03 June 2026

Business continuity and disaster recovery in digital governance

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

Kelebogile Moyo
State Information Technology Agency (SITA)

Strategies to maintain operations during cyber threats

Understanding Business Continuity as a Discipline

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Definition and Scope

Business Continuity ensures critical products and services continue after disruptions, covering people, processes, technology, and facilities.

Prioritization of Critical Functions

Identifying and prioritizing key business functions allows strategic restoration and alternative workarounds during incidents.

Governance Framework

Clear roles and responsibilities reduce confusion, supporting crisis management and alignment with standards

Business Continuity for Ransomware

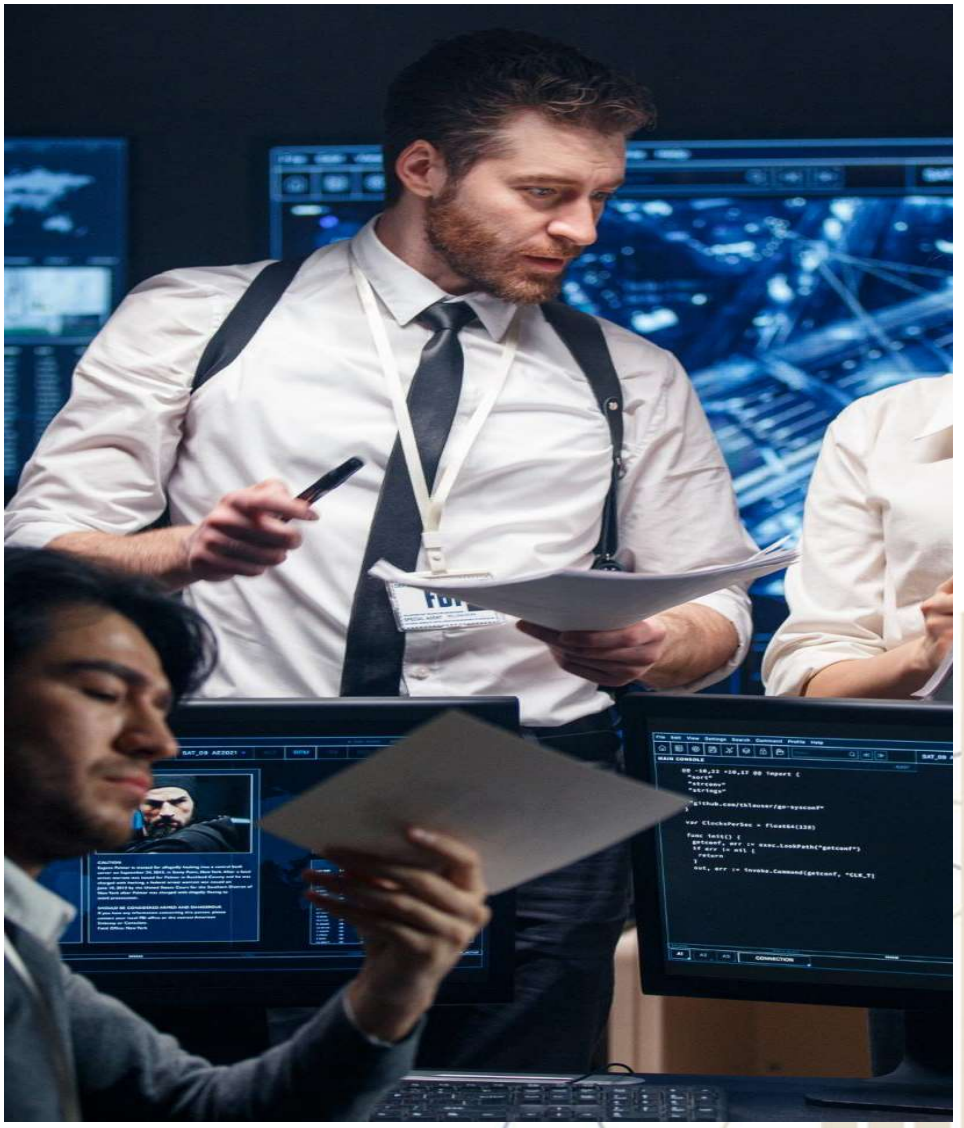
CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Ransomware Threat Complexity
Ransomware attacks are intentional, adaptive, and prolonged, requiring plans that assume intelligent adversaries targeting recovery systems.

