FEATURE

Download a Contingency Plan Workbook template (Excel)

Information System Contingency Planning Guidance

When planning information security for a system, it is essential to remember to include contingency planning because it provides the resilience needed to respond to technical disruptions and ensure the system is available. The critical planning component is an information system contingency plan (ISCP), which contains information about the system hardware and software, application and data backups, dependent processes, data interfaces, support staff and vendors, recovery priorities, and plan maintenance.

Metrics to support the need for an ISCP can be found in the white paper *The State of IT Resilience*, which states that 91 percent of respondents have experienced tech-related business disruption in the past two years, 91.2 percent of respondents have experienced some type of business disruption in the past two years and 57.8 percent of respondents believe their data protection requirements will be more complex in the coming years.[1] These metrics are significant and indicate a critical need for an ISCP.

Larry G. Wlosinski, CISA, CRISC, CISM, CDPSE, CAP, CBCP, CCSP, CDP, CIPM, CISSP, ITIL v3, PMP
Is a senior consultant at Coalfire-Federal. He has more than 21 years of experience in IT security and privacy and has spoken at US government and professional conferences on these topics. He has written numerous magazine and newspaper articles, reviewed various ISACA® publications, and written questions for the Certified Information Security Manager® (CISM®) and Certified in Risk and Information Systems Control® (CRISC®) examinations.

The consequences of tech-related business disruptions include:

- Employee overtime
- Direct cost to recover
- Loss of employee productivity
- Unrecoverable data
- Direct loss of revenue
- Damage to enterprise reputation
- Permanent loss of customers
- Noncompliance with government regulations (and possible fines)

Disruptions to an enterprise can come from technologies, new products or services, new business models, customer requirements, and competitors. A significant disruption to organizations is the loss of data, and the top reasons for unrecoverable data loss include: the loss of data occurred between backups, there was a backup/recovery system failure, human errors related to system processing, and lost or damaged tapes.

Information systems that are critical, important, centralized and support the organization in any way should have contingency plans. These information systems provide a degree of resilience to the organization and help ensure that the services provided will be available.

Threats and Areas of Risk

Threats to computer systems can be categorized as illustrated in **figure 1**. The effect of these threat events range from short to long term depending on the organization's ability to recover.

Figure 1—Threats With Degree of Control		
Threat Category	**Examples**	**Degree of Control**
Natural	Hurricane, tornado, fire (direct or nearby), ice, wind, lightning, extreme heat, snow, flood	Not controllable
Building environmental	Heating, ventilation and air conditioning system (HVAC); power; building deterioration (e.g., electrical, pipes, roof)	Controllable
Intentional internal staff	Disgruntled employee, contractor, dishonest employee, political activist, extorted or corrupted individual, work stoppage	Difficult to control
Unintentional internal staff	Undertrained employee, irresponsible employee, apathetic employee, lack of separation of duties, loss of organization's computing devices	May be controllable
External actor	Hacker, cracker, criminal, terrorist, espionage, former employee	Not controllable, but protective measures can be implemented
Locational	Biological, bomb/explosion, chemical, civil disturbance, community disaster, metropolitan commuting failure	Not controllable
Internal computer	Hardware or software failure, new technology (i.e., unknown vulnerabilities), unpatched software, misconfigured systems, insufficient traffic and log activity monitoring, injection flaws, malware/virus infection	Controllable
External cyber	Denial-of-service attack, telecommunications loss, ransomware, data breach, partner or supplier compromise, cloud provider security compromise/failures	Not controllable, but preventive or proactive measures can be implemented
Other	Health/pandemic, kidnapping/hostage, airborne crash (e.g., airplane, meteor)	Not controllable

Planning Considerations

Before creating an ISCP, an organization's policies must be in place to ensure support from top management and collaboration across departments.

The objective of an ISCP is to address and respond to threats to the computer system. When planning, it is necessary to be aware of the current system environment and the capabilities of the recovery site. The recovery site can be hot, warm, cold or mobile.

Hot sites are facilities that mirror the primary production center. Warm sites are sites where not all the hardware and supporting software are current and active. A warm site provides space, utilities and equipment, but requires installation of software and data to be operational. A cold site has little or no hardware equipment installed. A mobile site is a mobile structure that has computing infrastructure or can quickly be configured to customer requirements.

Key areas of concern include site readiness to run the systems, application status as it applies to installation, data communications capability, data for the application(s) and cost. Costs and capabilities vary depending on square footage, cooling, power, utilities, Internet access speed, number of units, up-front acquisition, ongoing maintenance and operational costs. **Figure 2** provides some comparison of disaster recovery sites.

