, and maintain and should be considered only for those high-impact information systems categorized with a high-availability security objective. Lower-impact information systems may be able to use less expensive contingency options and tolerate longer downtimes for recovery or restoration of data.

Effective contingency planning includes incorporating security controls early in the development of an information system, and maintaining these controls on an ongoing basis. Appendix B identifies eleven Contingency Planning (CP) security controls for information systems. Not all controls are applicable to all systems. The security impact

[2] The Department of Homeland Security (DHS) Risk Lexicon (September 2008) defines resilience as the "ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions." The DHS Risk Lexicon can be found at www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf.

level categorization determines which controls apply to a particular system. For example, information systems that have availability as a security objective categorized as low impact do not require alternate processing or storage sites, and information systems that have an availability security objective categorized as moderate impact require compliance with only the first system backup control enhancements.

Several CP controls reference environmental controls, which are part of the Physical and Environmental Protection (PE) control family (Appendix C). Environmental controls considerations are only for the locations or buildings that house the information system. The environment includes the hardware and technology assets that support the information system.

There are options available to system teams to facilitate compliance with the CP controls. UITS allows for compensating security controls to provide comparable protection for an information system to comply with the intent of a CP control. An organization may use a compensating security control in lieu of a CP control as long as there is justification for the use of the compensating control and willingness to accept the risk of the compensating control implementation.

UITS Contingency Plan Development

Information system contingency planning represents a broad scope of activities designed to sustain and recover critical system services following an emergency event. Information system contingency planning fits into a much broader security and emergency management effort that includes organizational and business process continuity, disaster recovery planning, and incident management. Ultimately, UITS uses a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the University's information systems, mission/business functions, personnel, and the facility. Because there is an inherent relationship between an information system and the mission/business process it supports, there must be coordination between each plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.

Continuity and contingency planning are critical components of emergency management and organizational resilience but are often confused in their use. *Continuity planning* normally applies to the mission/business itself; it concerns the ability to continue critical functions and processes during and after an emergency event. *Contingency planning* normally applies to information systems, and provides the steps needed to recover the operation of all or part of designated information systems at an existing or new location in an emergency. *Cyber Incident Response Planning* is a type of plan that normally focuses on detection, response, and recovery to a computer security incident or event.

In general, universally accepted definitions for information system contingency planning and the related planning areas have not been available. Occasionally, this leads to confusion regarding the actual scope and purpose of various types of plans. To provide a common basis of understanding regarding information system contingency planning, this

section identifies several other types of plans UITS is developing and describes their purpose and scope relative to information system contingency planning. Because of the lack of standard definitions for these types of plans, the scope of actual plans developed by local IT organizations may vary from the descriptions below. This guide applies the descriptions and references in sections below to security and emergency management-related plans. The plans listed are in alphabetical order and do not imply any order of importance.

Business Continuity Plan (BCP)

The BCP focuses on sustaining an organization's mission/business functions during and after a disruption. An example of a mission/business function may be an organization's payroll process or customer service process. A BCP may be written for mission/business functions within a single business unit or may address the entire organization's processes. The BCP may also be scoped to address only the functions deemed to be priorities. A BCP may be used for long-term recovery in conjunction with the COOP plan, allowing for additional functions to come online as resources or time allow. Because mission/business functions use information systems (ISs), the business continuity planner must coordinate with information system owners to ensure that the BCP expectations and IS capabilities are matched.

Continuity of Operations (COOP) Plan

COOP focuses on restoring an organization's *mission-essential functions* (MEF) at an alternate site and performing those functions for up to 30 days before returning to normal operations. Additional functions, or those at a field office level, may be addressed by a BCP. Minor threats or disruptions that do not require relocation to an alternate site are typically not addressed in a COOP plan.

Standard elements of a COOP plan include:

- Program plans and procedures
- Risk management
- Budgeting and acquisition of resources
- Essential functions
- Order of succession
- Delegation of authority
- Continuity facilities
- Continuity communications
- Vital records management
- Human capital
- Test, training, and exercise
- Devolution
- Reconstitution

Crisis Communications Plan (CCP)

The most effective way to provide helpful information and to reduce rumors is to *communicate clearly and often*. The UITS CCP documents standard procedures for

internal and external communications in the event of a disruption. It also prepares the organization for the possibility that during a significant disaster, the organization may be a communication-forwarding point between personnel, civil, state and federal authorities as designated by the Department of Public Safety, and affected families and friends.

The plan provides various formats for communications appropriate to the incident. The CCP designates specific individuals as the only authority for answering questions from or providing information to the public regarding emergency response. It also includes procedures for disseminating reports to personnel on the status of the incident.

Critical Infrastructure Protection (CIP) Plan

Critical infrastructure and key resources (CIKR) are those components of the UITS infrastructure that are deemed so vital that their loss would have a debilitating effect on the safety, security, economy, and/or health of the University of Connecticut. Protecting and ensuring the resiliency of UConn's CIKR is essential to the University's security, public health and safety, economic vitality, and way of life. Attacks on or failures of CIKR could significantly disrupt UConn. Direct terrorist attacks and natural, manmade, or technological hazards could produce catastrophic losses in terms of human casualties, property destruction, and economic effects, as well as profound damage to student, faculty and staff morale and confidence.

The UITS CIP plan is a set of policies and procedures that serve to protect and recover these assets and mitigate risks and vulnerabilities. The CIP plan defines the roles and responsibilities for protection, develop partnerships and information sharing relationships, implement the risk management framework, and integrate emergency preparedness, protection and resiliency of critical infrastructure.

Associated with the CIP is the CIP Test Plan that documents, at a procedural level, the steps required to test the CIKR documented in the CIP.

Cyber Incident Response Plan (CIRP)

The UITS CIRP establishes procedures to address cyber attacks against the University's information system(s). These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware, software, or data (e.g., malicious logic, such as a virus, worm, or Trojan horse). This plan is included as an appendix of the BCP.

Disaster Recovery Plan (DRP)

The UITS DRP applies to major physical disruptions to service that deny access to the primary facility infrastructure for an extended period. The DRP is an information system-

focused plan designed to restore operability of the target system, application, or data center infrastructure at an alternate site after an emergency. The DRP is supported by multiple information system contingency plans to address recovery of impacted individual systems once the alternate facility has been established. The DRP supports BCP or COOP plans by recovering supporting systems for mission/business functions or mission essential functions at an alternate location. The DRP only addresses information system disruptions that require relocation.

Information System Contingency Plan (ISCP)

An ISCP provides established procedures for the assessment and recovery of a system following a system disruption. The ISCP provides key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system.

The ISCP differs from a DRP primarily in that the information system contingency plan procedures are developed for recovery of the system regardless of site or location. An ISCP can be activated at the system's current location or at an alternate site. In contrast, a DRP is primarily a site-specific plan developed with procedures to move operations of one or more information systems from a damaged or uninhabitable location to a temporary alternate location. Once the DRP has successfully transferred an information system site to an alternate site, each affected system would then use its respective information system contingency plan to restore, recover, and test systems, and put them into operation.

ISCPs are integrated into the UITS System Development Life Cycle and are required for all systems before being deployed to production. UITS has three ISCP templates available for systems of low, moderate, or high security impact level.

Occupant Emergency Plan (OEP)

The Department of Public Safety develops OEPs for the University and UITS follows those procedures. The OEP outlines first-response procedures for occupants of a facility in the event of a threat or incident to the health and safety of personnel, the environment, or property. Such events include a fire, bomb threat, chemical release, domestic violence in the workplace, or a medical emergency. Shelter-in-place procedures for events requiring personnel to stay inside the building rather than evacuate are also addressed in an OEP.

Table 1: Summary of Plan Types

Plan	Purpose	Scope	Plan Relationship
Business Continuity Plan (BCP)	Provides procedures for sustaining mission/business operations while recovering from a significant disruption.	Addresses mission/business functions at a lower or expanded level from COOP mission-essential functions.	Mission/business process focused plan that may be activated in coordination with a COOP plan to sustain non-mission-essential functions.
Continuity of Operations (COOP) Plan	Provides procedures and guidance to sustain an organization's mission essential functions at an alternate site for up to 30 days	Addresses mission-essential functions at a facility; information systems are addressed based only on their support of the mission-essential functions.	Mission-essential functions focused plan that may also activate several business unit-level BCPs, ISCPs, or DRPs, as appropriate.
Crisis Communications Plan (CCP)	Provides procedures for disseminating internal and external communications; means to provide critical status information and control rumors.	Addresses communications with personnel and the public; not information system- focused.	Incident-based plan often activated with a COOP or BCP, but may be used alone during a public exposure event.
Critical Infrastructure Protection (CIP) Plan	Provides policies and procedures for protection of University critical infrastructure components	Addresses critical infrastructure components that are supported or operated by an agency or organization.	Risk management plan that supports COOP plans for organizations with critical infrastructure and key resource assets.
Cyber Incident Response Plan (CIRP)	Provides procedures for mitigating and correcting a cyber attack, such as a virus, worm, or Trojan horse.	Addresses mitigation and isolation of affected systems, cleanup, and minimizing loss of information.	Information system-focused plan that may activate an ISCP or DRP, depending on the extent of the attack.
Disaster Recovery Plan (DRP)	Provides procedures for relocating information systems operations to an alternate location.	Activated after major system disruptions with long-term effects.	Information system-focused plan that activates one or more ISCPs for recovery of individual systems.
Information System Contingency Plan (ISCP)	Provides procedures and capabilities for recovering an information system.	Addresses single information system recovery at the current or, if appropriate alternate location.	Information system-focused plan that may be activated independent from other plans or as part of a larger recovery effort coordinated with a DRP, COOP, and/or BCP.
Occupant Emergency Plan (OEP)	Provides coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat.	Focuses on personnel and property particular to the specific facility; not mission/business process or information system-based.	Incident-based plan that is initiated immediately after an event, preceding a COOP or DRP activation.