Focus on Resilience and Recovery
Business Continuity prioritizes resilience, rapid recovery, and controlled decision-making to limit downtime and losses.

Operational Priorities During Attacks
Identifying critical services and alternative operations ensures business functions continue despite system disruptions.

Governance and Coordination
Aligning IT, legal, compliance, and leadership avoids conflicting responses and ensures disciplined execution under pressure.



Ransomware Threat Landscape Overview

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Ransomware Evolution

Ransomware attacks have evolved from opportunistic to organized criminal operations using double and triple extortion.

Common Attack Vectors

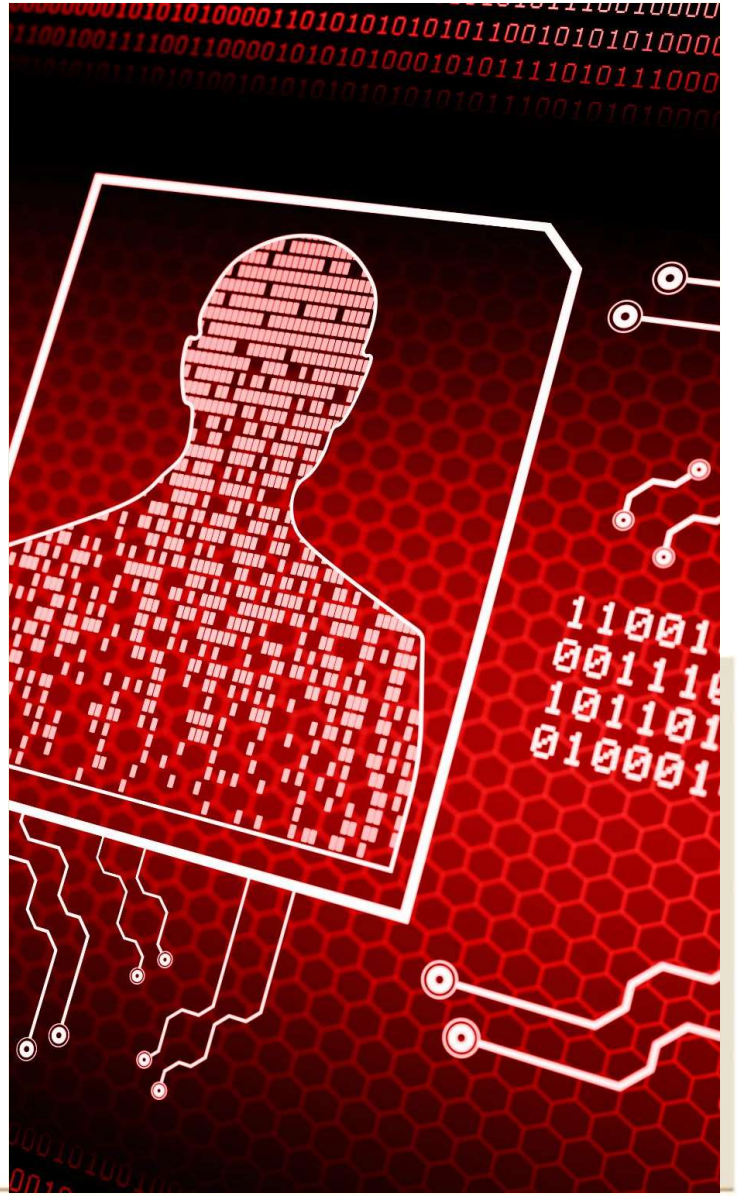
Phishing, compromised remote access, unpatched vulnerabilities, and supply chain attacks are common ransomware entry points.

Impact on Business Continuity

Ransomware causes severe financial loss, operational disruption, and risks human safety in critical sectors.

Recovery and Preparedness

Effective business continuity plans must address complex ransomware threats with comprehensive recovery and communication strategies.



Why Business Continuity is Critical for Ransomware Attacks

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Operational Impact of Ransomware

Ransomware attacks cause immediate operational disruption by denying access to critical systems and data.

