GIS Odyssey Journal

2024 • Volume 4 • Number 1

https://doi.org/10.57599/gisoj.2024.4.1.39

Maciej Kiedrowicz[1], Jerzy Stanik[2]

GIS INFORMATION SYSTEM CONTINGENCY PLAN AS A KEY ARTIFACT IN THE CYBERSECURITY MANAGEMENT LIFECYCLE

Abstract: The article discusses the methodology of conducting a contingency planning process that an organization can use to develop and maintain a viable contingency planning program for IT/computer GIS systems. The process steps (seven steps) are designed to be integrated into each stage of the GIS lifecycle. This document guides building the organizational chart/structure of a contingency planning team and the persons/roles responsible for preparing and maintaining information system contingency plans (ISCPs). In addition, the article discusses the basic components and processes of a contingency plan, highlights specific considerations and issues related to contingency planning relating to different types of GIS platforms, and provides elements of good practice to help readers develop their ISCPs.

Keywords: GIS, contingency plan, contingency planning team

Received: 07 May 2024; accepted: 06 July 2024

[1] Military University of Technology, Faculty of Cybernetics, Warsaw, Poland, ORCID ID: https://orcid.org/0000-0002-4389-0774, email: maciej.kiedrowicz@wat.edu.pl

[2] Military University of Technology, Faculty of Cybernetics, Warsaw, Poland, ORCID ID: https://orcid.org/0000-0002-0162-2579, email: jerzy.stanik@wat.edu.pl

Introduction

GIS data/information assets and computer systems are some of the most valuable assets of GIS organizations or users today. Their protection has become a priority, and the business depends on its effectiveness – its maintenance and success (Coresite, 2016).

In the face of growing cyber threats and increasing financial and reputational losses to organizations due to cyberattacks, a contingency plan for the GIS information system and IT infrastructure security have become a priority for IT departments and cybersecurity teams around the world. In addition, the introduction of new compliance standards, e.g. NIS 2 directives, GDPR, and NIST, imposes new obligations on GIS class systems, increasing their responsibility for reliability, accountability, non-repudiation, integrity, availability, and confidentiality of data.

Contingency planning for a GIS information system refers to a coordinated strategy that includes plans, procedures, and technical measures that enable the recovery of information systems, operations, and geodata after a disruption:

- Contingency planning typically includes one or more of the following approaches to restoring disrupted services:
- Restore IT systems using alternative hardware;
- Recovering the functioning of IT systems in an alternative location (typically only acceptable in the event of long-term disruption or those that physically affect the facility).

Implementation of appropriate contingency planning safeguards based on the level of impact of the IT system on cybersecurity.

This document has been created for managers and people responsible for IT systems or the security of these systems. It also assists management personnel in crises, who coordinate unforeseen situations at the organizational level with activities that support the contingency planning of the IT system.

The recipients of this article may be people who are just learning the principles and assumptions of building GIS information security, in particular:

- GIS, information security, risk management, and oversight personnel, including CIOs, SAISOs, Information Systems Administrators, GIS hardware and software developers, system integrators, and purchasing or procurement personnel;
- Individuals responsible for security assessment and monitoring, including auditors, GIS assessors, security assessors, independent verifiers, validators, and analysts.

This article is also intended to logically guide the reader through the process of developing a contingency plan. The resulting contingency plan serves as a "user manual" to execute the strategy in the event of a GIS disruption.

Background

GIS computer systems are susceptible to various types of interference, from mild (e.g. short-term power outage, disk failure) to serious (e.g. equipment damage, flood, fire). High vulnerability can be minimized or eliminated by managerial, operational, or technical safeguards to achieve resilience to such events, but it is virtually impossible to completely eliminate the impact of all threats.

Contingency planning aims to reduce the risk of system and service unavailability by providing effective and efficient solutions to increase system availability. GIS contingency planning encompasses a wide range of activities to maintain and recover critical system services after an emergency. Contingency planning in the GIS information system is a much broader range of activities related to security and crisis management, which concern the continuity of organizational and information processes, than disaster recovery planning and incident management.

In conclusion, with respect to GIS class systems, an organization would use a set of plans to adequately carry out response, recovery, and continuity activities in the event of disruptions affecting GIS computer systems, GIS purpose-related processes, staffing, and headquarters. Because there is an intrinsic link between the GIS and the processes it supports in the organization's operations, there must be coordination between all plans when developing and updating plans to ensure that recovery strategies and supporting resources do not negate each other or duplicate efforts.

Materials and methodology

Literature review. In this review, the authors have taken into account the latest compliance standards, standards, codes of practice, and specialist journals on cybersecurity, information security, security plans, and contingency plans published in the NCS (National Cybersecurity Standards) and NIST (National Institute of Science and Technology) knowledge bases, peer-reviewed scientific journals, and doctoral dissertations – hereinafter referred to as "articles".

Four main criteria were used in the process of this review when considering the inclusion of articles related to building IT contingency plans:

1. Guides and methodological journals that will facilitate the development of contingency plans for the GIS system based on elements of good practices.
2. Articles that describe the elements of successful implementation of contingency plans or business continuity management of information systems.
3. Articles that described the benefits of implementing business continuity management systems and contingency plans for business success – reviewed articles that met at least one of these two criteria.
4. The articles were published no earlier than 2014.