Figure 1 shows the interrelationship of each plan as they are implemented to respond to an event as applicable to their respective scopes. The UConn logo in the center of the drawing represents both the University as a whole and any department required to develop plans under the Business Continuity and Disaster Recovery Policy.

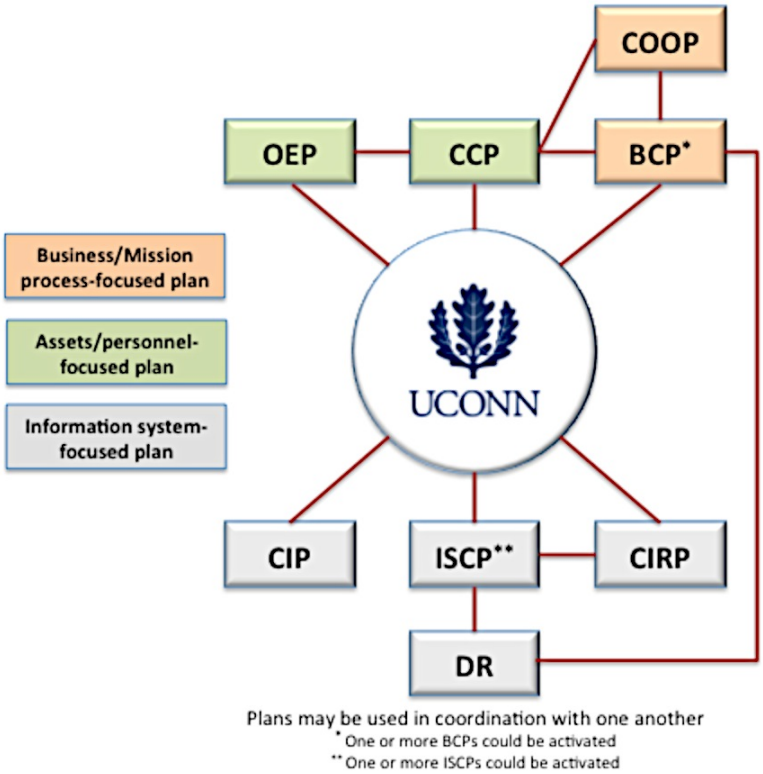

Figure 1: Contingency-Related Plan Relationships

Information System Contingency Planning Process

This section describes the UITS process to develop and maintain an effective information system contingency plan. The process presented is common to all information systems. The six steps in the process are:

1. Conduct the business impact analysis (BIA);
2. Identify preventive controls;
3. Create contingency strategies;
4. Develop an information system contingency plan;
5. Ensure plan testing, training, and exercises; and
6. Ensure plan maintenance.

These steps represent key elements in a comprehensive information system contingency planning capability. Performing system BIA(s) are accomplished early in the SDLC (see

Appendix D) and before the systems are categorized in accordance with the Risk Management Framework (RMF). Five of the six planning process steps are discussed in this section. Step 4, develop an information system contingency plan, is detailed in a separate document.

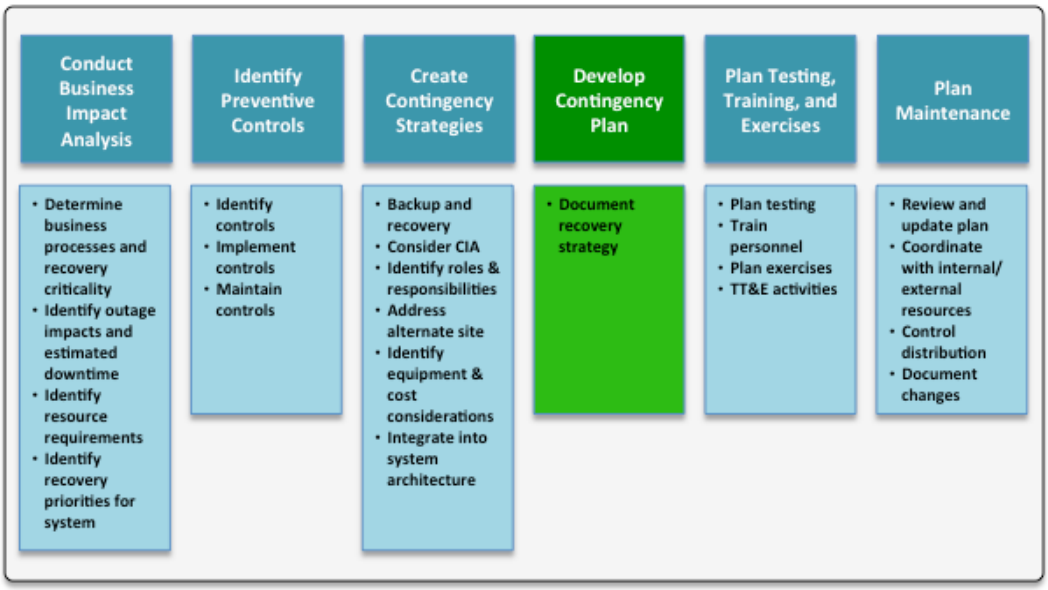

Figure 2: UITS Information System Contingency Planning Process

Responsibility for the planning process generally falls under the auspice of the BCP/DR Coordinator. The BCP/DR Coordinator develops the strategy in cooperation with other functional and resource managers associated with the system or the mission/business functions supported by the system. The BCP/DR Coordinator also manages development and execution of the contingency plan. All University information systems must have a contingency plan.

Conduct the Business Impact Analysis (BIA)

The BIA is a key step in implementing the CP controls and in the contingency planning process overall. The BIA enables the BCP/DR Coordinator to characterize the system components, supported mission/business functions, and interdependencies. The BIA purpose is to correlate the system with the critical mission/business processes and services provided, and based on that information, characterize the consequences of a disruption. The BCP/DR Coordinator uses the BIA results to determine contingency planning requirements and priorities.

Results from the BIA are incorporated into the analysis and strategy development efforts for the organization's COOP, BCPs, and DRP. The BIA is performed during the Initiation phase of the SDLC. As the system design evolves and components change, the BIA may need to be revised during the Development/Acquisition phase of the SDLC.

Incorporating the security impact levels and select security controls helps to ensure that the BIA accounts appropriately for the level of risk to the organization.

Three steps are involved in accomplishing the BIA:

1. **Determine mission/business functions and recovery criticality**.
   Mission/Business functions supported by the system are identified and the impact of a system disruption to those functions is determined along with outage impacts and estimated downtime. The downtime reflects the maximum time that an organization can tolerate while still maintaining the mission.

2. **Identify resource requirements**.
   Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business functions and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.

3. **Identify recovery priorities for system resources**.
   Based upon the results from the previous activities, system resources can be linked more clearly to critical mission/business processes and functions. Priority levels can be established for sequencing recovery activities and resources.

The sample BIA process and data collection activities, outlined in this section and illustrated in Figure 3, consisting of a representative information system with multiple components (servers), are designed to help streamline and focus contingency plan development activities to achieve a more effective plan.[3] In this sample the overall contingency planning impact level assessment for the information system is moderate because the maximum potential impact value for the availability security objective for one or more of the system components is moderate.

[3] For completeness and to assist ISCP Coordinators who may be new to or unfamiliar with the information system, the sample BIA process presented includes basic steps. In many cases, the ISCP Coordinator will be very familiar with specific system components and the ways in which they support business processes and may modify the approach to fit the respective system and contingency needs.

