Business Continuity Plan (BCP) tailored to a typical Electronics Security Services Company.

This plan includes recovery metrics and test steps to ensure resilience in the face of disruptions Using

NIST SP 800-34 Rev. 1 framework:

Version: 1.0

By

Engr. Jerry Ebruvwiyor Osiobe, MNSE, MNIMMME.

MSc. Systems Engineering.

B.Eng. Metallurgical and Materials Engineering.

National Diploma (ND) Ceramics and Glass Technology.

Date: [12/09/2025]

Abstract

This Business Continuity Plan (BCP), tailored for an Electronic Security Services Company and aligned with the NIST SP 800-34 Rev. 1 framework, establishes a structured approach to ensure resilience against disruptions such as cyberattacks, natural disasters, pandemics, and system failures. The plan integrates risk assessment, business impact analysis (BIA), disaster recovery planning (DRP), and contingency strategies to safeguard critical assets, personnel, and operations. Recovery metrics—including Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)—are defined for essential systems such as CAD/CAE, ERP, communication platforms, HRMS, and file servers. Preventive controls (e.g., encrypted backups, redundant power, cybersecurity training) and contingency measures (e.g., cloud-based recovery, alternate office sites, manual workarounds) are outlined to minimize downtime and financial loss. Activation criteria, notification procedures, recovery steps, and reconstitution processes ensure structured response and restoration. Regular testing, training, and maintenance cycles validate plan effectiveness and adaptability. Overall, the BCP provides a comprehensive roadmap for maintaining operational continuity, protecting stakeholders, and ensuring rapid recovery of IT and business functions in the face of disruptions.

1.0 Introduction.

A Business Continuity Plan (BCP) is a strategic document outlining how an organization will maintain essential functions during and after unexpected disruptions (like cyberattacks, disasters, or pandemics) by protecting staff, assets, and data, minimizing downtime, and ensuring quick recovery to normal operations, acting as a roadmap for resilience and swift response.

1.1 Key Components & Purpose

- Risk Identification: Identifies potential threats (natural disasters, tech failures, supply chain issues) and critical business functions.
- Procedures & Instructions: Details steps to take before, during, and after an event to keep services running.
- Protect Assets & People: Ensures employee safety and safeguards critical resources.
- Minimize Downtime: Reduces operational disruptions and financial/reputational loss.
- Recovery Roadmap: Provides a clear path to resume normal business activities.

1.2 How It Works

1. Analysis: Conduct a Business Impact Analysis (BIA) to understand risks and critical functions.
2. Strategy Development: Create strategies for data backup, alternative work sites, and communication.
3. Documentation: Write the formal BCP document with clear roles, responsibilities, and actions.
4. Testing & Review: Regularly test the plan to find weaknesses and update it to reflect business changes.

1.3 Disaster Recovery Plan (DRP)

- **Scope:** Technical, focused on IT infrastructure, systems, data, and applications.
- **Goal:** Restore technology and data as quickly as possible after a disaster (e.g., fire, cyberattack, hardware failure).
- **Focus:** Data backups, system recovery, defining Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), and establishing recovery sites.

1.4 How They Work Together

- A DRP is activated within the broader BCP.
- The BCP identifies what needs to continue (e.g., sales, payroll) and how (e.g., alternative work locations).
- The DRP provides the technical means (e.g., restoring the e-commerce server) to support those ongoing business functions.

1.5 Business Continuity Plan (BCP) vs. Disaster Recovery (DR)

Think of **BCP** as the whole "keep the lights on" plan (people, processes, facilities, tech), and **DR** as the technical "get the servers back" plan.

Business continuity and **disaster recovery plans** are risk management strategies that businesses rely on to prepare for unexpected incidents. While the terms are closely related, there are some key differences worth considering when choosing which is right for you:

Business continuity plan (BCP): A BCP is a detailed plan that outlines the steps an organization will take to return to normal business functions in the event of a disaster. Where other types of plans might focus on one specific aspect of recovery and interruption prevention (such as a natural disaster or cyberattack), BCPs take a broad approach and aim to ensure an organization can face as broad a range of threats as possible.

