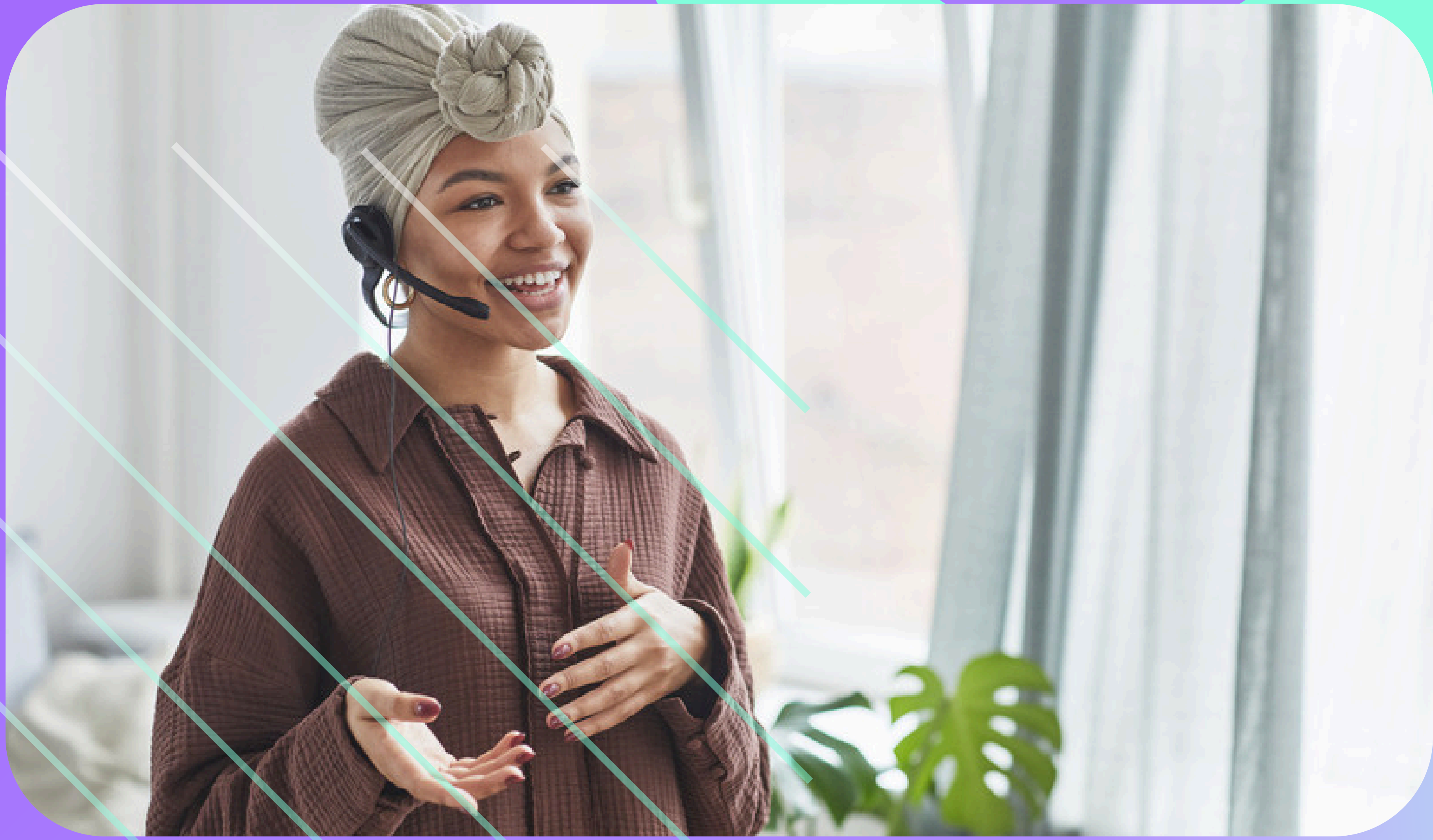
Business Impact Analysis & Business Continuity Planning

Ensuring Operational Resilience for a Healthcare Technology Organization



Presented By: **Jacinta Izundu**

Context & Organization Overview

Purpose of This Project

- Conducted a full Business Impact Analysis (BIA) and Business Continuity Plan (BCP)
- Focused on business and IT operations supporting healthcare services
- Designed to reduce operational, financial, and regulatory risk