This review does not include articles that only describe the technical aspects of contingency planning (for example, malware protection), without discussing the relationship to other non-technical aspects of GIS. The reason for this exclusion is that there are many articles and studies that cover the technical aspects of building

a contingency plan – this area is much better explored than the managerial or strategic aspects of contingency planning or GIS business continuity. Contingency planning documents, knowledge security, were also taken into account, even though the term knowledge is a broader concept than information or data, as knowledge includes "experiences, values, contextual information, and expert insights" (Ahmad et al., 2014). Papers on contingency planning are also included.

Research methodology and methods. The review of source materials and journals was carried out in three phases:

- in the first phase, the intention was to review standards and methodological guides that will facilitate contingency planning and build an effective contingency plan based on the practice used in the US federal administration – the NIST standard (NSC 800-18; NSC 800-34, NSC 800-60],
- in the second phase, the intention was to clarify the research task by reviewing articles from the best journals in the field of information systems GIS (European Journal of Information Systems, Information Systems Journal, Information Systems Research, Journal of AIS – Journal of the Association for Information Systems, Journal of Information Technology, Journal of MIS – Journal of Management Information Systems), Journal of Strategic Information Systems and MIS Quarterly),
- in the third phase, the intention was to explore the topics in more depth through scientific articles other than those from the most frequently mentioned journals,
- in the fourth phase, it was monitored whether the recently published scientific papers explored the topics on which the authors focused their attention in more depth.

In parallel with the literature review, a pilot study was conducted, interviewing cybersecurity and contingency planning specialists. This research strategy is qualitative and interpretive (Eskola, 1998). Empirical data include twelve semi-structured thematic interviews (Kovalainen, 2008). Respondents were selected using the method of purposive sampling (Patton, 2002). Using knowledge and experience in GIS lifecycle, contingency planning, and cybersecurity, a group of high-ranking authorities in research, data analytics, and consulting was selected as a requirement for participation. The survey prioritized respondents with in-depth knowledge of contingency planning security technologies. Respondents' job descriptions were a mix of executives, ranging from analyst/manager to senior executives.

Result and discussion

Elements of good practice in the area of contingency planning

It is widely believed that 'good practices' are actions that produce concrete and positive results, are sustainable and repeatable, and can be applied under similar conditions elsewhere or by other actors (Dobre praktyki (*Good practices*)).

They are often used to improve compliance standards, business frameworks, improve the quality of human capital, and teach how to benefit from the experiences of others. Good

practices can cover various areas of life, including contingency planning, and are not a common solution, but should contain elements of innovation and serve as a model for others (Czym są dobre praktyki? (*What are good practices?*).

Good practices in the area of contingency planning of the GIS information system are crucial to ensure the continuity of its operations in the face of unforeseen events. Table 1 contains several important aspects – good practices related to contingency planning.

Table 1. Examples of good practice in the area of contingency planning

Name	Description
Contingency Planning Policy Statement	This is the first step in developing an IT GIS contingency plan. These policies can exist at the organization and/or GIS level. The declaration should define the overall goals of contingency planning and identify management, roles and responsibilities, resource requirements, testing, training, and exercise schedules, as well as service plans and minimum requirements for backup frequency.
Basic Steps of the Contingency Planning Process	Information system contingency planning refers to the dynamic development of a coordinated strategy for recovering information systems, operations, and data after a disruption occurs. The planning process requires seven steps: the development of a contingency planning policy statement; conducting a business impact analysis (BIA); identifying safeguards; developing a recovery strategy; development of an IT system contingency plan (ISCP); testing the feasibility of the plan and train staff; keeping the plan up-to-date.
The relationship between the risk management framework and the contingency planning of the system	The Risk Management Framework (RMF) covers a wide range of activities aimed at identifying, controlling, and mitigating risks to an information system during the system lifecycle. One of the activities is the development of the ISCP.
Contingency Planning in the Face of a Cyber Resilience Program	The goal of a resilient GIS is to always function continuously during any type of disruption. Resilient GIS are constantly working to adapt to changes and risks that may affect their ability to maintain business continuity. Risk management, contingency planning, and continuity planning are individual GIS security activities.
System Lifecycle Contingency Planning (SDLC)	Although contingency planning is linked to the activities that occur in the operation/maintenance phase of the system, contingency measures should be identified and integrated in all phases of the SDLC. Incorporating contingency planning into the SDLC reduces overall contingency planning costs, increases contingency capabilities, and reduces the impact on system operations when a contingency plan is deployed.
Contingency planning of the IT system and GIS security policy	In addition to integrating contingency planning with the SDLC, GIS information system contingency planning should be coordinated with cybersecurity policy. Applying appropriate system safeguards can help protect against malicious code or attacks that could compromise the availability of the GIS system and are closely coordinated with incident response procedures. The ISCP should be closely coordinated with all other disaster preparedness plans associated with the GIS information system or the interconnected systems and business processes of the GIS-based organization.
ISCP Update	An up-to-date ISCP is essential for successful recovery operations. As a rule, ISCP should be checked for accuracy and completeness at least once a year, as well as after significant changes to any ISCP component, system, business processes supported by the system, or resources used for recovery procedures. Maintenance schedules should be specified in the ISCP Policy Statement.
ISCP Testing	Testing helps assess the feasibility of the plan's procedures, determine the ability of recovery personnel to implement the plan and identify gaps in the plan. Testing should be done when significant changes are made to the IT system or ISCP. Each ISCP component must first be tested individually and then as a whole to confirm the accuracy of the recovery procedures and overall effectiveness. The schedule of tests and exercises should be provided in the ISCP policy statement.