Financial Consequences of Downtime

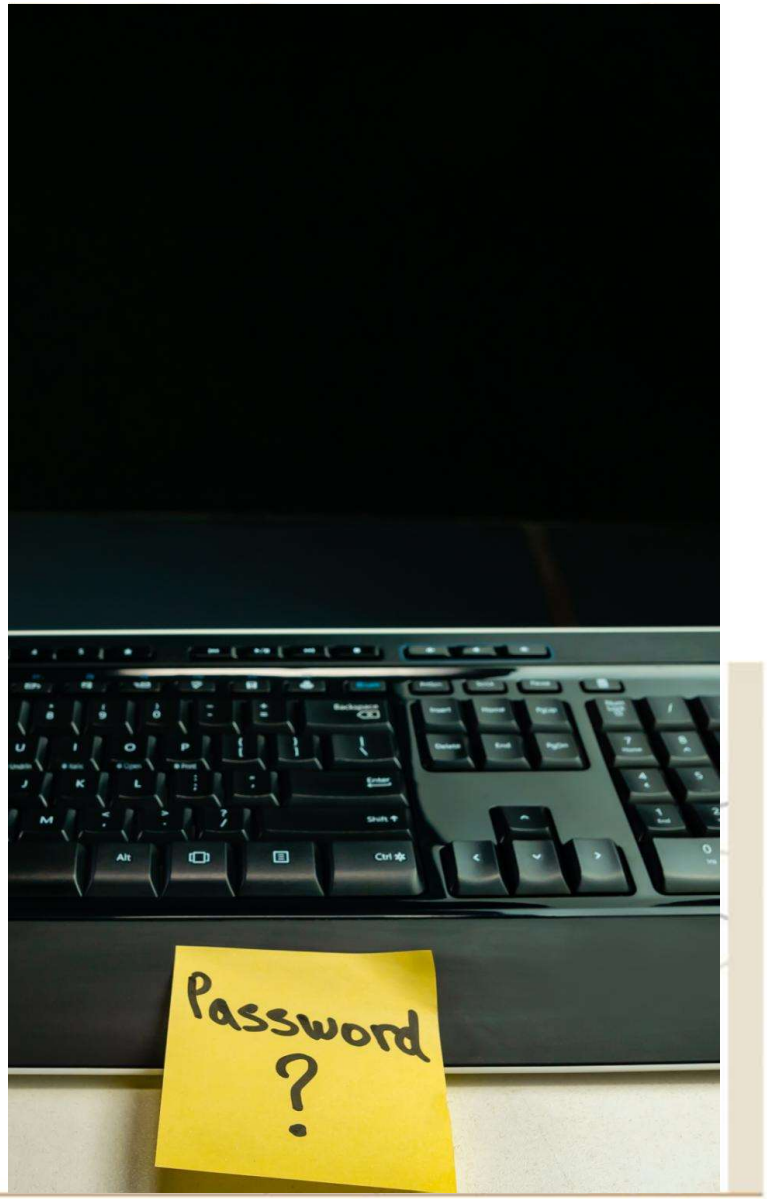
Downtime leads to rapid revenue loss while fixed costs continue, escalating financial risks.

Regulatory and Legal Risks

Failing to restore services timely can result in fines, sanctions, or loss of licenses.

Reputational Protection

Effective business continuity ensures transparent communication preserving stakeholder trust during disruptions.



Principles, Planning, and Integration

Core Business Continuity Principles for Ransomware

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Assume Breach Mindset

Plan for the likelihood of a successful attack to develop realistic recovery strategies.