Prevention

Another planning aspect is preventing events that can damage the system (and affect the organization) due to weaknesses in the environment (physical and digital). Examples include network compromise, malware attack and ransomware. Prevention is an important aspect of contingency planning because it helps minimize the need to use the ISCP. Having a defense-in-depth (DiD) security architecture is a good practice for preventing loss due to threats.[2] DiD is an approach to cybersecurity where multiple defensive mechanisms are in place to protect the systems, devices, data and facility as necessary.

Figure 2—Disaster Recovery Site Type Summary				
Area of Concern	**Hot**	**Warm**	**Cold**	**Mobile**
Readiness	Minutes to hours	Hours to days	Days to weeks	Days to weeks
Application system status	Loaded and ready	Present but not ready	Absent; must be purchased and installed	Hardware must be purchase and installed; software must be loaded
Data communications	Ready to go	Capable	Little to none	Little to none
Application data	Up to date	Not up to date; must be refreshed	Data not present or loaded	Not present; must be loaded
Up front cost	Very high	Moderate	Low	High

Cost and Budget
Another important planning consideration is the cost of establishing the contingency plan and what the budget will allow. Cost and budget considerations can be high because they can include vendor readiness and resilience, additional/mirrored system hardware and software, travel for support staff, labor, contractors, testing, and supplies. If there are dependencies, it is necessary to make sure the interfacing system(s) have a budget for any requirements they may need. This can help an organization avoid a recovery situation where it is unable to recover due to a dependency that may be missing or unavailable.

Agreements
Agreements are needed to support the ISCP because they are critical to system recovery. Example agreements include service level agreements (SLAs), telecommunication agreements, interconnection agreements, and agreements with the disaster recovery team and alternate recovery site. When developing agreements with vendors, include the following system recovery considerations:

- Contract/agreement duration
- Cost/fee structure
- Site/facility priority access and use
- Site guarantee
- Contract/agreement termination
- Guarantee of compatibility
- Information system requirements
- Change management and notification requirements
- Security requirements
- Staff support provided/not provided
- Facility services (e.g., onsite office equipment, cafeteria)
- Testing (i.e., scheduling, availability, test time duration, additional testing)
- Records management
- Workspace requirements (e,g., chairs, desks, telephones, personal computers)
- Supplies (e.g., office supplies)
- Additional costs not covered

Backups
Having system and data backups are key to system resilience because without them the organization would not be able to recover from a catastrophic or disruptive event. Data backup options[3] include removable media, redundancy, external hard drives, hardware appliances, backup software and backup services. The 3-2-1 backup strategy is a best practice and consists of:

- **Three copies of data**—Each copy should include the original data and two duplicates. This ensures that a lost backup or corrupted media does not affect recoverability.
- **Two different storage types**—Having varied storage types reduces the risk of failures related to a specific medium by using two different technologies. Common choices include internal

and external hard drives, removable media, and cloud storage.

- **One copy offsite**—Having an offsite copy eliminates the risk associated with a single point of failure. Offsite duplicates are needed for robust disaster and data backup recovery strategies and can allow for failover during local outages.

In general, server backup solutions should include the following features:

- **Support for diverse file types**—In particular, solutions should support documents, spreadsheets, media and configuration files.
- **Backup location**—The solution should provide backup support to a variety of locations and media, including on- and offsite resources.
- **Scheduling and automation**—In addition to enabling manual backups, solutions should support backup automation through scheduling. This helps ensure that there is always a recent backup and that backups are created consistently.
- **Backup management**—Managing the life cycle of backups includes the number of backups stored and length of retention time. The solution should also enable easy export of backups for transfer to external resources or for use in migration.
- **Partition selection**—Partitions are isolated segments of a storage resource and are often used to separate data within a system. A server backup solution should enable independent data backup and restoration of partitions.
- **Data compression**—To minimize the storage needed for numerous backups, the solution should compress backup data.
- **Backup type selection**—There are a variety of backup types, including full, differential and incremental backups. Differential backups create a backup of changes since the last full backup, while an incremental backup records the changes since the last incremental backup. Using the backup types can help reduce the size of the backups and speed up backup time.
- **Scaling**—Backups should not be limited by the volume of data on the servers. Solutions should scale as data does and support backups of any size.

> "HAVING VARIED STORAGE TYPES **R**EDUCES THE RISK OF FAILURES RELATED TO A SPECIFIC MEDIUM BY USING TWO DIFFERENT TECHNOLOGIES."

There are many vendors[4, 5, 6, 7, 8, 9] that provide backup software and services. Practitioners should plan to research vendors before committing to one or more.