Source: Own study

GIS Contingency Planning Process

The first step in the contingency planning process is to develop a contingency planning policy statement supported by senior management (usually the head of the business unit. The policy should outline the overall objectives of GIS in the event of a disaster and should outline the organizational framework and responsibilities for contingency planning for the GIS information system. The policy statement should also address roles and responsibilities. The policy should be supported by procedures including training requirements, frequency of backups, off-site data storage, exercise planning, testing, and maintenance.

Contingency planning in GIS is a much broader scope of information security management activities. GIS IT contingency planning is a modular component of a broader contingency planning (CP) and continuity of operations planning (COOP) process that includes IT, business processes, risk management, financial management, crisis communications, personnel and property security, and continuity of management. Each of these element's functions on its own, but together they form a coordinated synergy that effectively and efficiently protects the entire organization/GIS. The contingency planning process for a GIS information system details the basic steps and planning principles implemented in the various phases of the system life cycle necessary to develop an effective failure management capability (Fig. 1).

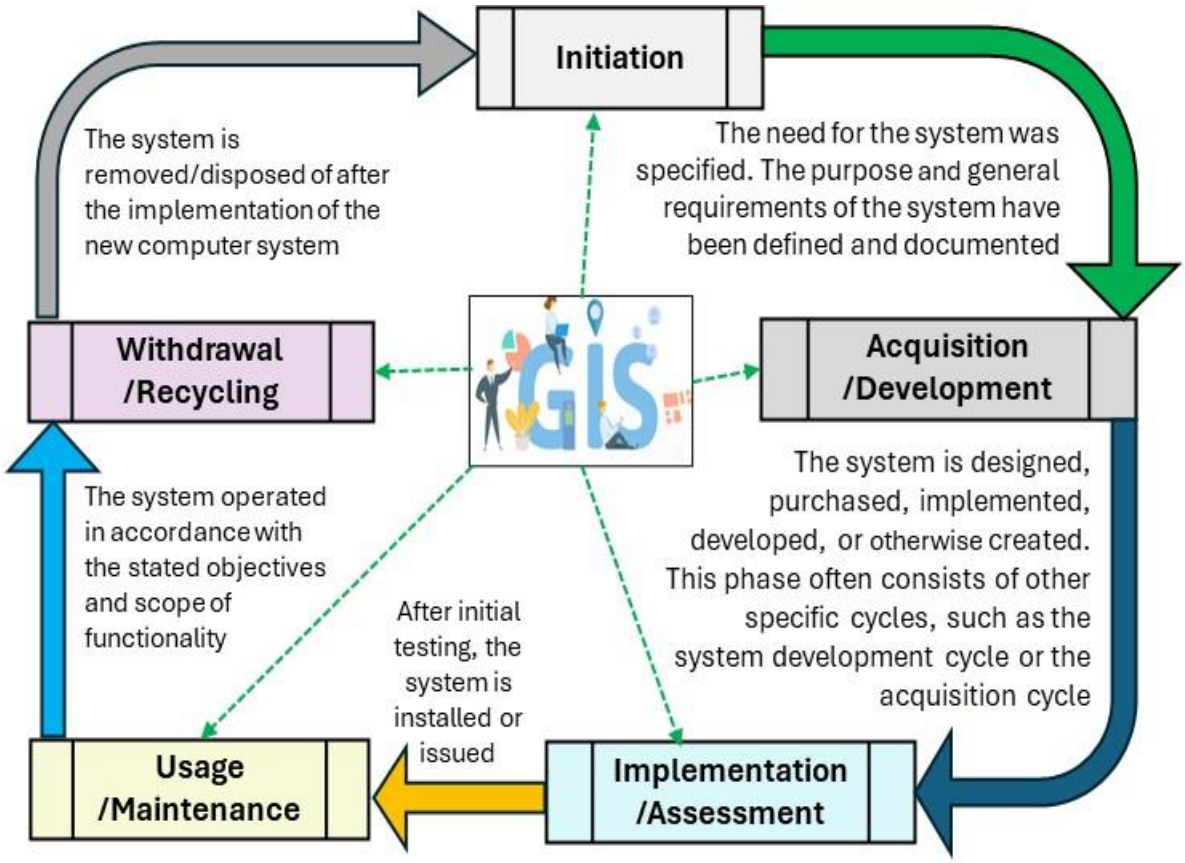

Fig. 1. System Development Life Cycle – SDLC
Source: Own study based on: NIST SP 800-100

In the contingency planning process, the following steps can be distinguished against the background of the GIS lifecycle (Fig. 2):

1. Developing a contingency planning policy;
2. Conduct a Business Impact Analysis (BIA);
3. Identification of preventive safeguards;
4. Creation of contingency strategies;
5. Development of an IT system contingency plan;
6. Scheduling tests, training and exercises;
7. Ensuring plans are kept up to date.

Figure 2 illustrates the contingency planning activities performed in each of these seven steps that need to be included in the System Development Life Cycle (SDLC).