Resilience Over Perfection

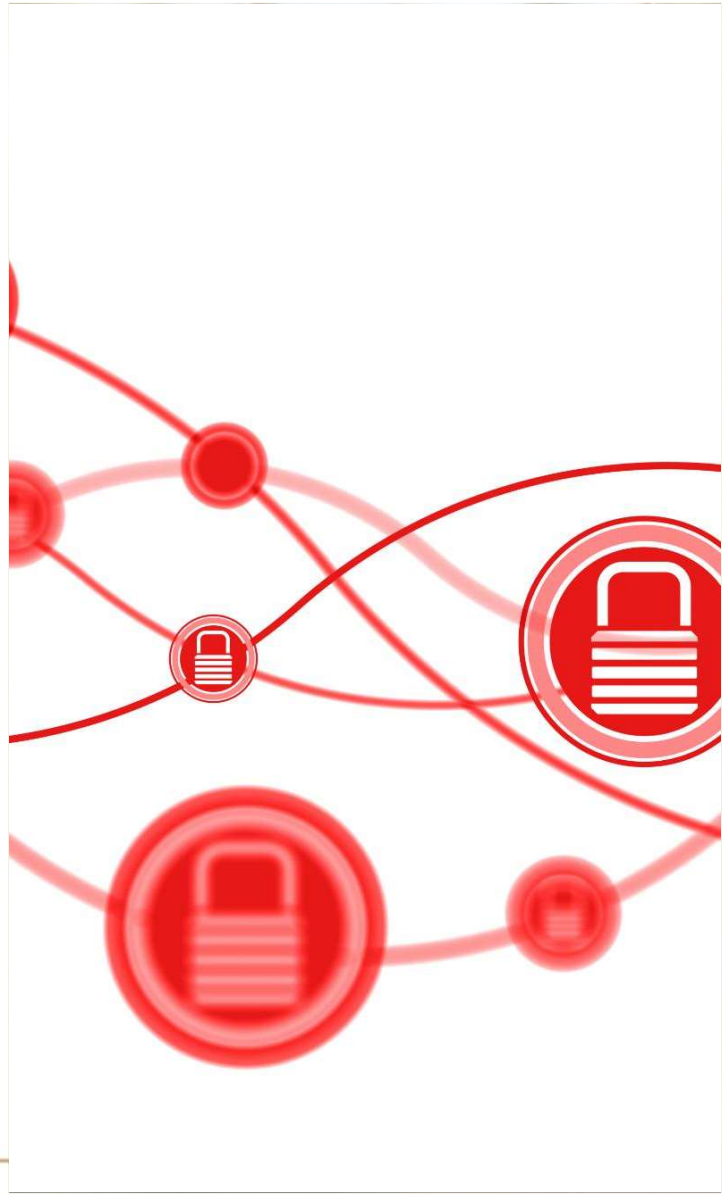
Prioritize maintaining critical services to stabilize operations and reduce impact during disruptions.

Segmentation and Isolation

Separate critical systems and backups to prevent attackers from compromising entire environments.

Clear Roles and Communication

Define decision rights and communication protocols for coordinated response during ransomware attacks.



Key Components of a Ransomware-Focused BC Plan

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Business Impact Analysis (BIA)

BIA identifies critical processes and downtime limits, guiding recovery time and point objectives effectively.

Ransomware Risk Assessment

Risk assessment focuses on ransomware threats, attack vectors, and system vulnerabilities to improve defenses.

Incident Response Integration

Incident Response coordinates attack containment with continuity plans to maintain or resume operations.

Disaster Recovery and Communication

Disaster recovery ensures IT system restoration while communication plans manage internal and external information flow.

Integrating Business Continuity with Incident Response

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Distinct Roles in Incident Management

Incident Response targets technical attack handling, while Business Continuity maintains or restores ongoing business functions effectively.

Shared Planning and Coordination

Integration starts with joint planning and clear communication between Incident Response and Business Continuity teams to prevent gaps and duplicated efforts.

Joint Exercises and Trust Building

Simulations and exercises foster shared awareness and trust, enhancing decision-making during ransomware incidents and complex trade-offs.

Implementation: From Analysis to Action

Conducting a Ransomware Risk Assessment

Identifying Ransomware Threats

Start by identifying realistic ransomware threat scenarios such as phishing, exposed service exploits, and insider threats.

Evaluating Vulnerabilities

Assess vulnerabilities in people, processes, and technology including patch gaps and weak authentication methods.

Estimating Business Impact

Estimate financial loss, downtime, regulatory risks, and reputational damage to prioritize continuity efforts.

Business Impact Analysis (BIA)

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Purpose of BIA

BIA identifies essential business processes and prioritizes their restoration during ransomware incidents.

