Student:	Email:
Bradley Adams	badams10@my.athens.edu

Time on Task:	Progress:
	100%

Report Generated: Monday, April 7, 2025 at 11:26 AM

Guided Exercises

Part 1: Research BIA and BCP

3. **Write** a **brief summary** of the information you found in the articles and websites. In your summary, **describe** what a BCP is and list the steps for developing a BCP. Also, **describe** what a BIA is, how you conduct a BIA, and how the BIA is related to the BCP.

Business Continuity Planning (**BCP**) and Business Impact Analysis (**BIA**) create organizational resilience in the face of minor or catastrophic disruptions. A comprehensive BCP ensures that an organization can continue critical operations during and after an incident, minimizing financial loss and reputational damage. A BIA outlines procedures and instructions an organization must follow during a disruption, such as a natural disaster, cyberattack, or equipment failure. It defines roles, responsibilities, continuity strategies, communication protocols, backup procedures, recovery timelines, and recovery prioritization.

The goal of the BCP is to restore mission-critical operations within a defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO), ensuring minimal interruption to services.

Here are the steps to develop a BCP

*Conduct a BIA: Identify critical business functions and evaluate the effects of disruption.
*Perform Risk Assessment: Identify threats and vulnerabilities impacting operations.
*Determine Recovery Strategies: Define how to maintain and recover critical operations.
*Develop the Plan Framework: Document recovery procedures, contact lists, communication strategies, and vendor dependencies.
*Train and Test: Educate staff on their roles and conduct exercises to validate the plan's effectiveness.
*Maintain and Update: Regularly review and update the BCP to reflect business operations or risk changes.

A BIA is a systematic process that evaluates how disruptions to business functions affect operations. It identifies the critical business functions and dependencies, financial and operational impact of downtime, acceptable downtime durations (RTO/RPO), and prioritization of systems and resources for recovery.

Conducting a BIA

*Identify Business Processes: List all functions and supporting assets (systems, people, vendors).
*Gather Data: Use interviews, surveys, and documentation to assess dependencies and impacts.
*Assess Impact Severity: Determine the effect of function disruption on revenue, legal compliance, safety, and reputation.
*Define RTOs and RPOs: Establish time-based recovery and data restoration goals.
*Analyze and Prioritize: Rank functions by criticality to guide recovery planning.

How the BIA is related to the BCP

The BIA is the foundation of the BCP. It provides the necessary data to determine which business functions are critical and how quickly those functions must be restored. The BIA informs the BCP's prioritization and resource allocation strategies, guaranteeing that continuity planning is practical and aligned with business needs. The BIA identifies what needs to be protected and recovered, while the BCP defines how and when that protection and recovery occur. Together, they enable organizations to operate through crises with resilience and foresight.

Part 2: Create a BCP Policy

2. For each business function or process described above, **assign** a business impact factor of **Critical, Major, Minor,** or **None**.

*__Critical__ is fundamental to revenue generation, customer engagement, or operational continuity. Downtime would result in immediate and severe business impact.
*__Major__ are essential functions but can sustain short-term disruption without immediate catastrophic consequences.
*__Minor__ is valuable but non-essential for short-term business continuity.

Internal and external voice coms with customers in real-time = ***Critical***
Internal and external e-mail coms with customers via store and forward messaging = ***Major***
DNS server for internal and external IP coms = ***Critical***
Internet connectivity for e-mail and store-and-forward customer service = ***Critical***
Self-service web site for customer access to info and personal account info = ***Major***
e-Commerce site for online customer purchases or scheduling 24x7x365 = ***Critical***
Payroll and human resources for employees = ***Major***
Real-time customer service via web site, e-mail, or telephone (requires CRM) = ***Critical***
Network management and technical support = ***Critical***
Marketing and events = ***Minor***
Sales orders or customer/student registration = ***Critical***
Remote branch office sales order entry to headquarters = ***Major***
Voice and e-mail communications to remote branches = ***Major***
Accounting and finance support: Accounts payable, Accounts receivable, etc. = ***Critical***

*__None__ is NOT used due to all the listed functions influencing continuity to some extent. Based on introduction explaining, "busted microwave in the office kitchen."