Disaster recovery plan (DRP): More detailed in nature than BCPs, disaster recovery plans consist of contingency plans for how enterprises will specifically protect their IT systems and critical data during an interruption. Alongside BCPs, DR plans help businesses protect data and IT systems from many different disaster scenarios, such as massive outages, natural disasters, ransomware and malware attacks, and many others.

Business continuity and disaster recovery (BCDR): Business continuity and disaster recovery (BCDR) can be approached together or separately depending on business needs. Recently, more and more businesses are moving towards practicing the two disciplines together, asking executives to collaborate on BC and DR practices rather than work in isolation. This has led to combining the two terms into one, BCDR, but the essential meaning of the two practices remains unchanged

1.6 Purpose

To establish a structured approach for maintaining and restoring business operations and IT systems in the event of a disruption, in accordance with NIST SP 800-34 Rev.

To ensure the continuity of critical business operations during and after a disruption, minimizing downtime and financial loss, and protecting the interests of clients, employees, and stakeholders.

1.7 NIST SP 800-34 Rev. 1 Framework for BCP.

NIST SP 800-34 Rev. 1, the "Contingency Planning Guide for Federal Information Systems," provides a structured, seven-step framework for federal agencies (and widely used in the private sector) to develop and maintain effective Information System Contingency Plans (ISCPs), which are key components within broader Business Continuity Planning (BCP), focusing on IT recovery from disruptions like cyberattacks or natural disasters, integrating risk management, and ensuring system availability. NIST SP 800-34 Rev. 1 provides the "how-to" for the crucial IT recovery piece of a comprehensive Business Continuity Plan, ensuring systems can be restored effectively after any major incident.

➢ Key Role in BCP:

Foundation: NIST SP 800-34, Rev. 1, serves as a foundational guide for the IT recovery aspects of an organization's overall BCP.

ISCP Focus: It details the creation of Information System Contingency Plans (ISCPs) for different IT platforms (client/server, telecom, mainframe).

Integration: It links IT contingency planning with broader security, risk management, and emergency preparedness programs.

Key Steps & Concepts (from the guide):

- **Risk Management:** Understanding threats and vulnerabilities.
- **Business Impact Analysis (BIA):** Determining system criticality.
- **Recovery Strategies:** Developing methods to restore IT services.
- **Plan Development:** Creating the formal ISCP.
- **Testing, Training, & Exercises (TT&E):** Validating the plan.
- **Maintenance:** Updating the plan.
- **Authority:** Gaining formal approval.

How it Supports BCP:

- **Resilience:** Helps maintain vital functions during disruptions.
- **Compliance:** Aligns with other NIST standards (like SP 800-53) and supports requirements like FISMA.
- **Structured Approach:** Offers a systematic process for IT preparedness, complementing broader BCPs that cover people, processes, and physical locations.

1.8 Applicability

Applies to all departments, systems, and personnel involved in critical operations.

1.9 Scope

Covers contingency planning for:

- Engineering design and simulation systems

- IT infrastructure and data
- Client communications
- Human resources and payroll
- Supply chain and procurement
- Engineering project delivery
- Physical office locations

1.10 Objectives

- Maintain essential operations during a crisis
- Recover full functionality within defined timeframes
- Protect company assets and data
- Ensure employee safety and communication

2.0 Risk Assessment

Risk assessment in Business Continuity Planning (BCP) is the crucial process of identifying, analyzing, and prioritizing potential threats (like cyberattacks, natural disasters, or system failures) and vulnerabilities to understand their impact on critical business functions, enabling organizations to develop strategies and allocate resources effectively to minimize downtime and ensure operations can continue. It involves threat identification, vulnerability analysis, and impact assessment to build a resilient plan for recovery.