Recovery Time and Point Objectives

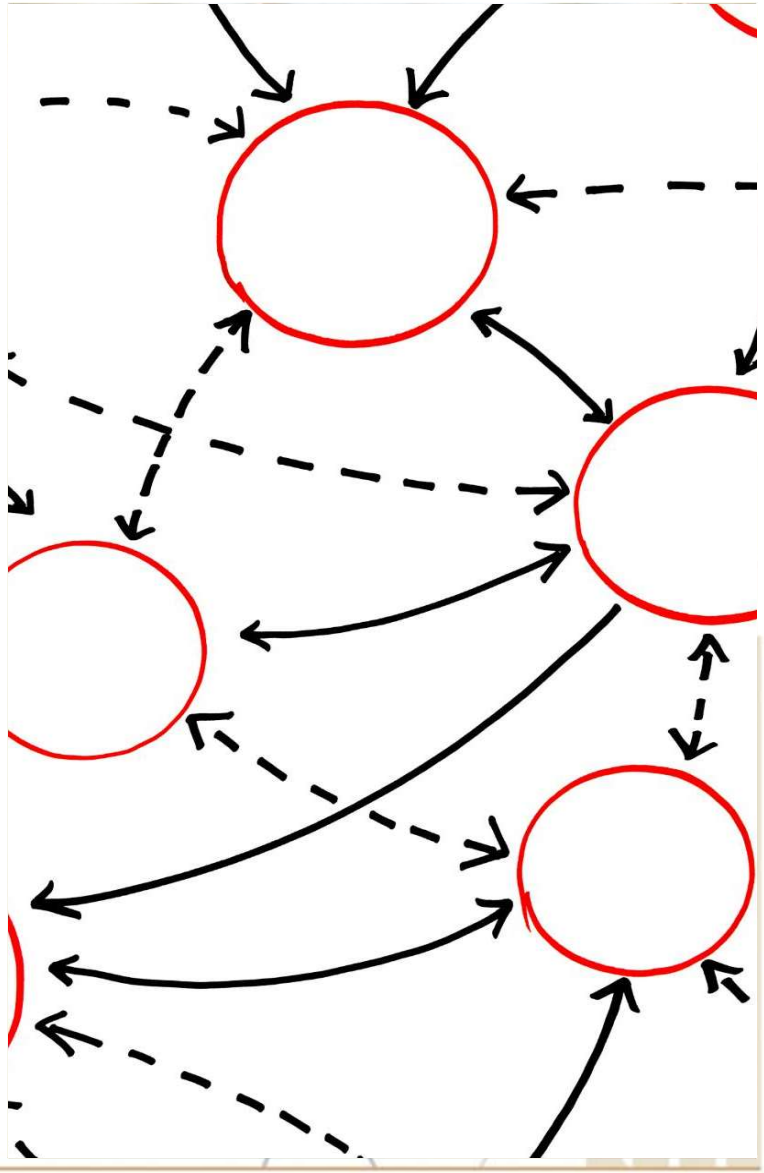
Defines RTOs and RPOs to determine acceptable downtime and data loss for critical systems.

Dependencies Identification

BIA maps key dependencies like suppliers, platforms, and personnel affecting recovery strategies.

BIA as Strategic Bridge

BIA connects business priorities to technical continuity solutions for effective ransomware response.



Developing Recovery Strategies

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Backup Protection

Backups must be isolated, immutable, and have restricted access to prevent ransomware attacks.

System Redundancy

Secondary data centers and cloud recovery environments help reduce downtime during recovery.

Alternative Workarounds

Manual processes and third-party services provide continuity when automated recovery is delayed.

Balanced Recovery Planning

Recovery strategies should align with business priorities balancing cost, complexity, and risk tolerance.

Communication, Testing, Monitoring, and Review

Communication Planning During Ransomware Incidents

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Importance of Communication Planning

Effective communication prevents reputational damage, reduces confusion, and mitigates regulatory risks during ransomware incidents.