3. For each business function or process described above, **identify** the IT systems and applications impacted by the business function (for example, determine what would be affected if the function or process failed).

Internal and external voice coms with customers in real-time = **VoIP systems, Unified Communication servers, Internet/WAN connectivity**

Internal and external e-mail coms with customers via store-and-forward messaging = **Email servers, gateways, spam filters**

DNS server for internal and external IP coms = **Internal and External DNS services, Active Directory**

Internet connectivity for e-mail and store-and-forward customer service = **Routers, firewalls, load balancers, ISPs leased lines, VPNs, Proxy servers, and DNS services**

Self-service web site for customer access to info and personal account info = **Web, application, and database servers**

e-Commerce site for online customer purchases or scheduling 24x7x365 = **Web and app servers, Payment services, Ordering systems, and Inventory databases**

Payroll and human resources for employees = **HR management system, Payroll system, and Active Directory**

Real-time customer service via website, email, or telephone (requires CRM) = **CRM software , Telephony connections, web and email servers**

Network management and technical support = **Network monitoring tools, Remote management tools, ticketing systems**

Marketing and events = **Email marketing software, Event platforms such as Zoom, and Social media**

Sales orders or customer/student registration = **CRM and E-commerce systems, Registration databases**

Remote branch office sales order entry to headquarters = **VPN networks, WAN routers/firewalls, and Authentication services**

Voice and e-mail communications to remote branches = **Unified Communications and mail servers, VPN connections, and DNS systems**

Accounting and finance support: AP/AR, etc. = **Financial software such as QuickBooks, Database**

systems, and backups

6. For each Business Function or Process, use the table above to **assign** an RTO/RPO according to the corresponding business impact factor.

Internal and external voice coms with customers in real-time = Critical = **RTO of 8 hours and RPO of 0 hours**

Internal and external e-mail coms with customers via store-and-forward messaging = Major = **RTO of 24 hours and RPO of 8 hours**

DNS server for internal and external IP coms = Critical = **RTO of 8 hours and RPO of 0 hours**

Internet connectivity for e-mail and store-and-forward customer service = Critical = **RTO of 8 hours and RPO of 0 hours**

Self-service web site for customer access to info and personal account info = Major = **RTO of 24 hours and RPO of 8 hours**

e-Commerce site for online customer purchases or scheduling 24x7x365 = Critical = **RTO of 8 hours and RPO of 0 hours**

Payroll and human resources for employees = Major = **RTO of 24 hours and RPO of 8 hours**

Real-time customer service via website, email, or telephone (requires CRM) = Critical = **RTO of 8 hours and RPO of 0 hours**

Network management and technical support = Critical = **RTO of 8 hours and RPO of 0 hours**

Marketing and events = Minor = **RTO of 1 week and RPO of 3 days**

Sales orders or customer/student registration = Critical = **RTO of 8 hours and RPO of 0 hours**

Remote branch office sales order entry to headquarters = Major = **RTO of 24 hours and RPO of 8 hours**

Voice and e-mail communications to remote branches = Major = **RTO of 24 hours and RPO of 8 hours**

Accounting and finance support: AP/AR, etc. = Critical = **RTO of 8 hours and RPO of 0 hours**

Policy Statement
Insert policy verbiage here.

Policy Statement

Bankwise Credit Union is committed to maintaining uninterrupted access to essential financial services, even during disruptive incidents. Bankwise establishes this Business Continuity Plan (BCP) Policy to provide resilience, rapid recovery, and sustained operations during any event that compromises normal business functions. This policy provides a formal structure for developing, implementing, testing, and maintaining business continuity and disaster recovery capabilities across all critical business units and the IT infrastructure. This policy includes safeguarding the confidentiality, integrity, and availability of systems and data vital to Bankwise.