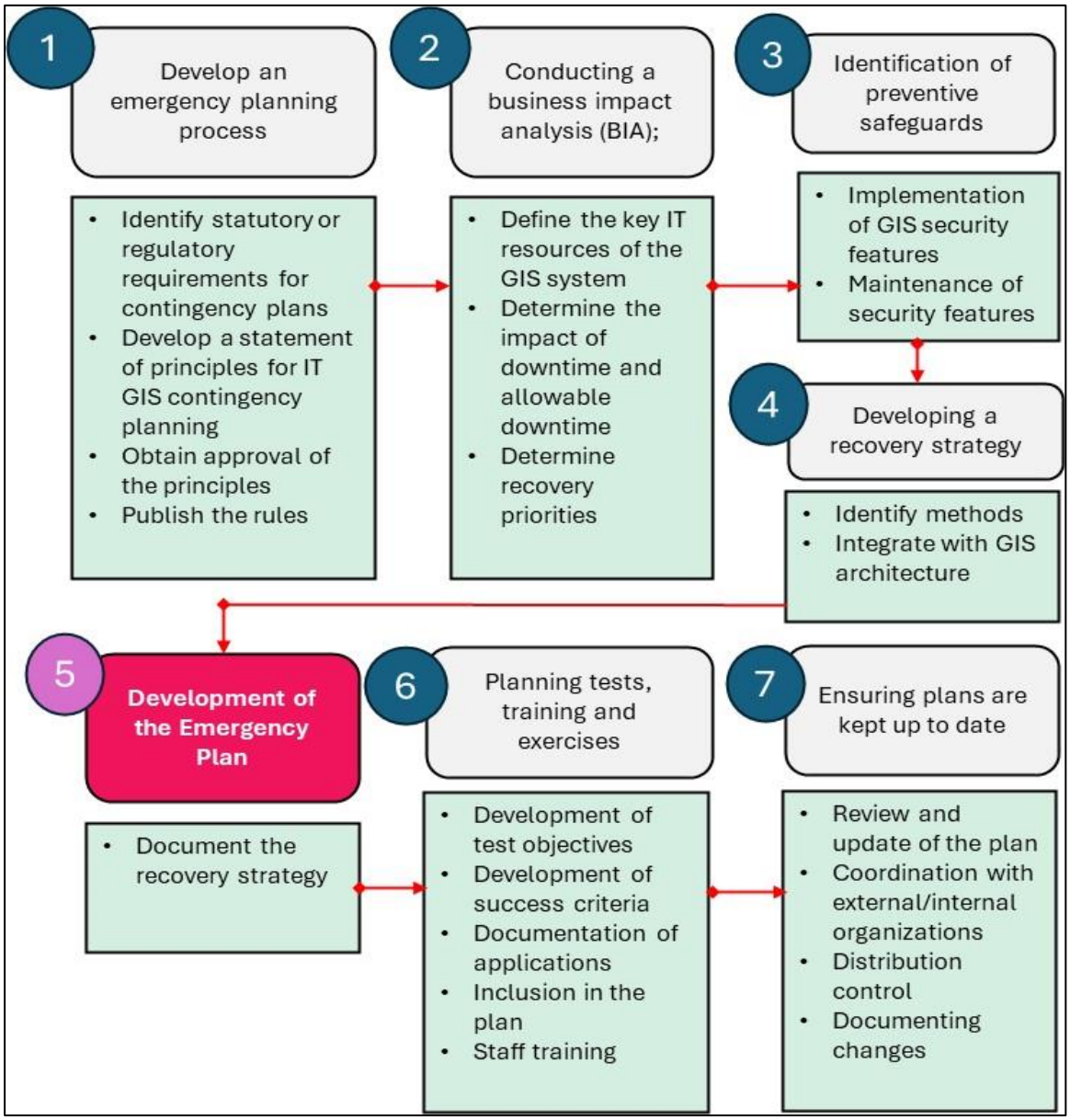

Fig. 2. The Seven Steps of Contingency Planning
Source: Own study

These steps are key components of a comprehensive GIS contingency planning system. A detailed description of these steps is provided in Table 2.

Table 2. Characteristics of contingency planning steps

Name	Characteristics of the activities
Step 1: Develop a contingency planning policy statement	The first step in developing an IT contingency plan is to establish a GIS contingency planning policy. The document should define the overall goals of contingency planning and identify management, roles and responsibilities, resource requirements, testing, training, and exercise schedules.
Step 2: Business Impact Analysis	Business Impact Analysis (BIA) is a crucial step toward understanding the components, interdependencies, and impact of potential downtime in GIS information systems. Conducting a BIA typically requires the following three steps: 1. Determine business processes and the criticality of their recovery. Business processes supported by GIS are identified, and the impact of a system failure on these processes is determined along with the effects of the failure and estimated downtime. Downtime should reflect the maximum time that an organization can tolerate while maintaining the purpose of its operation. 2. Identify resource requirements. Realistic corrective actions require a thorough assessment of the resources required to resume major information processes and related interdependencies as soon as possible. 3. Prioritize the recovery of GIS assets or components.
Step 3: Identify preventive safeguards	In some cases, implementing preventive safeguards can mitigate the effects of downtime outlined in the BIA. Preventive safeguards are measures that detect, prevent, and/or mitigate the impact of a disruption on the GIS system. Preventive measures are specific to the individual components and the environment in which those components operate.
Step 4: Develop a recovery strategy	In the event of a disruption despite the implementation of preventive measures, a recovery strategy is necessary to recover and restore data and system operations within the stipulated RTOs. A recovery strategy is designed as a combination of methods that together address the full spectrum of risk to information systems. During the development phase, several options can be evaluated, and based on the potential impact, the most cost-effective one should be selected and integrated into the information system architecture and operating procedures.
Step 5: Develop a contingency plan in IT	Procedures for implementing a recovery strategy are outlined in an IT contingency plan. The plan must be written in a format that provides users (management and recovery team members) with the context in which the plan should be implemented, as well as direct procedures to be followed by roles.
Step 6: Test the plan, training	The personnel selected to execute the IT contingency plan must be trained in the procedures, the plan must be rehearsed, and the GIS strategy tested. Plan testing exercises should be designed individually and then collectively examine the different components of the overall plan.
Step 7: Maintain the plan	An IT contingency plan must always be kept in a state of readiness for use immediately after notification. The plan must be periodically reviewed to ensure that key personnel, system components and interdependencies, recovery strategies, relevant records, and operational requirements are up to date. The BIA should be reviewed periodically and updated with new information to identify new requirements and contingency priorities. The revised plan or its relevant chapters shall be disseminated to persons whose responsibilities include the implementation of the plan.