Internal Communication Strategies

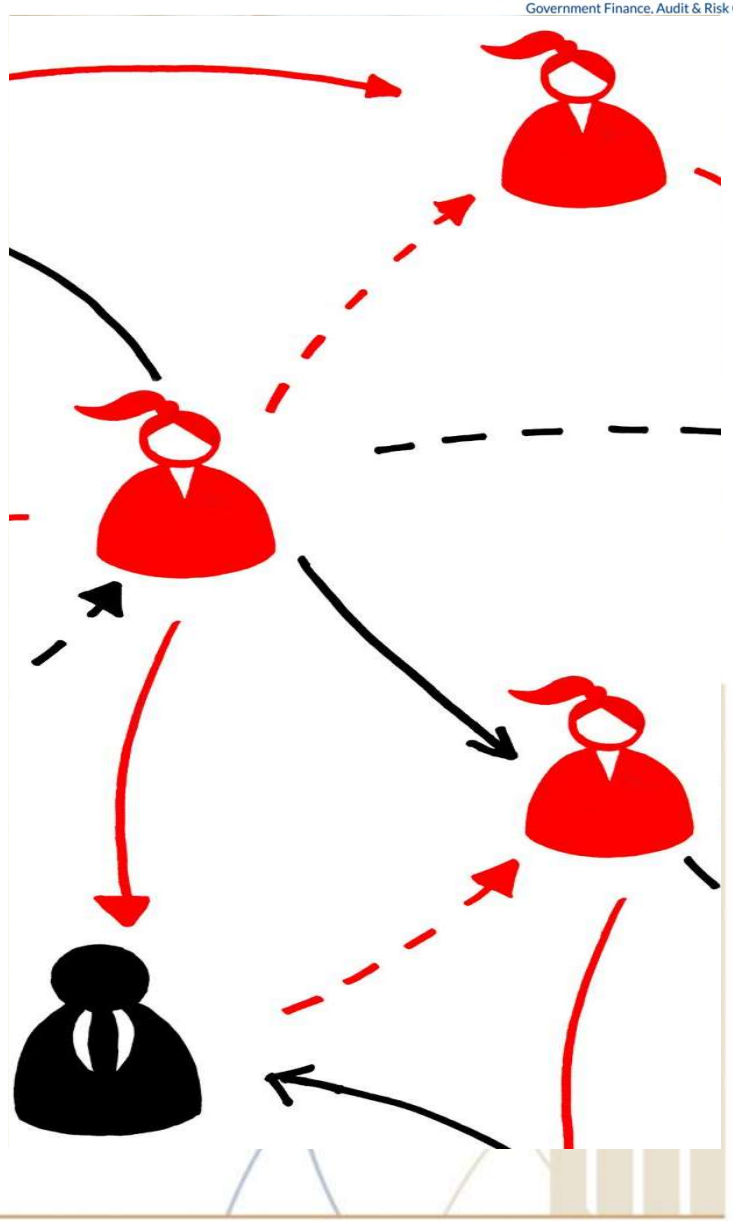
Clear internal messages ensure employees understand their roles and reduce misinformation and panic.

External Communication Coordination

Timely, accurate messages to customers, regulators, and media help maintain trust and compliance.

Alternative Communication Channels

Planning for backups like emergency messaging ensures communication continuity when primary systems fail.



Testing Business Continuity Plans

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Importance of Testing

Testing validates plans, roles, and recovery mechanisms to prevent critical gaps during real incidents.

Types of Tests

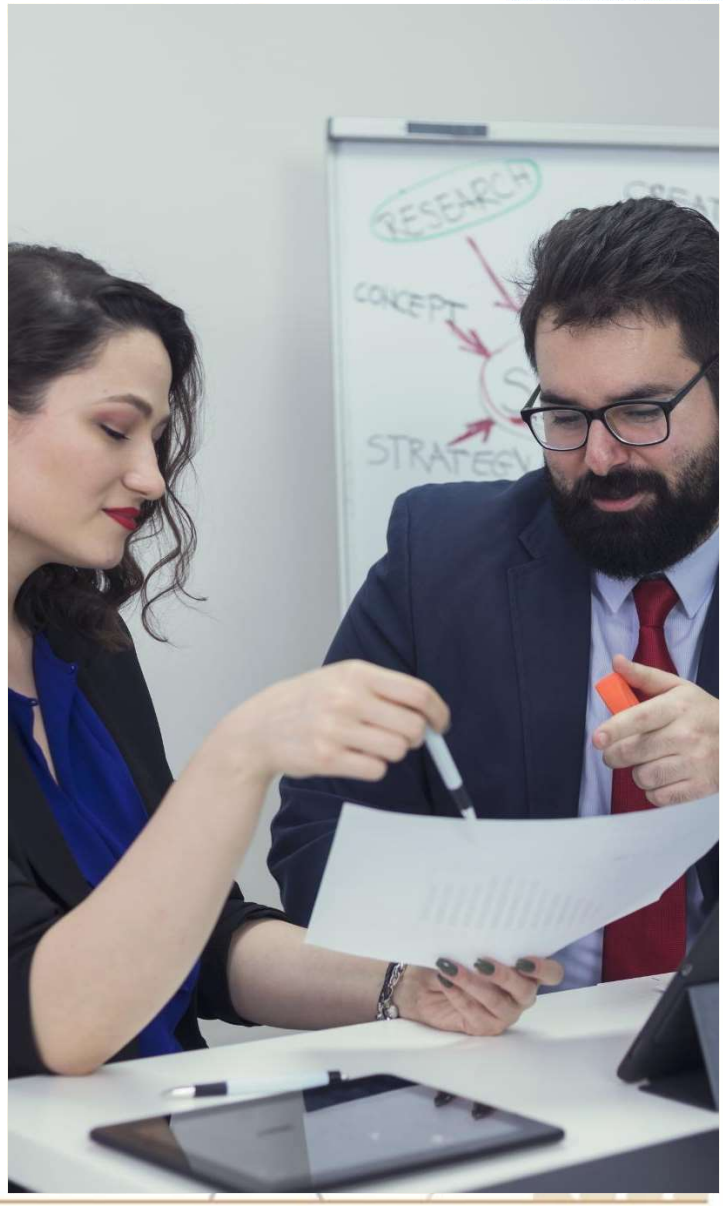
Tabletop, simulation, and full recovery tests serve distinct purposes in preparing for ransomware incidents.