This BCP Policy is established from strict Business Impact Analysis (BIA) assessments that have identified mission-critical functions, associated IT dependencies, and their required recovery timeframes. These assessments have identified our Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), which define acceptable limits for downtime and data loss in the event of a disruption.

Bankwise Credit Union recognizes that effective business continuity management is not a one-time activity but an ongoing process. This policy mandates regular reviews, risk assessments, training, and testing to guarantee continuity strategies align with evolving business needs, technological advancements, and regulatory requirements.

This policy must be familiar with and adhered to by all departments, employees, and contractors to ensure a coordinated and effective response to disruptions.

Purpose/Objectives

Define the policy's purpose and objectives. They should mirror the purpose/objectives of a business impact analysis (BIA).

Purpose and Objectives

Purpose

This business Continuity Plan (BCP) Policy establishes a structured, proactive approach to guaranteeing that Bankwise Credit Union can continue delivering essential banking services during and after a disruption. This policy provides a framework for identifying mission-critical business functions, evaluating the potential impact of service interruptions, and aligning IT systems and resources to meet defined recovery objectives. This policy is the foundation for building resilience in business operations, guiding the recovery of systems, data, and business processes within the identified timeframes that will mitigate identified financial, operational, reputational, and regulatory risks.

Objectives

Identify and prioritize mission-critical business functions across Bankwise Credit Union and assess their dependencies on IT systems, data, personnel, vendors, and infrastructure.

Evaluate business disruptions' operational and financial impacts, ranging from minor interruptions to catastrophic events, including natural disasters, cyberattacks, and systemic failures.

Establish Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for each critical function, defining acceptable limits for downtime and data loss.

Determine appropriate recovery methods and failover mechanisms to align continuity strategies with our risk tolerance and regulatory requirements.

Provide input to developing comprehensive recovery procedures, guaranteeing a timely and coordinated response that protects customer trust, business stability, and regulatory compliance.

Support an ongoing business continuity through regular testing, updates, and revalidation of recovery objectives in response to organizational and/ or technological changes.

Scope

Define this policy's scope and whom it covers.

Scope

This policy applies to all departments, business units, employees, contractors, and third-party service providers of Bankwise Credit Union who support or operate business functions, IT systems, applications, communications, and infrastructure critical to business continuity.

The scope of this Business Continuity Plan (BCP) Policy includes:

All mission-critical business processes identified through the current and approved Business Impact Analysis (BIA). These processes include customer service, transaction processing, lending, e-commerce, accounting, and regulatory reporting.

All IT systems and applications that support or enable critical operations, including internal servers, cloud-hosted environments, networking infrastructure, data centers, and endpoint devices.

All personnel whose roles contribute to the delivering, supporting, or recovering of business functions. These roles include executive leadership, department recovery team leads, IT staff, and vendor liaisons.

All physical and virtual assets. These assets include facilities, communication systems, and third-party services.

All the locations for Bankwise Credit Union's operations. These locations include headquarters, branch offices, call centers, and remote work environments.

Standards

Does this policy point to any hardware, software, or configuration standards? In this case, you need to reference the recovery time objectives (RTOs) and recovery point objectives (RPOs) as standards and metrics. List them here and explain the relationship of this policy to these standards.

Standards

This policy adopts and enforces standardized Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) as key performance metrics for determining acceptable downtime and data loss levels for each business function and associated IT system. These standards guide the development and validation of recovery strategies, define recovery priorities, and serve as benchmarks during disaster recovery operations and continuity testing.

Recovery Standards

Bankwise Credit Union categorizes its business functions by Business Impact Factor, each with

corresponding RTO and RPO requirements established through a Business Impact Analysis (BIA).