Source: Own study

GIS contingency plans

Organizations/GIS requires a set of plans to prepare for the response, continuity, recovery, and resumption of business processes and information systems when a disruption occurs (Dey, 2021). Figure 3 illustrates the relationship between these plans.

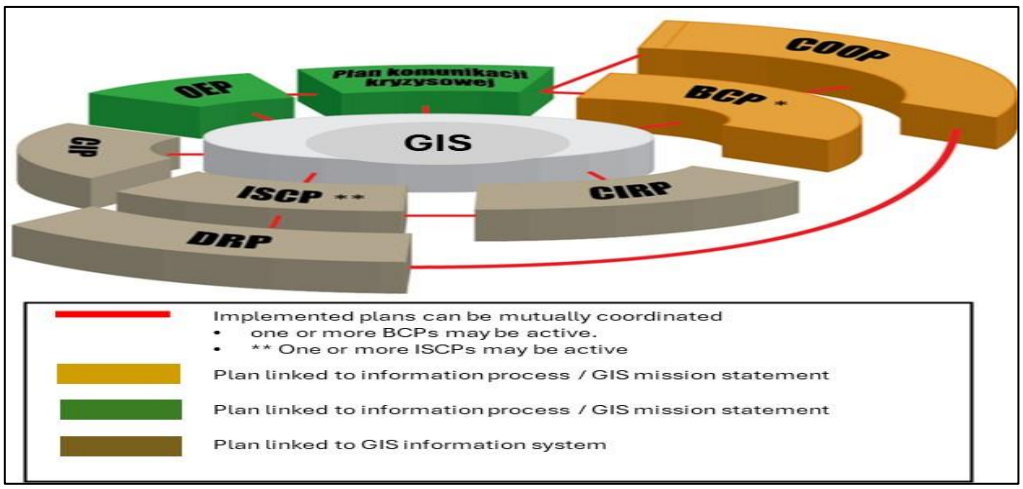

Fig. 3. Illustration the links between the plans
Source: Own study based on: NIST SP 800-34

Each plan has a specific purpose and scope; However, due to the lack of standard definitions for these types of plans, in some cases, the scope of the actual plans developed by organizations may differ from the basic descriptions. A brief description and the relationship between these plans can be found in Table 3.

Table 3. Characteristics and relationships between the different plans

Plan Name	Summary	Relationship between plans
Continuity of Operations Plan – COOP	It is required to maintain the organization's Mission Essential Functions (MEF) in an alternate location and to perform these functions for 30 days before returning to normal operation.	An MEF-focused plan can also activate BCP for specific business processes, ISCP or DRP, as the case may be.
Business Continuity Plan – BCP	It refers to sustaining business processes and the information systems that support those business processes during and after significant disruptions.	A business process-oriented plan that can be activated in conjunction with the COOP plan to maintain non-MEF functionality.
Critical Infrastructure Protection Plan – CIP	This plan is a set of policies and procedures that are used to protect and recover those elements of the system infrastructure that are considered so critical that their loss would have a debilitating impact on security.	A risk management plan that is included in COOPs in organizations with critical infrastructure and critical assets.
Crisis Comm. Plan – CCP	This plan is a set of procedures for the dissemination of internal and external communications	An incident-activated plan, often with a COOP or BCP, can be used on its own during an incident.
Disaster Recovery Plan – DRP	It refers to an information system-centered plan designed to restore the operation of one or more information systems in an alternative location after a major disruption.	An information system-oriented plan that activates one or more ISCPs to recover individual systems.
Information System Contingency Plan – ISCP	Provides recovery and resumption procedures for a single IT system resulting from disruptions that do not necessarily require a move to another location.	An information system-oriented plan that can be activated independently of other plans or as part of a larger corrective effort coordinated with the DRP, COOP, or BCP.
Cyber Incident Response Plan – CIRP	Establishes procedures to enable cybersecurity personnel to identify, mitigate, and recover from cyberattacks on GIS information systems.	An IT-oriented plan can activate ISCP or DRP, depending on the range of the attack.
Occupant Emergency Plan – OEP	Guides those on-site in the event of an emergency threatening the health and life of staff or environmental damage or property damage.	An incident plan that is initiated immediately after the incident precedes the activation of the COOP or DRP.

Source: Own study based on: NIST SP 800-34

Careful coordination between planmakers must be maintained so that their policies and procedures complement each other or do not contradict each other. Any changes to a single plan must be communicated to planners of related GIS systems and functions.

Contingency Plan Structure

GIS IT contingency plans are constructed, in addition to supporting information (introduction, concept) and appendices, from three basic phases, described in Table 4: Activation Phase, Recovery Phase, Playback Phase (NSC 800-18; NSC 800-17).