Business Impact Analysis

A business impact analysis (BIA) is part of an ISCP. The BIA document helps to prioritize the recovery activities and should define the following metrics:

- **Maximum tolerable downtime (MTD)**—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.
- **Recovery time objective (RTO)**—The maximum amount of time that a system resource can remain unavailable before there is an unacceptable effect on other system resources, supported mission/business processes and the MTD.
- **Recovery point objective (RPO)**—"The RPO represents the point in time, prior to a disruption or a system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. Unlike RTO, RPO is not considered as part of MTD. Rather, it is a factor of how much data loss the mission/business process can tolerate during the recovery process."[10]

The BIA for a large system is typically a standalone document and should contain an overview of the system and its interfaces, the purpose of the system, the system description, and information about the data collected. The BIA document should also include the system purpose and criticality, associated metrics (i.e., MTD, RTO, RPO), outage impact, resource requirements (e.g., hardware, software) and recovery priorities. Common impact categories are severe (e.g., temporary staffing, overtime, fees are greater than US$1 million), moderate (e.g., fines, penalties, liabilities potential US$550,000) and minimal (e.g., new contracts,

Enjoying this article?

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

supplies costing more than US$75,000). If the BIA is conducted for a small system, the information could be an appendix in the ISCP as opposed to a standalone document.

ISCP Contents

The organization's ISCP should contain an introduction, concept of operations, description of the three phases of recovery and related appendices.

Introduction

The introduction describes the objectives of the ISCP, its scope and any assumptions regarding system interfaces, hardware and software components, assumptions of what is not covered (e.g., other systems), situations that are not applicable, and relationship to other plans.

Concept of Operations

The concept of operations section contains a system description, an overview of the three phases of the plan, and the supporting roles and responsibilities.

Three Phases

The three phases include activation and notification steps and processes, recovery requirements and reconstitution activities as illustrated in **figure 3**.

Appendices

The appendices should include contact information for support and management personnel and vendors, recovery and alternate processing site procedures, system validation testing guidance, the location of alternate storage and processing site(s), information about the supporting applicable telecommunications companies and agreements, architectural and data flow diagrams, an inventory of the hardware and software, an interconnections table, an ISCP backup test, a document maintenance schedule, a list of associated plans and procedures, the BIA, and a document change page.

ISCP Coordinator Responsibilities

The person responsible for the contingency plan is often called the contingency plan coordinator or manager. That person is responsible for the alternate site contract, test times, offsite storage contract, associated software licenses, memorandums of understanding (MOUs), vendor support SLAs, hardware and software inventory and requirements, system interconnection security agreements (ISAs), security requirements, recovery strategy, training events and materials, testing scope, and updating other related plans.

The organization's ISCP can include responsibilities for other system support individuals or teams, as applicable. The teams would cover management, damage assessment, server restoration, application restoration, database restoration, security and help/service desk.

Training

Training is another important aspect of a contingency planning program. Training ensures that the response team knows its responsibilities, how and where to perform its tasks, what is in an

Figure 3—ISCP Phase Summary

Phase	Title	Tasks in Phase
1	Activation and notification	Discusses: • Activation criteria and procedure • Notification of all affected parties • Outage assessment
2	Recovery	Describes: • Sequence of recovery activities • Recovery procedure • Recovery escalation notices • Awareness
3	Reconstitution	Covers returning to normal operations by: • Validating data • Testing system functionality • Declaring system recovery • Notifying users • Removing and deactivating any temporary system and data backups

ISCP, and the order of recovery steps. Training considerations include cross-team coordination and communication, reporting procedures, security requirements, team-specific processes, and individual responsibilities.

To ensure that the ISCP is complete and can be effectively used, periodic testing is required with varying scenarios. Periodic exercises and testing are necessary as changes in technology (i.e., hardware, software processing environment), staffing turnover, changes in responsibilities, new hires, and significant changes to the application can occur, which can lead to necessary changes in the ISCP. Types of scenarios include short-term (less than one month) outage, long-term (more than three month) outage, local (site or campus) outage, regional issue impact, enterprisewide issue impact and cascading impact potential. Example scenarios can be a ransomware event, a malware infection, changed data files found upon review of audit logs, suspicious activity uncovered during a threat hunting activity or lost backup files.

Testing/Exercises

The objectives of testing/exercising the ISCP are to:

- Keep personnel assignments and notification/call lists current
- Acquaint new employees with responsibilities
- Verify backup storage procedures
- Verify that primary and backup sites have the same configurations
- Train staff on their assignments and procedures
- Test recovery procedures and checklists
- Identify and correct process weaknesses and technical vulnerabilities
- Identify and mitigate new threats

There are two types of exercises: tabletop and function.