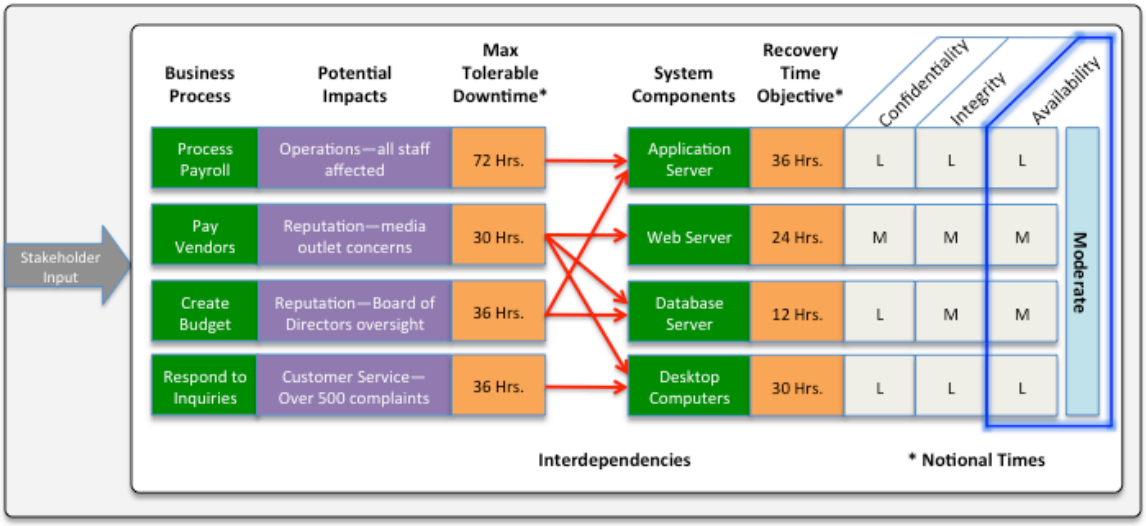

Figure 3: Sample Information System Business Impact Analysis Process

Determine Business Processes and Recovery Criticality

An information system can be very complex and often supports multiple mission/business functions, resulting in different perspectives on the importance of system services or capabilities. To accomplish the BIA and better understand the impacts a system outage or disruption can have on the organization, the BCP/DR Coordinator should work with management and internal and external points of contact (POC)[4] to identify and validate mission/business functions and processes that depend on or support the information system. The identified processes' impacts are then further analyzed in terms of availability, integrity, confidentiality, and the established impact level for the information system.

UITS requires system owners to categorize their information systems as low impact, moderate impact, or high impact for the security objectives of confidentiality, integrity, and availability. The category for the availability security objective serves as a basis of the BIA. Further identification of additional mission/business processes and impacts captures the unique purpose of the system. Organizational and system uniqueness are important considerations for contingency planning and business impact. Adding information types to address this uniqueness enhances the prioritization of system component impacts.

Unique processes and impacts can be expressed in values or units of measurement that are meaningful to the system owners. Values can be identified using a scale and should be characterized as an indication of impact severity to the organization if the process

[4] When identifying POCs, it is important to include organizations that provide or receive data from the system as well as POCs of any interconnected systems. Coordination enables the system manager to characterize the full range of support provided by the system, including security, managerial, technical, and operational requirements.

could not be performed. For example, an impact category such as "Costs" can be created with impact values expressed in terms of staffing, overtime, or fee-related costs.

The BCP/DR Coordinator next analyzes the supported mission/business processes and determines the downtime if a given process or specific system data were disrupted or otherwise unavailable. Downtime can be identified in several ways.

- **Maximum Tolerable Downtime** (MTD). The MTD represents the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave continuity planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.

- **Recovery Time Objective** (RTO). RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business functions, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD. When it is not feasible to immediately meet the RTO and the MTD is inflexible, a Plan of Action and Milestone should be initiated to document the situation and plan for its mitigation.

- **Recovery Point Objective** (RPO). The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. Because the RTO must ensure that the MTD is not exceeded, the RTO must normally be shorter than the MTD. For example, a system outage may prevent a particular process from being completed, and because it takes time to reprocess the data, that additional processing time must be added to the RTO to stay within the time limit established by the MTD.

The BCP/DR Coordinator, working with management, determines the optimum point to recover the information system by addressing the factors mentioned above while balancing the cost of system inoperability against the cost of resources required for restoring the system and its overall support for critical mission/business functions. This can be depicted using a simple chart, such as the example in Figure 4.

The longer a disruption is allowed to continue, the more costly it can become to the University and its operations. Conversely, the shorter the RTO, the more expensive the recovery solutions cost to implement. For example, if the system must be recovered immediately, zero downtime solutions and alternate processing site costs are much higher, whereas a low-impact system with a longer RTO is able to implement a less costly simple backup system. Plotting the cost balance points will show an optimal point between disruption and recovery costs. The intersecting point (Cost Balance Point in

Figure 4: Cost Balancing) will be different for every system based on the financial constraints and operating requirements.

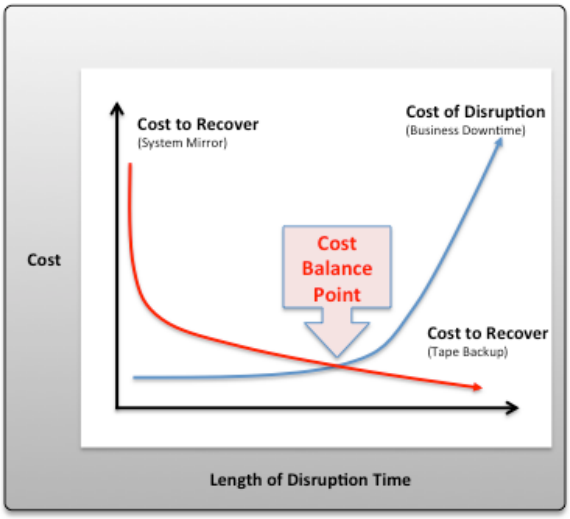

Figure 4: Cost Balancing

Identify Resource Requirements

Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business functions as quickly as possible. Working with management and internal and external POCs associated with the system, the BCP/DR Coordinator ensures that the complete information system resources are identified.[5]

Identify System Resource Recovery Priorities

Developing recovery priorities is the last step of the BIA process. Recovery priorities can be effectively established taking into consideration mission/business function criticality, outage impacts, tolerable downtime, and system resources. The result is an information system recovery priority hierarchy. The BCP/DR Coordinator considers system recovery measures and technologies to meet the recovery priorities.

Identify Preventive Controls

In some cases, the outage impacts identified in the BIA may be mitigated or eliminated through preventive measures that deter, detect, and/or reduce impacts to the system. Where feasible and cost-effective, preventive methods are preferable to actions that may be necessary to recover the system after a disruption. A variety of preventive controls are

[5] To avoid duplication of effort, this information may be obtained from the system component inventory and the system software inventory.

available, depending on system type and configuration; some common measures are listed below:

- Appropriately sized uninterruptible power supplies (UPS) to provide short-term backup power to all system components (including environmental and safety controls);
- Gasoline- or diesel-powered generators to provide long-term backup power;
- Air-conditioning systems with adequate excess capacity to prevent failure of certain components, such as a compressor;
- Fire suppression systems;
- Fire and smoke detectors;
- Water sensors in the computer room ceiling and floor;
- Heat-resistant and waterproof containers for backup media and vital non electronic records;
- Emergency master system shutdown switch;
- Offsite storage of backup media, non-electronic records, and system documentation;
- Technical security controls, such as cryptographic key management; and
- Frequent scheduled backups including where the backups are stored (onsite or offsite) and how often they are recirculated and moved to storage.

Create Contingency Strategies

All University IT organizations are required to adequately mitigate the risk arising from use of information and information systems in the execution of missions/business functions. The challenge is in implementing the right set of security controls. Guided by the UITS Information Security Office, security controls are selected and implemented. Contingency strategies are created to mitigate the risks for the contingency planning family of controls and cover the full range of backup, recovery, contingency planning, testing, and ongoing maintenance.

Backup and Recovery

Backup and recovery methods and strategies are a means to restore system operations quickly and effectively following a service disruption. The methods and strategies address disruption impacts and allowable downtimes identified in the BIA and are integrated into the system architecture during the Development/Acquisition phase of the SDLC. A wide variety of recovery approaches may be considered, with the appropriate choice being highly dependent upon the incident, type of system, BIA/security impact level, and the system's operational requirements.

Specific recovery methods are to be considered and may include commercial contracts with alternate site vendors, reciprocal agreements with internal or external organizations, and service-level agreements (SLAs) with equipment vendors. In addition, technologies

such as redundant arrays of independent disks (RAID), automatic failover, UPS, server clustering, and mirrored systems are considered when developing a system recovery strategy.

Several alternative approaches are considered when developing and comparing strategies, including cost, maximum downtimes, security, recovery priorities, and integration with larger, enterprise-level contingency plans. The following table is an example that can assist in identifying the linkage of availability impact level for the availability security objective, recovery priority, backup, and recovery strategy.

Availability Impact Level	Information System Target Priority and Recovery	Backup / Recovery Strategy
Low	Low priority - any outage with little impact, damage, or disruption to the organization.	Backup: Tape backup Strategy: Relocate or Cold site
Moderate	Important or moderate priority - any system that, if disrupted, causes a moderate problem to the organization and possibly other networks or systems.	Backup: Optical backup, WAN/VLAN replication Strategy: Cold or Warm site
High	Mission-critical or high priority - the damage or disruption causes the most impact on the organization, mission, and other networks and systems.	Backup: Mirrored systems and disc replication Strategy: Hot site

Backup Methods and Offsite Storage

System data is backed up regularly. The UITS Policy for system backups and cloud storage specifies the minimum frequency of backups (e.g., daily or weekly, incremental or full) based on data criticality and the frequency that new information is introduced. The data backup policy designates the location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite. Data is backed up on magnetic disk, tape, or optical disks, such as compact disks (CDs). The specific method chosen for conducting backups should be based on system and data availability and integrity requirements. These methods may include electronic vaulting, network storage, and tape library systems.