Table 4. Characteristics of the components of the contingency plan

Phase	Description
Activation Phase	Activation and Notification Phase – ISCP activation occurs after a disruption or failure that may cause system downtime beyond the RTOs set for that system. A failure can cause serious damage to the facility that houses the system, serious damage or loss of equipment, or other damage that typically results in long-term loss of information processing capacity. Once ISCP is activated, system owners and users are notified of a possible long-term shutdown and a thorough assessment of the system failure is performed. The information from the failure assessment is presented to the system owners and can be used to modify recovery procedures specific to the cause of the failure.
Recovery phase	Recovery Phase – The recovery phase provides detailed information about the actions and procedures for recovering the affected system. The actions and procedures are written at a level that allows a suitably qualified technician to recover the system without having strict knowledge of that system. This phase includes procedures for notification and escalation of actions to communicate the restoration status to system owners and users.
Playback phase	Recovery Phase – The Restore Phase defines the actions taken to test and validate the capabilities and functionality of the system at the original or new location. This phase consists of two main actions: validating the restoration and deactivating the plan: - During validation, the system is tested and verified that it has achieved the ability to operate as normal. Validation procedures may include functional or regression testing, concurrent processing, and/or validation of data. The system is considered by the owner to be reconstituted and able to operate normally after the successful completion of the validation tests. - Deactivation includes actions to notify users of the operational status of the system. This phase also includes documenting recovery efforts, finalizing the activity log, incorporating lessons learned into plan updates, and preparing resources for possible future events.

Source: Own study based on: NIST SP 800-18

Procedures are documented in the notification/commissioning, recovery, and restoration phases. Supporting information and annexes provide the supplementary information necessary to understand the context in which the plan is to be implemented and additional information that may be necessary to carry out the procedures (e.g. emergency contact details and BIA).

Contingency planning team structure and roles and responsibilities

Organization Chart

The structure of the planning team plays a key role in both the process of building the team diagram and the process of creating an effective contingency plan [ISCP]. A diagram of the organizational structure of the contingency planning team is shown in Figure 4.

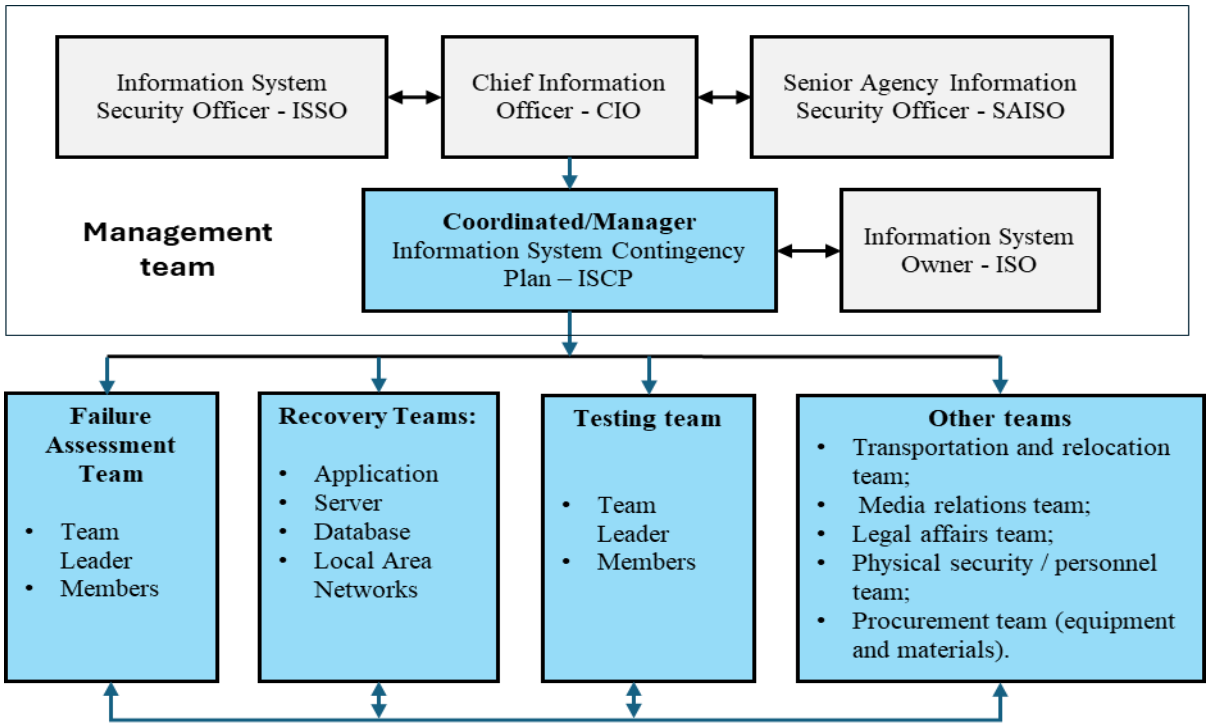

Fig. 4. Contingency planning team organizational chart
Source: Own study

The size of each team, team names, and hierarchy projects depend on the GIS class. In addition to a single authoritative role in overall decision-making responsibility, including plan activation, an effective strategy will require some or all of the following groups: A management team (including ISCP coordinator); Failure Assessment Team; Recovery teams; Telecommunication team; Test Team and Legal, Procurement Team, etc. A function/role, such as a CIO, provides the highest authority in activating the plan and making decisions about spending levels, acceptable risk, and inter-organizational coordination. A senior manager usually leads a management team. The management team facilitates communication between other teams, and supervises the testing and practice of the IT system contingency plan. Leadership roles should include the ISCP Manager, who has overall responsibility for managing the plan, and the ISCP Coordinator, who is responsible for overseeing recovery and recovery progress, initiating any necessary escalations or communication to inform the progress of work in ISCP, and establishing coordination with other recovery and recovery teams. Each team is managed by a team leader who directs the overall activities of the team, acts as a representative of the team at the management level, and collaborates with other team leaders. The team leader