Tabletop exercises are:

> *[D]iscussion-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.*[11]

> "TO ENSURE THAT THE ISCP IS COMPLETE AND CAN BE EFFECTIVELY USED, PERIODIC TESTING IS REQUIRED WITH VARYING SCENARIOS."

This exercise helps to enforce knowledge of the organization's ISCP and keep everyone involved informed of their responsibilities.

Functional exercises:

> *[A]llow 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).*[12]

The functional exercise is a full or partial test to ensure that the software, data files and restoration mechanisms are unable. Sometimes the restoration environment may become out of sync with changes in the hardware or software.

Suggested scenarios that can be used for tabletop exercises are:

- A disgruntled employee starts a data center fire
- An explosion at a nearby chemical plant releases deadly toxins
- A pandemic hits
- A natural disaster (e.g., tornado, hurricane) occurs
- Water floods the basement where staff members work

Variables that can be added to customize the tests include a power outage, loss of equipment or data, loss of connectivity, unavailability/loss of staff, staff

> "THE ABILITY TO RECOVER FROM A VARIETY OF THREATS DEPENDS ON THE ORGANIZATION'S ISCP."

turnover, level of testing (one sample, partial, full), stale documentation, contractual support issues, conflicting priorities (within the organization or with vendors), problems with on/offsite work environment, and issues with alternate location.

After testing is complete, it is necessary to write an After Action Report (AAR). The AAR documents what occurs during the tabletop exercises and functional testing. It should contain an executive summary, overview about the exercise (i.e., date, participants, scenario, description), the goals and objectives, a synopsis about the test, an analysis of the exercise, lessons learned, exercise concerns, action items, and recommendations.

The lessons learned should identify what went right, what went wrong, what should have been done differently, preventive measures and recommendations, follow-up actions needed (i.e., improvements to the plan, training, exercise), and changes needed to the ISCP.

ISCP Maintenance

Maintaining the organization's ISCP requires periodic reviews (at least annual or when a significant change to the system occurs), particularly for the areas that may change frequently. The areas that change are: operational requirements; information security requirements; technical procedures; hardware, software and other equipment inventory; names and contact information of team members and vendors (including alternate and offsite vendors) and their requirements; and associated recovery records (electronic and hard copy) of the procedures, backups and related documentation.

Conclusion

An ISCP is an important aspect of information security planning. The ability to recover from a variety of threats depends on the organization's ISCP. Therefore, it is important to research, develop a comprehensive plan, test it regularly, update it on a regular basis and train associated personnel. In a time of severe disruption or disaster, the ISCP will be the best guidance for application recovery.

Endnotes

1 IDC, *The State of IT Resilience Report 2019*, USA, 2019, *https://www.zerto.com/page/idc-the-state-of-it-resilience-report-2019/?z_asset=&z_campaign=2019_Annual_Adwords_The_State_of_IT_Resilience&z_content=White_Paper&z_leadsource=Google_Adwords&z_referrer=Adwords&z_source=7012I000001SPH8QAO&gclid=EAIaIQobChMIkbTZ3o-47QIVS42GCh21YACtEAAYAiAAEgKjlfD_BwE*

2 Wlosinski, L. G.; "Data Loss Prevention—Next Steps," *ISACA® Journal*, vol. 1, 2018, *https://www.isaca.org/archives*

3 Cloudian, "Data Backup in Depth: Concepts, Techniques and Storage Technologies," *https://cloudian.com/guides/data-backup/data-backup-in-depth/*

4 Mordy, J.; "10 Best Free and Open Source Backup Software," Goodfirms, *https://www.goodfirms.co/blog/best-free-open-source-backup-software*

5 Chang, J.; "15 Best Backup Software Systems: Comparison of Popular Solutions," FinanceOnline, *https://financesonline.com/top-15-backup-software-systems-comparison-popular-solutions/*

6 Fisher, T.; "33 Best Free Backup Software Tools," Lifewire, 1 April 2021, *https://www.lifewire.com/free-backup-software-tools-2617964*

7 Black, C.; "The Best Backup Software in 2021," *The TechLounge*, 7 April 2021, *https://www.thetechlounge.com/best-backup-software/*

8 Predictive Analysis Research, "Top 10 Backup Software," *https://www.predictiveanalyticstoday.com/top-backup-software/*

9 Top Best Alternatives, "Data Backup," *https://www.topbestalternatives.com/data-backup/*

10 Swanson, M.; P. Bowen; A. Phillips; D. Gallup; D. Lynes; *Contingency Planning Guide for Federal Information Systems*, National Institute of Standards and Technology (NIST), NIST Special Publication (SP) 800-34 Rev. 1, USA, 2010, *https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final*

11 *Op cit* Swanson, Bowen, Phillips, Gallup, Lynes

12 *Ibid.*