It is good business practice to store backed-up data offsite. Commercial data storage facilities are specially designed to archive media and protect data from threatening elements. If using offsite storage, data is backed up at the University's facility and then labeled, packed, and transported to the storage facility. If the data is required for recovery or testing purposes, UITS contacts the storage facility requesting specific data to be transported to the data center or to an alternate facility.[6] Commercial storage facilities often offer media transportation and response and recovery services. When selecting an offsite storage facility and vendor, the following criteria should be considered:

[6] Backup tapes should be tested regularly to ensure that data are being stored correctly and that the files may be retrieved without errors or lost data. Also, the Information System Planning Coordinator should test the backup tapes at the alternate site, if applicable, to ensure that the site supports the same backup configuration that the organization has implemented.

- **Geographic area**: distance from the Storrs campus and the probability of the storage site being affected by the same disaster as the primary data center;
- **Accessibility**: length of time necessary to retrieve the data from storage and the storage facility's operating hours
- **Security**: security capabilities of the shipping method, storage facility, and personnel; all must meet the data's security requirements;
- **Environment**: structural and environmental conditions of the storage facility (i.e., temperature, humidity, fire prevention, and power management controls); and
- **Cost**: cost of shipping, operational fees, and disaster response/recovery services.

Alternate Sites

As stated earlier, Appendix B identifies the CP controls for information systems. The Appendix A security categorization for the availability security objective determines which controls apply to a particular system. For example, an information system categorized with a low-availability security objective does not require alternate storage or a processing site (CP-6 and CP-7, respectively), and an information system with a moderate-availability security objective requires the system backup and testing the backup (CP-9 [1]).

Although major disruptions with long-term effects may be rare, they are accounted for in the contingency plan. Thus, for all moderate- or high-impact systems, the UITS plan includes a strategy to recover and perform system operations at an alternate facility for an extended period. The current on campus alternate facility for critical infrastructure key resources (CIKR) is the Chemistry building. At a later date, this equipment will be moved to the Library building. An alternate CIKR remote facility will be established in the data center of the University of Connecticut Health Center in Farmington in 2013.

Local IT organizations may consider low-impact systems for alternate site processing, but that is an organizational decision and not required. In general, three types of alternate sites are available:

- Dedicated site owned or operated by the University;
- Reciprocal agreement or memorandum of agreement with an internal or external entity; and
- Commercially leased facility.

Regardless of the type of alternate site chosen, the facility must be able to support system operations as defined in the contingency plan. The three alternate site types commonly categorized in terms of their operational readiness are cold sites, warm sites, or hot sites. Other variations or combinations of these can be found, but generally all variations retain similar core features found in one of these three site types. Progressing from basic to advanced, the sites are described below.

- **Cold Sites** are typically facilities with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support information system recovery activities.
- **Warm Sites** are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources.
- **Hot Sites** are facilities appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel.

As discussed above, these three alternate site types are the most common. There are also variations, and hybrid mixtures of features from any one of the three. Each IT unit should evaluate its core requirements in order to establish the most effective solution. Two examples of variations to the site types are:

- **Mobile Sites** are self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements.
- **Mirrored Sites** are fully redundant facilities with automated real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects.

There are obvious cost and ready-time differences among the options. In these examples, the mirrored site is the most expensive choice, but it ensures virtually 100% availability. Cold sites are the least expensive to maintain, although they may require substantial time to acquire and install necessary equipment. Partially equipped sites, such as warm sites, fall in the middle of the spectrum. In many cases, mobile sites may be delivered to the desired location within 24 hours, but the time necessary for equipment installation and setup can increase this response time. The selection of fixed-site locations should account for the time and mode of transportation necessary to move personnel and/or equipment there. In addition, the fixed site should be in a geographic area that is unlikely to be negatively affected by the same hazard as the UConn's primary site.

Table 2 summarizes the criteria to employ to determine which type of alternate site meets your requirements. Sites should be analyzed further including considerations given to business impacts and downtime defined in the BIA. As sites are evaluated, the BCP/DR Coordinator ensures that the system's security, management, operational, and technical controls are compatible with the prospective site. Such controls may include firewalls, physical access controls, and personnel security requirements of the staff supporting the site.

Table 2: Example Alternate Site Criteria

Site	Cost	Hardware Equipment	Telecommunications	Setup Time	Location
Cold Site	Low	None	None	Long	Fixed
Warm Site	Medium	Partial	Partial/Full	Medium	Fixed
Hot Site	Medium/High	Full	Full	Short	Fixed

Alternate sites may be owned and operated by UConn (internal recovery), or commercial sites may be available under contract. If contracting for the site with a commercial vendor, adequate testing time, workspace, security requirements, hardware requirements, telecommunications requirements, support services, and recovery days (how long the organization can occupy the space during the recovery period) must be negotiated and clearly stated in the contract. You must be aware that multiple organizations may contract with a vendor for the same alternate site; as a result, the site may be unable to accommodate all of the customers if a disaster affects enough of those customers simultaneously. The vendor's policy on how this situation should be addressed and how priority status is determined should be negotiated.

Two or more IT organizations with similar or identical system configurations and backup technologies may enter into a formal agreement to serve as alternate sites for each other or enter into a joint contract for an alternate site. This type of site is set up via a reciprocal agreement or memorandum of understanding (MOU). A reciprocal agreement should be entered into carefully because each site must be able to support the other, in addition to its own workload, in the event of a disaster. This type of agreement requires the recovery sequence for the applications from both organizations to be prioritized from a joint perspective, favorable to both parties. Testing is to be conducted at the partnering sites to evaluate the extra processing thresholds, compatible system and backup configurations, sufficient telecommunications connections, compatible security measures, and the sensitivity of data that might be accessible by other privileged users, in addition to functionality of the recovery strategy. Consideration should also be given to system interconnections and possible interconnection security agreements (ISAs).

An MOU or a Service Level Agreement (SLA) for an alternate site must be developed specific to your needs and the partner organization's capabilities. The UConn legal department must review and approve the agreement. In general, the agreement should address at a minimum, each of the following elements:

- Contract/agreement duration;
- Cost/fee structure for disaster declaration and occupancy (daily usage), administration, maintenance, testing, annual cost/fee increases, transportation support cost (receipt and return of offsite data/supplies, as applicable), cost/expense allocation (as applicable), and billing and payment schedules;
- Disaster declaration (i.e., circumstances constituting a disaster, notification procedures);
- Site/facility priority access and/or use;
- Site availability;
- Site guarantee;
- Other clients subscribing to same resources and site, and the total number of site subscribers, as applicable;
- Contract/agreement change or modification process;
- Contract/agreement termination conditions;
- Process to negotiate extension of service;

- Guarantee of compatibility;
- Information system requirements (including data and telecommunication requirements) for hardware, software, and any special system needs (hardware and software);
- Change management and notification requirements, including hardware, software, and infrastructure;
- Security requirements, including special security needs;
- Staff support provided/not provided;
- Facility services provided/not provided (use of onsite office equipment, cafeteria, etc.);
- Testing, including scheduling, availability, test time duration, and additional testing, if required;
- Records management (onsite and offsite), including electronic media and hardcopy;
- Service-level management (performance measures and management of quality of information system services provided);
- Work space requirements (e.g., chairs, desks, telephones, personal computers);
- Supplies provided/not provided (e.g., office supplies);
- Additional costs not covered elsewhere;
- Other contractual issues, as applicable; and
- Other technical requirements, as applicable.

Equipment Replacement

If the information system is damaged or destroyed or the primary site is unavailable, necessary hardware and software will need to be activated or procured quickly and delivered to the alternate location. UITS recommends and supports three basic strategies to prepare for equipment replacement.

- **Vendor Agreements**. SLAs with hardware, software, and support vendors are in place for emergency maintenance service. The SLAs specify how quickly the vendor must respond after being notified. The agreement also gives UConn priority status for the shipment of replacement equipment over equipment being purchased for normal operations. SLAs further discuss what priority status UITS receives in the event of a catastrophic disaster involving multiple vendor clients. In such cases, organizations with health- and safety-dependent processes receive the highest priority for shipment. The details of these negotiations are documented in the SLAs, which are maintained with the contingency plan.

- **Equipment Inventory**. Required equipment may be purchased in advance and stored at a secure offsite location, such as an alternate site where recovery operations will take place (warm or mobile site) or at another location where they will be stored and then shipped to the alternate site. This solution has certain drawbacks. Your organization must commit financial resources to purchase this

equipment in advance, and the equipment could become obsolete or unsuitable for use over time because system technologies and requirements change.

- **Existing Compatible Equipment**. Equipment currently housed and used by the contracted hot site or by another IT organization within UConn may be used. Agreements made with hot sites and reciprocal internal sites stipulate that similar and compatible equipment will be available for contingency use by the organization.

When evaluating the choices, the BCP/DR Coordinator considers that purchasing equipment when needed is cost-effective but can add significant overhead time to recovery while waiting for shipment and setup; conversely, storing unused equipment is costly, but allows recovery operations to begin more quickly. When selecting the most appropriate strategy, note that the availability of transportation may be limited or temporarily halted in the event of a catastrophic disaster. Based on impacts discovered through the BIA, consideration should be given to the possibility of a widespread disaster entailing mass equipment replacement and transportation delays that would extend the recovery period. Regardless of the strategy selected, detailed lists of equipment needs and specifications should be maintained within the contingency plan.