2.1 Key Steps in BCP Risk Assessment

1. **Identify Threats:** Catalog all potential internal and external events (e.g., power outages, data breaches, pandemics, hardware failures) that could disrupt operations.
2. **Analyze Vulnerabilities:** Examine weaknesses in existing systems, processes, and infrastructure that could be exploited by these threats.
3. **Assess Impact:** Determine the consequences (operational, financial, reputational) if a disruption occurs, often using qualitative (High/Medium/Low) or quantitative methods.
4. **Determine Likelihood:** Estimate how probable each threat-vulnerability combination is.
5. **Prioritize Risks:** Rank risks based on their combined impact and likelihood to focus on the most critical ones first.
6. **Develop Mitigation Strategies:** Create plans (e.g., data backups, alternate sites, incident response teams) to reduce or eliminate identified risks.

2.2 Core Components

- **Critical Assets & Functions:** What the business absolutely needs to keep running (data, systems, personnel).
- **Threats:** Things that could go wrong (fire, flood, cyberattack).
- **Vulnerabilities:** Weaknesses that make threats more likely or impactful (outdated software, lack of backup power).

- **Impact Analysis:** How bad it would be if it happened (lost revenue, regulatory fines).

Risk Assessment Table.

Threat	Likelihood	Impact	Mitigation Strategy
Cyberattack	High	High	Firewalls, backups, training
Power Outage	Medium	Medium	UPS systems, generators
Natural Disaster	Low	High	Remote work capability
Server Failure	Medium	High	Cloud backups, redundancy
Pandemic	Low	High	Remote work, health protocols

2.3 System Identification Table.

System Name	Function	Owner	Criticality
CAD/CAE Systems	Engineering Design	Engineering Dept.	High
ERP System	Resource Planning	Operations	High
Email & VoIP	Communication	IT Dept.	High
HRMS	Payroll & HR	HR Dept.	Medium
File Server	Data Storage	IT Dept.	Critical

3.0 Business Impact Analysis (BIA).

A Business Impact Analysis (BIA) is the foundational step in Business Continuity Planning (BCP), systematically identifying critical business functions, quantifying disruption impacts (financial, reputational, operational), and setting recovery priorities (RTO/RPO) to guide resource allocation for recovery and ensure resilience against disasters. It answers "what's critical," "how bad is the impact," and "how fast must we recover," directly informing the strategies within the broader BCP.

3.1 Key Components of a BIA in BCP

- **Identify Critical Processes:** Determine essential business functions and the supporting systems/resources.
- **Assess Impacts:** Evaluate potential consequences of disruption, including:
- **Financial:** Lost revenue, fines.
- **Reputational:** Loss of customer trust, brand damage.
- **Operational:** Service disruption, inability to deliver products.
- **Legal/Regulatory:** Non-compliance**.**
- **Define Downtime Tolerances:**
- **Maximum Tolerable Downtime (MTD):** The absolute longest a process can be down.
- **Recovery Time Objective (RTO):** Target time to restore a function after an outage (e.g., 4 hours).
- **Recovery Point Objective (RPO):** Maximum acceptable data loss (e.g., last hour's data).
- **Identify Dependencies:** Map interdependencies between processes, systems, and third-party vendors.
- **Prioritize Recovery:** Rank processes based on impact severity to focus recovery efforts.

3.2 How BIA Informs the BCP

- **Provides Data:** BIA supplies concrete data (RTOs, RPOs, impact levels) needed to build an effective BCP.

- **Guides Strategy:** Dictates what to protect and how quickly, influencing the choice of recovery methods (e.g., hot sites, data backups).
- **Saves Resources:** Prevents over-investing in low-priority areas by highlighting critical functions, optimizing resource use in a crisis.