Ransomware-Specific Scenarios

Testing scenarios include partial backups, compromised credentials, and system rebuilds to enhance readiness.

Continuous Improvement

Lessons learned from testing improve plans, training, and recovery strategies over time.



SITA Information and Cyber Security Services

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Security Consulting Services

Security Architecture

- ICT Security Strategy Development
- ICT Security Architecture Development

Security Governance

- ICT Security Policy Evaluation, Development
- Security Awareness

Security Risk Management

- ICT Security Risk Assessment
- Disaster Recovery Planning
- Business Continuity Planning
- Forensic

Security Operations

Security Operations

- Vulnerability Assessments
- Website Vulnerability Management
- SSL Certificates(TLS)
- Security Operations Centre (SIEM)
- Penetration Test **
- Endpoint Protection

Business Continuity Planning

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Service Description

We offer customers service packages that identify mission critical business functions and enact policies, processes, plans as well as procedures to ensure continuation of these functions in the case of an unforeseen event.

Business Continuity Planning (BCP) is a methodology used to create and validate a plan for maintaining continuous business operations before, during, and after disasters and disruptive events.

Business continuity has to do with keeping the company running, regardless of the potential risk, threat, or cause of an outage.

BCP focuses on sustaining an organization's mission/business functions during and after a disruption.

Deliverables	Activities
Project plan	1. Define project scope and approach 2. Manage performance of activities against the project plan
Information risk assessment	1. Review all areas for potential weaknesses 2. Information risk assessment report
Business impact analysis	1. Identify business processes 2. Categorise business functions and processes according to criticality 3. Determine business recovery objectives
Business continuity strategy	1. Identify and document business strategies 2. Identify actions for risk mitigations
Business continuity plan	1. Document the processes required to recover the orgnizations business operations
Business continuity plan maintenance	1. Update BC Plan

Disaster Recovery Planning

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Service Description

We develop information system-focused Disaster Recovery Plans for customers designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site in cases of emergency.

The Disaster Recovery Plan (DRP) applies to a major disruptions to service that deny access to the primary facility infrastructure for an extended period.

A DRP is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency.

The DRP may be supported by multiple information system contingency plans to address recovery of impacted individual systems once the alternate facility has been established.

Deliverables	Activities
Project plan	1. Define project scope and approach 2. Manage performance of activities against the project plan
Information Risk assessment	1. Review all areas for potential weaknesses 2. Information risk assessment report
Business impact analysis	1. Identify business processes 2. Categorise business functions and processes according to criticality 3. Determine business recovery objectives
Disaster Recovery strategy	1. Identify and document risk mitigations strategies
Disaster Recovery Plan	1. Document the processes required to recover the organization's business operations
Disaster Recovery Plan Maintenance	1. Maintain and continuously improve the DR Plan

Thank You!

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

www.cigfaro.co.za

SAQA Recognised Professional Body