Cost Considerations

The BCP/DR Coordinator ensures that the chosen strategy can be implemented effectively with available personnel and financial resources. The cost of each type of alternate site, equipment replacement, and storage option under consideration is weighed against budget limitations. The coordinator determines known contingency planning expenses, such as alternate site contract fees, and those that are less obvious, such as the cost of implementing an organization-wide contingency awareness program and contractor support. The budget must be sufficient to encompass software, hardware, travel and shipping, testing, plan training programs, awareness programs, labor hours, other contracted services, and any other applicable resources (e.g., desks, telephones, fax machines, pens, and paper). Local IT organizations should perform a cost-benefit analysis to identify the optimum contingency strategy. Table 3 provides a template for evaluating cost considerations.

Table 3: Contingency Strategy Budget Planning Template

Contingency Resources	Strategies	Vendor Costs	Hardware Costs	Software Costs	Travel/ Shipping Costs	Labor/ Contracting Costs	Testing Costs	Supply Costs
Alternate Site	Cold Site							
	Warm Site							
	Hot Site							
Offsite Storage	Commercial							
	Internal							
Equipment	SLA							
	Storage							

Replacement	Existing Use							

Plan Testing, Training, and Exercises (TT & E)

UITS maintains its ISCPs in a state of readiness, which includes having personnel trained to fulfill their roles and responsibilities within the plan, having plans exercised to validate their content, and having systems and system components tested to ensure their operability in the environment specified in the ISCP. While the majority of TT&E activities occur during a system's Operations/Maintenance phase, initial TT&E events are conducted during the Implementation/Assessment phase of the SDLC to validate ISCP recovery procedures.

UITS conducts TT&E events at least annually, following organizational or system changes, or the issuance of new TT&E guidance, or as otherwise needed. Execution of TT&E events assists UITS in determining the plan's effectiveness, and that all personnel know what their roles are in the conduct of each information system plan. For each TT&E activity conducted, results are documented in an after-action report, and Lessons Learned corrective actions are captured for updating information in the ISCP. The following sections summarize how to plan and conduct TT&E activities for information systems. A more comprehensive *Guide to Test, Training and Exercise Programs for Information Technology Plans and Capabilities* is also available.

Testing

Tests are evaluation tools that use quantifiable metrics to validate the operability of an information system or system component in an operational environment. For example, you could test call tree lists to determine if calling can be executed within prescribed time limits; another test may be removing power from a system or system component. A test is conducted in as close to an operational environment as possible; if feasible, an actual test of the components or systems used to conduct daily operations for the organization should be used.[7] The scope of testing can range from individual system components or systems to comprehensive tests of all systems and components that support an ISCP. Tests often focus on recovery and backup operations; however, testing varies depending on the availability impact level, the goal of the test, and its relation to a specific ISCP.

ISCP testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan. Testing can take on several forms and accomplish several objectives but is conducted in as close to an operating environment as possible. Each information system component is tested to confirm the accuracy of individual recovery procedures. The following areas are addressed in all UITS contingency plan tests, as applicable:

[7] Special consideration is given to systems with a need for real-time response and extremely high availability, predictability, and reliability. Thorough testing of these systems may not be possible during a single testing event.

- Notification procedures;
- System recovery on an alternate platform from backup media;
- Internal and external connectivity;
- System performance using alternate equipment;
- Restoration of normal operations; and
- Other plan testing (where coordination is identified, i.e., COOP, BCP).

For UITS to derive the most value from the test, the BCP/DR Coordinator develops a test plan designed to examine the selected element(s) against explicit test objectives and success criteria. The use of test objectives and success criteria enable the effectiveness of each system element and the overall plan to be assessed. The test plan includes a schedule detailing the time frames for each test and test participants. The test plan also clearly delineates scope, scenario, and logistics. The scenario chosen may be a worst-case incident or an incident most likely to occur. It mimics reality as closely as possible.

Training

Training refers only to informing personnel of their roles and responsibilities within a particular information system plan and teaching them skills related to those roles and responsibilities, thereby preparing them for participation in exercises, tests, and actual emergency situations related to the ISCP. Training personnel on their roles and responsibilities before an exercise or test event is typically split between a presentation on their roles and responsibilities and activities that allow personnel to demonstrate their understanding of the subject matter.

Training for UITS personnel with contingency plan responsibilities focuses on familiarizing them with ISCP roles and teaching skills necessary to accomplish those roles. This approach helps ensure that staff is prepared to participate in tests and exercises as well as actual outage events. Training is provided at least annually. Personnel newly appointed to ISCP roles receive training shortly thereafter. Ultimately, ISCP personnel are trained to the extent that that they are able to execute their respective recovery roles and responsibilities without aid of the actual ISCP document. This is an important goal in the event that paper or electronic versions of the plan are unavailable for the first few hours, as a result of the disruption. Recovery personnel are trained on the following plan elements:

- Purpose of the plan;
- Cross-team coordination and communication;
- Reporting procedures;
- Security requirements;
- Team-specific processes (Activation and Notification, Recovery, and Reconstitution Phases); and
- Individual responsibilities (Activation and Notification, Recovery, and Reconstitution Phases).

Exercises

An exercise is a simulation of an emergency designed to validate the viability of one or more aspects of an ISCP. In an exercise, personnel with roles and responsibilities in a particular ISCP meet to validate the content of a plan through discussion of their roles and their responses to emergency situations, execution of responses in a simulated operational environment, or other means of validating responses that do not involve using the actual operational environment. Exercises are scenario-driven, such as a power failure in one of the organization's data centers or a fire causing certain systems to be damaged, with additional situations often being presented during the course of an exercise.

UITS employs the following types of exercises widely used in information system TT&E programs:

- **Tabletop Exercises**. Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision-making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.

- **Functional Exercises**. Functional exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, emergency notifications, system equipment setup). Functional exercises vary in complexity and scope; from validating specific aspects of a plan to full-scale exercises that address all plan elements.[8] Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency situation, but in a simulated manner.

TT&E Program Summary

The UITS TT&E program provides an overall framework for determining, scheduling, and setting objectives for TT&E activities. The depth and rigor of ISCP TT&E activities increases with the availability security objective. All tests and exercises include some

[8] Planned and unplanned maintenance activities may also present opportunities to execute and document a Functional Exercise. This is often applicable to operational systems where it may be otherwise disruptive to test certain aspects of the system or contingency plan.

kind of determination of the effects on UITS's operations and provide for a mechanism to update and improve the plan as a result.

Each of the three ISCP Templates (low, moderate, and high) created to complement this guide contain details for conducting TT&E activities appropriate to their respective impact level.

- **For low-impact systems, a tabletop exercise conducted at least yearly is sufficient.** The tabletop simulates a disruption, includes all main ISCP points of contact, and is conducted by the system owner or responsible authority.

- **For moderate-impact systems, a functional exercise is conducted at least yearly.** The functional exercise includes all ISCP points of contact and is facilitated by the system owner or responsible authority. Exercise procedures are developed to include an element of system recovery from backup media.

- **For high-impact systems, a full-scale functional exercise is conducted at least yearly.** The full-scale functional exercise includes a system failover to the alternate location. This includes additional activities such as full notification and response of key personnel to the recovery location, recovery of a server or database from backup media or setup, and processing from a server at an alternate location. The test also includes a full recovery and reconstitution of the information system to a known state.

Table 4 summarizes UITS TT&E activity cross-referencing CP controls and as required by the availability impact level.

Table 4: UITS ISCP TT&E Activities

TT&E Event	Activity	Availability Security Objective
ISCP Training (CP-3)	A seminar and/or briefing used to familiarize personnel with the overall ISCP purpose, phases, activities, and roles and responsibilities.	Low Impact = Yes Mod. Impact = Yes High Impact = Yes
Instruction (CP-3)	Instruction of contingency personnel on their roles and responsibilities within the ISCP and includes refresher training. (For a high-impact system, incorporate simulated events.)	Low Impact = Yes Mod. Impact = Yes High Impact = Yes
Contingency Plan Test / Exercise (CP-4)	Test and/or exercise the contingency plan to determine effectiveness and the organization's readiness. This could include planned and unplanned maintenance activities.	Low Impact = Yes Mod. Impact = Yes High Impact = Yes
Tabletop Exercise (CP-4)	Discussion-based simulation of an emergency situation in an informal, stress-free environment; designed to elicit constructive scenario-based discussions for an examination of the existing ISCP and individual state of preparedness.	Low Impact = Yes Mod. Impact = Yes High Impact = Yes
Functional Exercise (CP-4)	Simulation of a disruption with a system recovery component such as backup tape restoration or server recovery.	Mod. Impact = Yes High Impact = Yes
Full-Scale Functional Exercise (CP-4)	Simulation prompting a full recovery and reconstitution of the information system to a known state and ensures that staff are familiar with the alternate facility.	High Impact = Yes

TT&E Event	Activity	Availability Security Objective
Alternate Processing Site Recovery (CP-7)	Test/exercise the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and evaluate the site's capabilities to support contingency operations. Includes a full recovery and return to normal operations to a known secure state. *(For a high-impact system, the alternate site should be fully configured as defined in the plan.)*	Low Impact = N/A Mod. Impact = Yes High Impact = Yes
System Backup (CP-9)	Test backup information to verify media reliability and information integrity. (For a high-impact system, use sample backup information and ensure that backup copies are stored in a separate facility.)	Low Impact = N/A Mod. Impact = Yes High Impact = Yes

Plan Maintenance

To be effective, UITS maintains all ISCP plans in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. During the Operation/Maintenance phase of the SDLC, information systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies. Therefore, it is essential that ISCPs be reviewed and updated regularly, as part of UITS's change management process, to ensure that new information is documented and contingency measures are revised if required. The continuous monitoring process provides UITS with an effective tool for plan maintenance, producing ongoing updates to security plans, security assessment reports, and plans of action and milestone documents.