Standards Defined

Impact Factor = RTO & RPO

Critical = 8 hours & 0 hours*****
Major = 24 hours & 8 hours
Minor = 1 week & 3 days
None = 1 month & 7 days
*******0 hours translates to real-time or near-real-time*

Standards Relationship to Business Continuity Plan Policy

-All BCP activities must align with the identified RTO and RPO standards. These activities include but are not limited to, system architecture design, data continuity strategies, vendor service level agreements, and BCP continuity procedures.

-Any business function that exceeds its assigned RTO or RPO during an incident or test shall be considered non-compliant and will undergo corrective action planning.

-The IT and Cyber Incident Response team will test all continuity and disaster recovery plans against these standards to validate their effectiveness and identify technical or procedural gaps.

-These standards set the minimum requirements for Bankwise Credit Union's resilience, impacting how we manage our backup, disaster recovery, infrastructure, and data retention procedures.

-Whenever business operations or IT systems experience changes that could affect RTO or RPO, a formal BIA must be conducted to reassess these requirements.

These standards form the technical foundation of the Bankwise Credit Union Business Continuity Program and guarantee that recovery efforts are prioritized, measurable, and aligned with industry best practices and compliance regulations.

Procedures

Explain how you intend to implement this policy across the entire organization.

Procedures

The successful implementation of the Bankwise Credit Union Business Continuity Plan (BCP) Policy requires a structured, organization-wide approach that integrates business operations, IT, and risk management practices. By making these procedures standard practice, Bankwise Credit Union guarantees that business continuity is a core part of its daily operations. These procedures outline how Bankwise Credit Union will implement the BCP policy across the entire organization. They will be implemented as part of a Phased, Iterative Implementation Model.

Business Impact Analysis (BIA) Undertaking

-Each department must perform a Business Impact Analysis annually to identify mission-critical functions, dependencies, and potential downtime impacts.
-The BIA will document each business function's Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
-The BCP Coordinator and IT Security Team will review the BIA quarterly.

Continuity Plan Development

-Based on BIA results, department leaders will work with IT and compliance personnel to develop tailored continuity and recovery plans for their functions.
-Plans must include detailed recovery workflows, escalation procedures, alternate work locations, resource requirements, and contact lists.

Infrastructure and Technology Alignment

-IT will map recovery priorities (RTOs/RPOs) to system architecture to ensure proper redundancy, failover mechanisms, data replication, and backup policies are in place.
-The BCP Coordinator shall evaluate systems supporting critical and major functions quarterly to meet performance thresholds.

Employee Awareness and Training

-All employees will receive annual BCP training. This training includes each employee's role during an incident, how to access recovery documentation, and participation in drills.
-The IT security team will deliver specific training to key personnel involved in continuity plan activation, IT recovery procedures, and communications policies.

Testing and Exercises

-Full-scale BCP tests and tabletop exercises will be conducted semi-annually, with scenarios covering different disruptions.
-The BCP Coordinator will review vendor BCP documentation and service level agreements during onboarding and reassess annually.

Plan Maintenance and Review

All continuity and recovery plans will undergo a formal annual review or immediate revision if significant changes in business processes or technology occur, any post-incident after-action review recommendations are made, and /or any new regulatory or industry requirements are identified.

Guidelines

Explain any roadblocks or implementation issues that you must address in this section and how you will overcome them per defined policy guidelines.

Guidelines

Implementing a comprehensive Business Continuity Plan (BCP) across a financial institution like Bankwise Credit Union involves several challenges that can interfere with timely and effective execution. These guidelines identify common roadblocks and specify policy-based solutions.

Incomplete or Outdated BIA Information

Challenge: Departments may delay or neglect BIA updates, resulting in inaccurate prioritization of systems and recovery requirements.
Policy Guideline: BIAs are mandatory annually or following any impactful change in business operations, staffing, or IT systems. The BCP Coordinator shall track compliance and escalate any concerns to executive leadership if they are overdue.