disseminates the word to team members and approves any decisions that need to be made within the team. The team leader should have a designated deputy to act as a manager if the lead leader is unavailable. For most systems, a management team is necessary to provide general guidance in the event of a major system failure. The required team types depend on the affected GIS and can be adjusted according to the impact levels (NSC 199; NSC 800-60) to reflect specific differences in requirements and procedures for creating effective security, including backups. Each team should be trained and ready to respond in the event of a disruption that requires plan activation.

Roles and responsibilities

Responsibility for the planning process generally rests with the IT contingency plan coordinator or ISCP coordinator, who is typically the functional or GIS resource manager. The ISCP coordinator develops the strategy in collaboration with other functional managers and managers of system-related resources or the business processes supported by the system. The ISCP coordinator usually also manages the development and implementation of the contingency plan. All IT systems of public entities must have a contingency plan. Figure 5 illustrates the contingency planning process. Part or all of the management team may lead specialized recovery teams. The ISCP Manager/Coordinator establishes several roles related to the support of GIS recovery and restoration. Individuals or teams assigned to ISCP roles should be trained to respond to an emergency event affecting GIS. Recovery personnel should be assigned to one of several specific teams that will respond to the incident, recover capabilities, and return the system to normal operation. To do this, recovery team members need to clearly understand the purpose of the recovery effort, the individual procedures the team will follow, and how the interdependencies between recovery teams might affect overall strategies. Depending on the GIS class, you should consider responsibilities for each team/role and coordination with other recovery and recovery teams. At a minimum, establish the role of System Owner or Business Unit Contact, Recovery Coordinator, and Technical Recovery Contact Point. You should select the staff to support these teams based on their skills and knowledge. Teams should consist of personnel responsible for the same or similar functions under normal circumstances. For example, the members of the server recovery team should be the administrators of that server. Team members need to understand not only the purpose of the contingency plan, but also the procedures necessary to execute the recovery strategy. Teams should be sized enough to remain profitable. If some members are unable to participate in a team, alternate team members should be appointed. Team members should be familiar with the goals and procedures of other teams to facilitate cross-team coordination. Table 5 lists the specifications of roles and responsibilities for selected team members.

Table 5. Role and Responsibility Specifications

Role	Responsibility
Chief Information Officer – CIO	A CIO (Chief Information Officer) is a key person in an organization who is responsible for developing and maintaining an organization-wide information security program. Assigned responsibilities for system security planning: - appointing a SAISO (Senior Agency Information Security Officer) to carry out the CIO's tasks in the field of system security planning; - developing and maintaining information security policies, procedures, and security techniques to incorporate system security planning; - manage security identification, implementation, and assessment; - ensure that the personnel responsible for the system's security plans are trained; - assisting the managers of organizational units in the organization in fulfilling their system security plans; - identify and develop security in your organization. If the organization has not designated a formal CIO position, it is required that the related duties be performed by someone of comparable rank within the organization.
Information System Owner – ISO	An Information System Owner is a person in an organization who is responsible for the procurement, development, integration, modification, or operation and maintenance of an information system. The owner of the information system has the following responsibilities related to system security plans: - developing a system security plan in coordination with information owners, system administrator, ISSO (Information System Security Officer), SAISO, and end users maintaining the system security plan, and ensuring that the system is implemented and operated by agreed security requirements; - ensure that system users and support personnel are adequately trained in security (e.g., by the Rules of Conduct Manual) and assist in identifying, implementing, and evaluating security measures. The role of the information system owner can be interpreted in many ways, depending on the specific organization and the phase of the SDLC in which the information system is located. Some organizations may refer to the owners of the information system as program managers or business/asset/mission owners.
Senior Agency Information Security Officer – SAISO	A SAISO is a person in an organization who acts as the CIO's primary liaison to the owners of the information system and ISSO in the organization. SAISO has the following responsibilities related to system security plans: - carrying out the CIO's tasks in the field of system security planning, coordinating the development, review and approval of system security plans with the owners of information systems, ISSO and the authorizer, - coordinating the identification, implementation and assessment of common safeguards; - Possess the professional qualifications, including training and experience, required to develop and review system security plans.
Information System Security Officer – ISSO	An ISSO is a person in an organization to whom the SAISO, the authorizer, the manager, or the owner of the information system has been assigned the responsibility of ensuring that an appropriate level of operational security is maintained for the information system. ISSO has the following responsibilities related to system security plans: - assistance of SAISO in identifying, implementing and assessing safeguards, - playing an active role in the development and maintenance of the system security plan, as well as coordinating with the information system owner any changes to the system and assessing the security impact of these changes.
Manager Information System Contingency Plan – ISCP	The responsibility of the IT contingency plan manager is crucial to ensure business continuity and security of information systems. Its tasks include, among others: - Develop and update a contingency plan and incident response procedures. - Ensuring that all components of the system are regularly tested and that emergency tests are carried out to verify the effectiveness of the plan. - Training staff in emergency procedures and preventive actions. - Monitor systems to quickly detect potential threats and respond to incidents. - Collaborate with other departments of the organization to ensure data integrity and security.
Failure Assessment Team	The IT Failure Assessment Team plays a key role in identifying, analyzing, and managing incidents related to information systems. Their tasks include: - Analyze the causes of the failure to understand what went wrong and what factors contributed to the incident. - Assess the impact of an outage on your organization's operations, including operations, finances, and reputation. - Recommending corrective and preventive actions to avoid the recurrence of similar problems in the future. - Collaborate with IT departments to develop business continuity and disaster recovery plans. - Communicate with stakeholders, including management, employees, and customers, to ensure transparency and understanding of the situation. This team must also be prepared to react quickly in the event of a failure to minimize its negative effects. This requires not only the right tools and procedures but also communication and management skills to effectively manage actions in crises.