As a general rule, plans are reviewed for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan. Certain elements, such as contact lists, require more frequent reviews. The plans for moderate- or high-impact systems are reviewed more often, at least every six months. At a minimum, plan reviews focus on the following elements:

- Operational requirements;
- Security requirements;
- Technical procedures;
- Hardware, software, and other equipment (types, specifications, and amount);
- Names and contact information of team members;
- Names and contact information of vendors, including alternate and offsite vendor POCs;
- Alternate and offsite facility requirements; and
- Vital records (electronic and hardcopy).

Because ISCPs contain potentially sensitive operational and personnel information, its distribution is marked accordingly and controlled. Copies of the plan are provided to recovery personnel for storage. A copy is also stored at the alternate site and with the backup media. Storing a copy of the plan at the alternate site ensures its availability and

good condition in the event local plan copies cannot be accessed because of disaster. The BCP/DR Coordinator maintains a record of copies of the plan and to whom they were distributed. Other information stored with the plan includes contracts with vendors (SLAs and other contracts), software licenses, system user manuals, security manuals, and operating procedures.

Changes made to the plan, strategies, and policies are coordinated through the BCP/DR Coordinator, who communicates changes to the representatives of associated plans or programs, as necessary. The BCP/DR Coordinator records plan modifications using a record of changes, which lists the page number, change comment, and date of change.

The BCP/DR Coordinator frequently coordinates with associated internal and external organizations and system POCs to ensure that impacts caused by changes within any organization is reflected in the contingency plan. Strict version control is maintained by requesting old plans or plan pages to be returned to the BCP/DR Coordinator in exchange for the new plan or plan pages. The BCP/DR Coordinator also evaluates supporting information to ensure that the information is current and continues to meet system requirements adequately. This information includes the following:

- Alternate site contract, including testing times;
- Offsite storage contract;
- Software licenses;
- MOUs or vendor SLAs;
- Hardware and software requirements;
- System interconnection agreements;
- Security requirements;
- Recovery strategy;
- Contingency policies;
- Training and awareness materials;
- Testing scope; and
- Other plans, e.g., COOP, BCP.

Although some changes are quite visible, others require additional analysis. When a significant change occurs, the BIA is updated with the new information to identify new contingency requirements or priorities. As new technologies become available, preventive controls may be enhanced and recovery strategies may be modified. Finally, plan maintenance is continued as the information system passes through the Disposal phase of its life cycle to ensure that the plan accurately reflects recovery priorities and concurrent processing changes.

Appendix A—Categorization of University Information and Information Systems

The Information Security Policy Manual defines the following data classification levels:

Confidential Data requires the highest level of privacy and may not be released. Confidential Data is data that is protected by either:

- Legal or regulatory requirements (e.g., HIPAA)
- Contractual agreements (e.g., Non Disclosure Agreements)

Protected Data must be appropriately protected to ensure a lawful or controlled release (e.g. Connecticut Freedom of Information Act requests). This is all data that is neither Confidential or Public data (e.g., employee email).

Public Data is open to all users, with no security measures necessary. Data is public if:

- There is either an obligation to make the data public (e.g., Fact Sheets), or
- The information is intended to promote or market the University, or pertains to institutional initiatives (e.g., brochures)

This appendix describes the security categories for both University information[9] and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

Security Objectives

There are three security objectives for information and information systems:

4. **Confidentiality:** A loss of *confidentiality* is the unauthorized disclosure of information.
5. **Integrity:** A loss of *integrity* is the unauthorized modification or destruction of information.
6. **Availability:** A loss of *availability* is the disruption of access to or use of information or an information system.

[9] Information is categorized according to its *information type*. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by the University or, in some instances, by a specific law, directive, policy, or regulation.

Potential Impact on Organizations and Individuals

There are three levels of *potential impact* on the University or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization and the overall University interest.

The *potential impact* is **LOW** if—

- The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on operations, assets, or individuals.[10]

Amplification: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to University assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The *potential impact* is **MODERATE** if—

- The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on operations, assets, or individuals.

Amplification: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to University assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The *potential impact* is **HIGH** if—

- The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on operations, assets, or individuals.

Amplification: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the University is not able to perform one or more of its primary functions; (ii) result in major damage to University assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

[10] Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.

The following table summarizes the potential impact definitions for each security objective—confidentiality, integrity, and availability.

Security Categorization Applied to Data Classification Levels

The security category of an information type can be associated with both user information and system information[11] and can be applicable to information in either electronic or non-electronic form. It can also be used as input in considering the appropriate security category of an information system. Establishing an appropriate security category for a data classification level essentially requires determining the *potential impact* for each security objective associated with the particular information type.

The generalized format for expressing the security category, **SC**, of an information type is:

SC information type = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},
where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE.[12]

EXAMPLE 1: An University IT group manages *public information* on its web server and determines that there is no potential impact from a loss of confidentiality (i.e., confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability. The resulting security category, SC, of this information type is expressed as:

SC public information = {(**confidentiality**, NA), (**integrity**, MODERATE), (**availability**, MODERATE)}.

EXAMPLE 2: The University's Department of Public Safety manages extremely sensitive *investigative information* and determines that the potential impact from a loss of confidentiality is high, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is moderate. The resulting security category, SC, of this information type is expressed as:

SC investigative information = {(**confidentiality**, HIGH), (**integrity**, MODERATE), (**availability**, MODERATE)}.

EXAMPLE 3: The University's financial organization manages routine administrative information (not privacy-related information) and determines that the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low. The resulting security category, SC, of this information type is expressed as:

---

[11] System information (e.g., network routing tables, password files, and cryptographic key management information) must be protected at a level commensurate with the most critical or sensitive user information being processed, stored, or transmitted by the information system to ensure confidentiality, integrity, and availability.

[12] The potential impact value of *not applicable* only applies to the security objective of confidentiality.

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

Security Categorization Applied to Information Systems

Determining the security category of an information system requires slightly more analysis and must consider the security categories of all information types resident on the information system. For an information system, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) shall be the highest values (i.e., high water mark) from among those security categories that have been determined for each type of information resident on the information system.[13]

The generalized format for expressing the security category, SC, of an information system is:

SC information system = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

Note that the value of *not applicable* cannot be assigned to any security objective in the context of establishing a security category for an information system. This is in recognition that there is a low minimum potential impact (i.e., low water mark) on the loss of confidentiality, integrity, and availability for an information system due to the fundamental requirement to protect the system-level processing functions and information critical to the operation of the information system.

EXAMPLE 4: A contract management system used for the University's Legal Department contains sensitive contract information and routine administrative information. The department's management determines that: (i) for the sensitive contract information, the potential impact from a loss of confidentiality is moderate, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is low; and (ii) for the routine administrative information (non-privacy-related information), the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low. The resulting security categories, SC, of these information types are expressed as:

SC contract information = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)},

and

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

[13] It is recognized that information systems are composed of both programs and information. Programs in execution within an information system (i.e., system processes) facilitate the processing, storage, and transmission of information and are necessary for the organization to conduct its essential mission-related functions and operations. These system-processing functions also require protection and could be subject to security categorization as well. However, in the interest of simplification, it is assumed that the security categorization of all data classification levels associated with the information system provide an appropriate *worst case* potential impact for the overall information system—thereby obviating the need to consider the system processes in the security categorization of the information system.

The resulting security category of the information system is expressed as:

SC contract management system = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)},

representing the high water mark or maximum potential impact values for each security objective from the information types resident on the acquisition system.

EXAMPLE 5: UConn's cogeneration power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for the University. The SCADA system contains both real-time sensor data and routine administrative information. The cogeneration plant's management determines that: (i) for the sensor data being acquired by the SCADA system, there is no potential impact from a loss of confidentiality, a high potential impact from a loss of integrity, and a high potential impact from a loss of availability; and (ii) for the administrative information being processed by the system, there is a low potential impact from a loss of confidentiality, a low potential impact from a loss of integrity, and a low potential impact from a loss of availability. The resulting security categories, SC, of these information types are expressed as:

SC sensor data = {(**confidentiality**, NA), (**integrity**, HIGH), (**availability**, HIGH)},

and

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

The resulting security category of the information system is initially expressed as:

SC SCADA system = {(**confidentiality**, LOW), (**integrity**, HIGH), (**availability**, HIGH)},

representing the high water mark or maximum potential impact values for each security objective from the information types resident on the SCADA system. The power plant's management chooses to increase the potential impact from a loss of confidentiality from low to moderate reflecting a more realistic view of the potential impact on the information system should there be a security breach due to the unauthorized disclosure of system-level information or processing functions. The final security category of the information system is expressed as:

SC SCADA system = {(**confidentiality**, MODERATE), (**integrity**, HIGH), (**availability**, HIGH)}.