Lack of Employee Awareness

Challenge: Staff unawareness of continuity procedures may result in confusion or noncompliance during a disruption.
Policy Guideline: All employees must complete mandatory annual training. Attendance and test performance are logged in HR systems and mapped to compliance audits.

Insufficient IT Infrastructure for Meeting RTO/RPO

Challenge: Legacy systems or underfunded infrastructure may not meet recovery standards, particularly for "Critical" or "Major" business functions.
Policy Guideline: IT is required to conduct quarterly recovery assessments against documented RTO/RPO. Any non-compliant systems must be reported and remediated within a defined action plan reviewed by the BCP Coordinator.

Unverified Third-Party Vendors

Challenge: External vendors may lack sufficient continuity plans or fail to meet Bankwise's internal RTO/RPO requirements.
Policy Guideline: All third-party service providers supporting critical operations must submit annual BCP compliance documentation and agree to service-level agreements corresponding to Bankwise's continuity standards. Non-compliant vendors will trigger risk mitigation.

Failure to Test and Validate Plans

Challenge: Continuity and recovery plans that are not tested risk failing when needed.
Policy Guideline: The organization shall conduct semi-annual continuity testing, including tabletop simulations and live system recovery drills. The BCP Coordinator will document the results and, if necessary, initiate update procedures to any findings within 30 days.

Challenge Exercise

Use the internet to find further information on the differences between policies and plans in information security in general. Use this information to create a high-level explanation for C-level executives. Provide examples of real business continuity policies and how they could be useful in your organization.

Understanding the Difference Between Business Continuity Policies and Plans at Bankwise Credit Union

As C-level executives, it's essential to understand the distinction between policies and plans, especially in the context of business continuity, where misalignment or confusion can hinder our ability to respond to and recover from serious disruptions.

What Is a Business Continuity Policy?
A Business Continuity Policy is a high-level governing document that sets the intent, principles, and expectations for how the organization prepares for, responds to, and recovers from disruptions. Think of it as the "what," "why," and "who."
-What we must do to remain operational during outages
-Why it is essential. So we can serve customers, maintain trust, and comply with regulations.
-Who is responsible for overseeing and implementing it?

It outlines organizational standards such as Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) and assigns accountability across business units. A policy does not include specific recovery instructions but instead sets the stage for how continuity planning will be executed and measured.
Example Policy Use Case at Bankwise:
Our BCP policy may state: "All critical systems must be restored within 8 hours (RTO) with zero data loss (RPO)." This provides the benchmark against which recovery strategies are developed and tested.

What Is a Business Continuity Plan?
A Business Continuity Plan is the "how". It provides the tactical, step-by-step procedures required to achieve the goals outlined in the policy. These steps include:
-Communication plans
-Recovery steps for IT systems and services
-Staff roles and responsibilities during a disaster
-Procedures for alternate site operations

Each department or function will have its own BCP tailored to its specific systems and risks, aligned to the global BCP policy.
Example Plan Use Case at Bankwise:
The IT Department's BCP may include: "In the event of a ransomware attack, restore core banking servers from the immutable backup repository stored at Site B, test system integrity, and re-enable online member access within the 8-hour RTO window."

Why This Distinction Matters

As noted by Integris and ITLawCo, failing to distinguish between a policy and a plan can result in policy non-compliance, operational delays, and legal exposure. Policies provide governance; plans offer execution. Both must work together for resilience.

A mature business continuity capability means that the policy sets clear expectations that are aligned to business risk, and the plan guarantees those expectations are met through real-world actions. By keeping policies strategic and plans tactical, Bankwise Credit Union guarantees we can respond to disruption quickly, clearly, and confidently while protecting our customers, data, and brand.

References:

https://integrisit.com/what-is-a-cybersecurity-plan-policy-procedure/
https://itlawco.com/difference-between-policies-plans-procedures-processes-programmes-practices/