System/Process	Impact of Downtime	RTO	RPO
CAD/CAE Systems	Project delays, client dissatisfaction	24 hrs	4 hrs
ERP System	Operational disruption	8 hrs	2 hrs
Email & VoIP	Communication breakdown	4 hrs	1 hr
HRMS	Payroll delays	48 hrs	24 hrs
File Server	Data loss, project halt	8 hrs	2 hrs

Business Function	Impact of Disruption	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)
Engineering Design Services	High	24 hours	4 hours
Client Communication	High	4 hours	1 hour
IT Infrastructure	Critical	8 hours	2 hours
HR & Payroll	Medium	48 hours	24 hours
Procurement & Supply Chain	Medium	72 hours	12 hours

In essence, the BIA is the analysis, and the BCP is the plan developed from that analysis to ensure the business can withstand and recover from disruptions.

3.3 Roles and Responsibilities

Role	Responsibility
BCP Coordinator	Oversee BCP execution
IT Manager	Restore systems and data
HR Manager	Employee communication
Project Managers	Client updates and project continuity
Safety Officer	Physical safety and evacuation

4.0 Preventive Controls

- Daily encrypted backups to cloud
- Redundant power supply (UPS + generator)
- Endpoint protection and firewalls
- Employee cybersecurity training
- Physical access controls to server rooms

5.0 Contingency Strategies

➢ **Backup and Recovery**

- Offsite and cloud backups
- Weekly full backups, daily incremental

- Backup verification monthly

➢ **Alternate Processing**

- Cloud-based CAD/CAE access
- Remote work infrastructure (VPN, laptops)
- Alternate office location in Ikeja, Lagos

➢ **Manual Workarounds**

- Paper-based documentation for procurement and HR
- Mobile phones for client communication

6.0 Plan Activation and Notification

➢ **Activation Criteria**

- System outage > 2 hours
- Natural disaster affecting office
- Cyberattack or data breach

➢ **Notification Procedures**

- Notify BCP Coordinator
- Activate emergency communication tree
- Inform clients via email and website

7.0 Recovery Procedures.

❖ **CAD/CAE Systems**

- Restore from cloud backup
- Validate file integrity
- Resume design operations

❖ **ERP System**

- Restore database

- Test transaction processing
- Resume procurement and inventory tracking

❖ **Communication Systems**

- Switch to backup VoIP
- Use mobile and SMS alerts
- Resume email services

8.0 Reconstitution

- Restore full operations at primary site
- Conduct post-incident review
- Update BCP based on lessons learned
- Notify stakeholders of full recovery

9.0 Testing, Training, and Exercises

➢ **Test Types**

- **Tabletop Exercises**: Simulate cyberattack response
- **Functional Tests**: Restore systems from backup
- **Full-Scale Exercises**: Remote work simulation

➢ **Frequency**

- Tabletop: Quarterly
- Functional: Bi-annually
- Full-scale: Annually

➢ **Training**

- Annual BCP training for all staff
- Role-specific training for IT and engineering teams

10. Maintenance

- Review BCP annually or after major changes
- Update contact lists and system inventories
- Document all tests and incidents

11. Appendices

- **A**: Emergency Contact List
- **B**: Critical Vendors and Suppliers
- **C**: Backup Locations and Cloud Providers
- **D**: Insurance and Legal Documents
- **E**: BCP Test Log Template

References.

- National Institute of Standards and Technology. (2010). *Contingency planning guide for federal information systems* (NIST Special Publication 800-34, Rev. 1). Gaithersburg, MD: U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-34r1 (doi.org in Bing)
- National Institute of Standards and Technology. (2013). *Security and privacy controls for federal information systems and organizations* (NIST Special Publication 800-53, Rev. 4). Gaithersburg, MD: U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r4 (doi.org in Bing)
- Federal Information Security Management Act of 2002, 44 U.S.C. § 3541 et seq. (2002).
- Osiobe, J. E. (2025). *Business continuity plan (BCP) tailored to a typical electronic security services company: Using NIST SP 800-34 Rev. 1 framework* (Version 1.0).