Table 5: Potential Impact Definitions For Security Objectives

	Potential Impact		
Security Objective	**Low**	**Moderate**	**High**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Appendix B—Contingency Planning Controls Summary

Control No.	Control Name	Controls Baseline		
		Low	Mod	High
CP-1	**Contingency Planning Policy and Procedures**	✓	✓	✓
CP-1 (1)	Contingency Planning Policy and Procedures / Defined by UConn Leadership	✓	✓	✓
CP-2	**Contingency Plan**	✓	✓	✓
CP-2 (1)	*Contingency Plan | Coordinate With Related Plans*		✓	✓
CP-2 (2)	*Contingency Plan | Capacity Planning*			✓
CP-2 (3)	*Contingency Plan | Resume Essential Missions / Business Functions*		✓	✓
CP-2 (4)	*Contingency Plan | Resume All Missions / Business Functions*			✓
CP-2 (5)	*Contingency Plan | Continue Essential Missions / Business Functions*			✓
CP-2 (6)	*Contingency Plan | Alternate Processing / Storage Site*			
CP-2 (7)	*Contingency Plan | Coordinate With External Service Providers*			
CP-2 (8)	*Contingency Plan | Identify Critical Assets*		✓	✓
CP-3	**Contingency Training**	✓	✓	✓
CP-3 (1)	*Contingency Training | Simulated Events*			✓
CP-3 (2)	*Contingency Training | Automated Training Environments*			
CP-4	**Contingency Plan Testing**	✓	✓	✓
CP-4 (1)	*Contingency Plan Testing | Coordinate With Related Plans*		✓	✓
CP-4 (2)	*Contingency Plan Testing | Alternate Processing Site*			✓
CP-4 (3)	*Contingency Plan Testing | Automated Testing*			
CP-4 (4)	*Contingency Plan Testing | Full Recovery / Reconstitution*			✓
CP-5	**Contingency Plan Update**	✓	✓	✓
CP-6	**Alternate Storage Site**		✓	✓
CP-6 (1)	*Alternate Storage Site | Separation From Primary Site*		✓	✓
CP-6 (2)	*Alternate Storage Site | Recovery Time / Point Objectives*			✓
CP-6 (3)	*Alternate Storage Site | Accessibility*		✓	✓
CP-7	**Alternate Processing Site**		✓	✓
CP-7 (1)	*Alternate Processing Site | Separation From Primary Site*		✓	✓
CP-7 (2)	*Alternate Processing Site | Accessibility*		✓	✓
CP-7 (3)	*Alternate Processing Site | Priority of Service*		✓	✓
CP-7 (4)	*Alternate Processing Site | Configuration For Use*			✓
CP-7 (5)	*Alternate Processing Site | Equivalent Information Security Safeguards*			
CP-7 (6)	*Alternate Processing Site | Inability To Return To Primary Site*			
CP-8	**Telecommunications Services**		✓	✓
CP-8 (1)	*Telecommunications Services | Priority of Service Provisions*		✓	✓
CP-8 (2)	*Telecommunications Services | Single Points of Failure*		✓	✓
CP-8 (3)	*Telecommunications Services | Separation of Primary / Alternate Providers*			✓
CP-8 (4)	*Telecommunications Services | Provider Contingency Plan*			✓

Control No.	Control Name	Controls Baseline		
		Low	Mod	High
CP-8 (5)	*Telecommunications Services | Alternate Telecommunication Service Testing*			
CP-9	**Information System Backup**	✓	✓	✓
CP-9 (1)	*Information System Backup | Testing For Reliability / Integrity*		✓	✓
CP-9 (2)	*Information System Backup | Test Restoration Using Sampling*			✓
CP-9 (3)	*Information System Backup | Separate Storage For Critical Information*			✓
CP-9 (4)	*Information System Backup | Protection From Unauthorized Modification*	✓	✓	✓
CP-9 (5)	*Information System Backup | Transfer To Alternate Site*			✓
CP-9 (6)	*Information System Backup | Redundant Secondary System*			
CP-9 (7)	*Information System Backup | Two-Person Rule*			
CP-10	**Information System Recovery and Reconstitution**	✓	✓	✓
CP-10 (1)	*Information System Recovery And Reconstitution | Contingency Plan Testing*	Incorporated into CP-4		
CP-10 (2)	*Information System Recovery And Reconstitution | Transaction Recovery*		✓	✓
CP-10 (3)	*Information System Recovery And Reconstitution | Compensating Security Controls*		✓	✓
CP-10 (4)	*Information System Recovery And Reconstitution | Restore Within Time Period*			✓
CP-10 (5)	*Information System Recovery And Reconstitution | Failover Capability*			✓
CP-10 (6)	*Information System Recovery And Reconstitution | Component Protection*			
CP-11	**Predictable Failure Prevention**			✓
CP-11 (1)	*Predictable Failure Prevention | Transferring Component Responsibilities*			
CP-11 (2)	*Predictable Failure Prevention | Time Limit On Process Execution Without Supervision*			
CP-11 (3)	*Predictable Failure Prevention | Manual Transfer Between Components*			
CP-11 (4)	*Predictable Failure Prevention | Standby Component Installation / Notification*			

Appendix C—Physical and Environmental Protection Controls Summary

Control No.	Control Name	Controls Baseline		
		Low	Mod	High
PE-1	**Physical and Environmental Protection Policy and Procedures**	✓	✓	✓
PE-2	**Physical Access Authorizations**	✓	✓	✓
PE-2 (1)	*Physical Access Authorizations | Access By Position / Role*			
PE-2 (2)	*Physical Access Authorizations | Two Forms of Identification*			
PE-2 (3)	*Physical Access Authorizations | Restrict Unescorted Access*			
PE-3	**Physical Access Control**	✓	✓	✓
PE-3 (1)	*Physical Access Control | Information System Access*			✓
PE-3 (2)	*Physical Access Control | Facility / Information System Boundaries*			
PE-3 (3)	*Physical Access Control | Continuous Guards / Alarms / Monitoring*			
PE-3 (4)	*Physical Access Control | Lockable Casings*			
PE-3 (5)	*Physical Access Control | Tamper Protection*			
PE-3 (6)	*Physical Access Control | Penetration Testing*			
PE-4	**Access Control for Transmission Medium**		✓	✓
PE-5	**Access Control for Output Devices**		✓	✓
PE-5 (1)	*Access Control For Output Devices | Automated Access Control / Identity Linkage*			
PE-6	**Monitoring Physical Access**	✓	✓	✓
PE-6 (1)	*Monitoring Physical Access | Intrusion Alarms / Surveillance Equipment*		✓	✓
PE-6 (2)	*Monitoring Physical Access | Automated Intrusion Recognition / Responses*			✓
PE-6 (3)	*Monitoring Physical Access | Video Surveillance*			
PE-7	**Visitor Access Records**	✓	✓	✓
PE-7 (1)	*Visitor Access Records | Automated Records Maintenance / Review*			✓
PE-7 (2)	*Visitor Access Records | Physical Access Records*			
PE-8	**Power Equipment and Cabling**		✓	✓
PE-8 (1)	*Power Equipment And Cabling | Redundant Cabling*			
PE-8 (2)	*Power Equipment And Cabling | Automatic Voltage Controls*			
PE-9	**Emergency Shutoff**		✓	✓
PE-9 (1)	*Emergency Shutoff | Accidental / Unauthorized Activation*			
PE-10	**Emergency Power**		✓	✓
PE-10 (1)	*Emergency Power | Long-Term Alternate Power Supply - Minimal Operational Capability*			✓

Control No.	Control Name	Controls Baseline		
		Low	Mod	High
PE-10 (2)	*Emergency Power | Long-Term Alternate Power Supply -Self-Contained*			
PE-11	**Emergency Lighting**	✓	✓	✓
PE-11 (1)	*Emergency Lighting | Essential Missions / Business Functions*			
PE-12	**Fire Protection**	✓	✓	✓
PE-12 (1)	*Fire Protection | Detection Devices / Systems*		✓	✓
PE-12 (2)	*Fire Protection | Suppression Devices / Systems*		✓	✓
PE-12 (3)	*Fire Protection | Automatic Fire Suppression*		✓	✓
PE-12 (4)	*Fire Protection | Inspections*			
PE-13	**Temperature and Humidity Controls**	✓	✓	✓
PE-13 (1)	*Temperature And Humidity Controls | Automatic Controls*			
PE-13 (2)	*Temperature And Humidity Controls | Monitoring With Alarms / Notifications*			
PE-14	**Water Damage Protection**	✓	✓	✓
PE-14 (1)	*Water Damage Protection | Automation Support*			✓
PE-15	**Delivery and Removal**	✓	✓	✓
PE-16	**Alternate Work Site**		✓	✓
PE-17	**Location of Information System Components**		✓	✓
PE-17 (1)	*Location Of Information System Components | Facility Site*		✓	✓

Appendix D—Contingency Planning and the System Development Life Cycle (SDLC)

The system development life cycle (SDLC) refers to the full scope of activities conducted by University information system owners associated with a system during its life span. The life cycle begins with Initiation and ends with Disposition.[14] Although contingency planning is associated with activities occurring mostly in the Operation/Maintenance phase, identification and integration of contingency and continuity strategies at all phases of the information system life cycle allow the owner to build layered protection against risks and assist implementation of effective recovery strategies early on in the system development. This approach reduces overall contingency planning costs, enhances contingency capabilities, and reduces impacts to system operations when the contingency plan is implemented. This appendix introduces common ways in which contingency strategies can be incorporated throughout the SDLC. A summary of implementation periods for CP controls throughout the SDLC is provided in Table 3.