Source: Own study based on: NSC 800-34; NSC 800-61

Conclusion

All GIS class systems should have IT contingency plans for their certified and accredited information systems and are required to have an organizational follow-up plan for their key functions (Cybersecurity Framework, 2018; NSC 199; NSC 800-18). In general, universal, universally accepted definitions of contingency planning for the information system and related planning areas are not available. This sometimes leads to confusion about the actual scope and purpose of different types of plans. To provide a common basis for understanding IT contingency planning, this article lists several other types of plans and describes their purpose and scope as they relate to GIS contingency planning. Because there are no standard definitions for these types of plans, the scope of actual GIS plans can vary.

GIS systems must be characterized by the ability to develop resilience to various types of threats and achieve the ability to maintain their functionality and usefulness despite changes in the environment. These changes can be gradual, such as economic or technological conditions, or changes in the purpose of the organization, or sudden, such as disasters. Instead of merely identifying and mitigating the impact of threats, vulnerabilities, and risks, a GIS system should have a defined cyber resilience strategy and built infrastructure resilience that minimizes the impact of disruptions on the core functions of its purpose. Resilience is the ability to quickly adapt and regain the ability to function after known or unknown changes in the environment. Resilience is not a process, but rather an end state.

The goal of GIS resiliency is to be able to continue essential functions in the event of any disruption. Resilient GISs must constantly adapt to changes and related risks that may affect their ability to continue with key functions. Risk Management, contingency planning, and continuity planning are essential security and crisis management activities that should be implemented holistically across GIS as part of a cyber resilience program. Effective contingency planning begins with developing a GIS contingency planning policy and subjecting each IT system to a Business Impact Analysis (BIA). This makes it easier to prioritize systems and processes and develop a recovery priority strategy to minimize waste. It is essential to determine the impact of an information system disruption on an organization's operations and assets, individuals, other organizations, and society through a formula that analyzes three security attributes: confidentiality, integrity, and availability. For each safety attribute, the impact of the interference is determined as high, moderate, or low. The highest level of impact on individual security attributes is used to determine the overall level of impact on the security of the GIS information system.

Contingency planning considerations and strategies concern the level of impact on the security attribute related to the availability of information systems. Strategies for high-performance IT systems should include high availability and redundancy options. Options can include fully redundant systems with load balancing in alternate locations, data mirroring, and offsite database replication. High availability options are typically expensive to set up, operate, and maintain and should only be considered for high-impact IT systems classified as the high availability security attribute. Less impactful information

systems can benefit from less expensive emergency options and tolerate longer downtime for data recovery or restoration.

References

Ahmad A., Bosua R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective. Computers & Security, vol. 42, pp. 27–39.

Bhattacharya J. (2015). Quality Risk Management – Understanding and controlling the risk in the pharmaceutical manufacturing industry. International Journal of Pharmaceutical Science Invention, vol. 4, no. 1, pp. 29–4.

Coresite C. (2016). Hybrid cloud and business continuity planning. https://www.coresite.com/blog/cloud-business-continuity-planning [access: 07.05.2024].

Cybersecurity Framework v 1.1 – CSF Tools, 2018.

Czym są dobre praktyki? (*What are good practices?*) https://metoda.spoledkurs.pl/dobre-praktyki/wprowadzenie/ [access: 07.05.2024].

Dey M. (2021). Business Continuity Planning (BCP) Methodology-Essential For Every Business. IEEE GCC Conference and Exhibition, pp. 19–22.

Dobre praktyki (*Good practices*). https://mfiles.pl/pl/index.php/Dobre_praktyki [access: 07.05.2024].

Eskola J., Suoranta J. (1998). Johdatus laadulliseen tutkimukseen (*An introduction to qualitative research*). Vastapaino.

Kovalainen A., Eriksson P. (2008). Qualitative Methods in Business Research: Narrative Research, in series: Introducing Qualitative Methods. SAGE Publications Ltd. doi: 10.4135/9780857028044.

NIST SP 800-34, Revision 1 – Contingency Planning Guide for Federal Information Systems, Marianne Swanson.

NSC 199, Security Categorization Standards – Based on FIPS 199.

NSC 800-18, Guide for the Development of Information Systems Security Plans in Public Entities – Based on NIST SP 800-18.

NSC 800-34, Contingency Planning Guide – Based on NIST SP 800-34.

NSC 800-37, Framework for Risk Management in Organizations and Information Systems. Security and privacy in the system lifecycle – based on NIST SP 800-37.

NSC 800-61, Computer Security Incident Handling Guide – Based on NIST SP 800-61.

Patton M.Q. (2002). Qualitative research and evaluation methods, Sage Publications, 2002.