Initiation Phase

Contingency planning requirements should be considered when a new information system is conceived. During *Initiation*, early contingency planning considerations may become apparent as information system requirements are identified and matched to their related operational functions, a risk assessment is conducted to understand what the system will need protection against, and confidentiality, integrity, and availability objectives are set. High information system availability requirements may indicate that redundant, real-time mirroring at an alternate site and failover capabilities should be built into the system design. Similarly, if the system is intended as a virtual application, the design may need to include additional features, such as remote diagnostic or self-healing capabilities.

During the *Initiation*, the mission/business functions that the new information system will support should be evaluated to determine the users' recovery time requirements.

Contingency Planning controls to be addressed during this phase include:

- CP 6: Alternate Storage Site;
- CP 7: Alternate Processing Site;
- CP 8: Telecommunications Services; and
- CP 9: Information System Backup.

Development/Acquisition Phase

[14] There are several models for a system development life cycle. The model used for this appendix is consistent with a waterfall variant.

As initial concepts evolve into information system development, specific contingency solutions may be determined. As in the Initiation phase, technical contingency planning considerations in this phase should reflect system and operational requirements. The design should incorporate redundancy and robustness directly into the system architecture to optimize reliability, maintainability, and availability during the later Operation/Maintenance phase.

By considering the recovery strategy during the initial design, costs are reduced and problems associated with retrofitting or modifying the system during the Operation/Maintenance phase are minimized. Security controls are refined during the Development/Acquisition phase, lending an opportunity to ensure that contingency planning controls are appropriately addressed by the recovery strategy. If multiple applications are hosted within the new information system, recovery priority sequence for those applications should be set to assist with selecting the appropriate recovery strategy and sequencing for the contingency plan implementation.

Examples of contingency measures that should be considered in this phase are redundant communications paths, elimination of single points of failure, enhanced fault tolerance of network components and interfaces, power management systems with appropriately sized backup power sources, load balancing, and data mirroring and replication to ensure a uniformly robust system. If a recovery site is chosen as part of the strategy, requirements for the alternate site should be addressed in this phase.

Contingency Planning controls to be addressed during this phase include:

- CP 6: Alternate Storage Site;
- CP 7: Alternate Processing Site;
- CP 8: Telecommunications Services; and
- CP 9: Information System Backup.

Implementation/Assessment Phase

The recovery strategy selected is now documented into the formal Information System Contingency Plan in coordination with the System Test and Evaluation (ST&E) effort. As the system undergoes an initial testing, contingency strategies also should be exercised to resolve any issues with the procedures. Exercise results may prompt modifications to the recovery procedures and the contingency plan.

Contingency Planning controls to be addressed during this phase include:

- CP 2: Contingency Plan;
- CP 3: Contingency Training; and
- CP 4: Contingency Plan Testing and Exercise.

Operation/Maintenance Phase

When the information system is operational, users, administrators, and managers should maintain a test, training, and exercise program that continually validates the contingency plan procedures and technical recovery strategy. Exercises and tests should be conducted on a scheduled basis to ensure that procedures continue to be effective. Full and incremental backups should be routinely conducted, stored offsite, rotated, and periodically validated. The contingency plan should be updated to reflect changes to procedures based on lessons learned from tests, exercises, and actual disruptions. When the information system undergoes upgrades or other modifications, such as changes to external interfaces, these modifications should be reflected in the contingency plan. Coordinating and documenting changes in the plan should be performed in a timely manner to maintain an effective plan.

Contingency Planning controls to be addressed during this phase include:

- CP 2 Contingency Plan;
- CP 3: Contingency Training;
- CP 4: Contingency Plan Testing and Exercise;
- CP 5: Contingency Plan Update
- CP 9: Information System Backup;
- CP 10: Information System Recovery and Reconstitution; and
- CP 11: Predictable Failure Prevention.

Disposal Phase

Contingency considerations should not be neglected because an information system is retired and another system replaces it. Until the new system is operational and fully tested (including its contingency capabilities), the original system's ISCP should be maintained in a ready state for implementation. As legacy systems are replaced, they may provide a valuable capability as a redundant system if a loss or failure of the new information system should occur. In some cases, equipment parts (e.g., hard drives, power supplies, memory chips, or network cards) from hardware that has been replaced can be used as spare parts for new operational equipment. In addition, legacy information systems can be used as test systems for new applications, allowing potentially disruptive system flaws to be identified and corrected in a nonproduction environment.

Contingency Planning controls to be addressed during this phase include:

- CP 2 Contingency Plan;
- CP 9: Information System Backup; and
- CP 10: Information System Recovery and Reconstitution.

Table 6: CP Control Implementation in the SDLC

Control No.	Control Name	Initiation Phase	Acquisition / Development Phase	Implementation / Assessment Phase	Operation/ Maintenance Phase	Sunset
CP-1	Contingency Planning Policy and Procedures	Defined by UConn				
CP-2	Contingency Plan			✓	✓	✓
CP-3	Contingency Training			✓	✓	
CP-4	Contingency Plan Testing			✓	✓	
CP-5	Contingency Plan Update				✓	
CP-6	Alternate Storage Site	✓	✓			
CP-7	Alternate Processing Site	✓	✓			
CP-8	Telecom Services	✓	✓			
CP-9	Information System Backup	✓	✓		✓	✓
CP-10	Information System Recovery and Reconstitution				✓	✓
CP-11	Predictable Failure Prevention				✓	

Appendix E—Glossary

Backup: A copy of files and programs made to facilitate recovery if necessary.

Business Continuity Plan (BCP): The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business functions will be sustained during and after a significant disruption.

Business Impact Analysis (BIA): An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

Cold Site: A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site.

Computer: A device that accepts digital data and manipulates the information based on a program or sequence of instructions for how data is to be processed.

Confidential Data: Information that requires the highest level of privacy and may not be released.

Contingency Planning: See Information System Contingency Plan.

Continuity of Operations (COOP) Plan: A predetermined set of instructions or procedures that describe how an organization's mission-essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations.

Disaster Recovery Plan (DRP): A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.

Disruption: An unplanned event that causes an information system to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

Hot Site: A fully operational offsite data processing facility equipped with hardware and software, to be used in the event of an information system disruption.

Impact: The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Impact Level: High, Moderate, or Low security categories of an information system which classify the intensity of a potential impact that may occur if the information system is jeopardized.

Incident Response Plan: The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's information system(s).

Information System: A discrete set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System Contingency Management Plan (ISCP): policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters.

Maximum Tolerable Downtime: The amount of time mission/business process can be disrupted without causing significant harm to the organization's mission.

Protected Data: Information that must be appropriately protected to ensure a lawful or controlled release (e.g. Connecticut Freedom of Information Act requests).

Public Data: Information that is open to all users, with no security measures necessary.

Reciprocal Agreement: An agreement that allows two organizations to back up each other.

Recovery Point Objective: The point in time to which data must be recovered after an outage.

Recovery Time Objective: The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business functions.

Resilience: The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning.

Risk Management: The process of managing risks to University operations (including mission, functions, image, or reputation), University assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.

Security Controls: The management, operational, and technical controls prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

System Development Life Cycle (SDLC): The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

Warm Site: An environmentally conditioned workspace that is partially equipped with information systems and telecommunications equipment to support relocated operations in the event of a significant disruption.

Appendix F—Acronyms

Selected acronyms used in this document are defined below.

BCP	Business Continuity Plan
BIA	Business Impact Analysis
CCP	Crisis Communication Plan
CIKR	Critical Infrastructure And Key Resources
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIRP	Cyber Incident Response Plan
CISO	Chief Information Security Officer
COOP	Continuity Of Operations
CP	Contingency Plan/Contingency Planning
DRP	Disaster Recovery Plan
IS	Information System
ISA	Interconnection Security Agreement
ISCP	Information System Contingency Plan
ISSM	Information System Security Manager
ISSO	Information System Security Officer
MAO	Maximum Allowable Outage
MEF	Mission-Essential Functions
MOA	Memorandum Of Agreement
MOU	Memorandum Of Understanding
MTD	Maximum Tolerable Downtime
OEP	Occupant Emergency Plan
PMEF	Primary Mission-Essential Functions
POC	Point Of Contact
RMF	Risk Management Framework
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SDLC	System Development Life Cycle
SLA	Service-Level Agreement
TT&E	Test, Training, And Exercise