Organization Profile

- Healthcare technology organization with 600+ employees
- Multiple locations and geographically distributed data centers
- Supports secure messaging, billing, and provider directory services

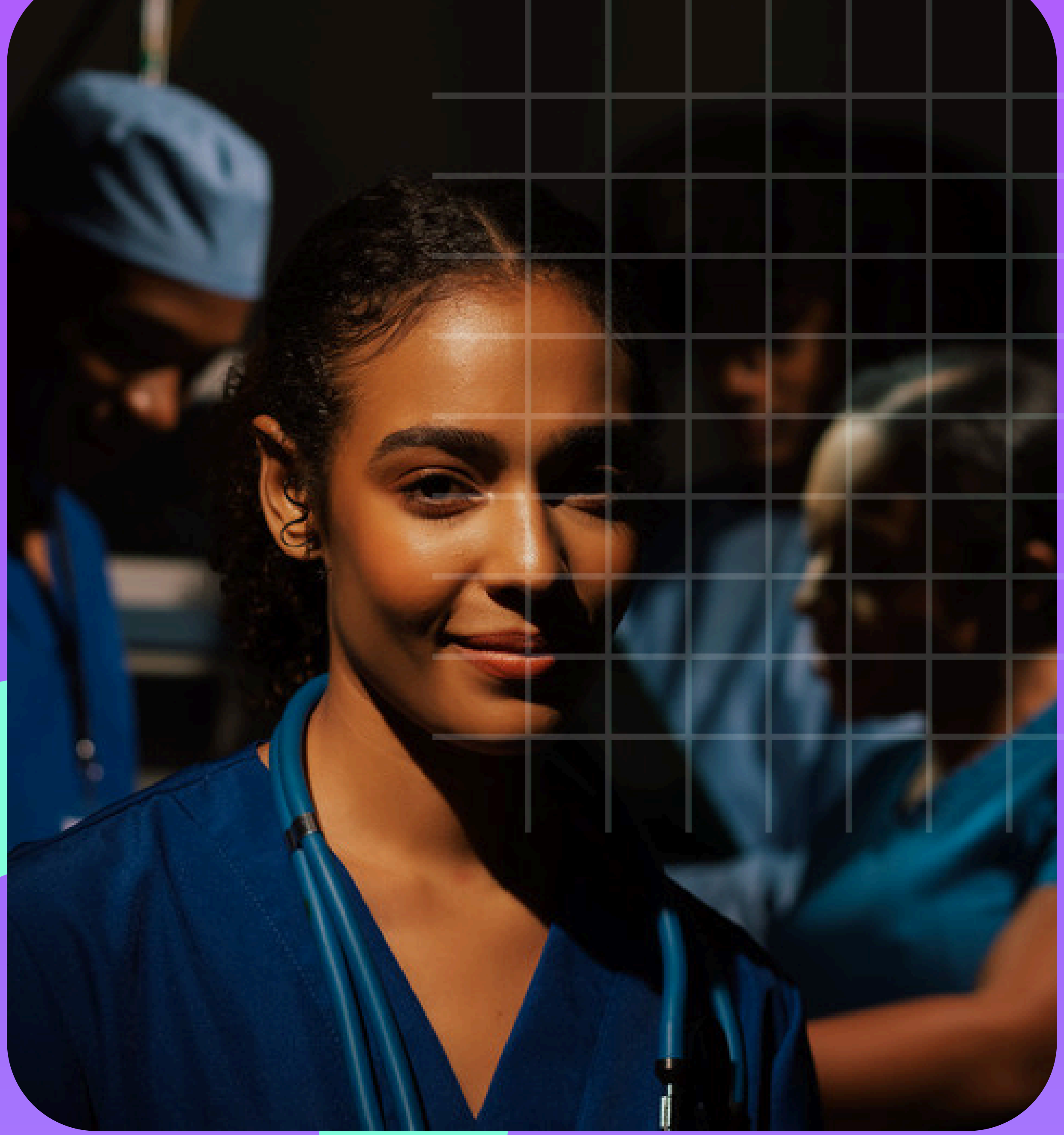
Why Business Continuity Matters in Healthcare

Key Business Risks Addressed

- Revenue loss from system downtime
- Regulatory exposure (HIPAA, PCI-DSS)
- Reputational damage
- Disruption to patient-supporting services

Goal

- Ensure critical business functions remain available
- Enable fast, compliant recovery during disruptions



Scope of The BIA & BCP

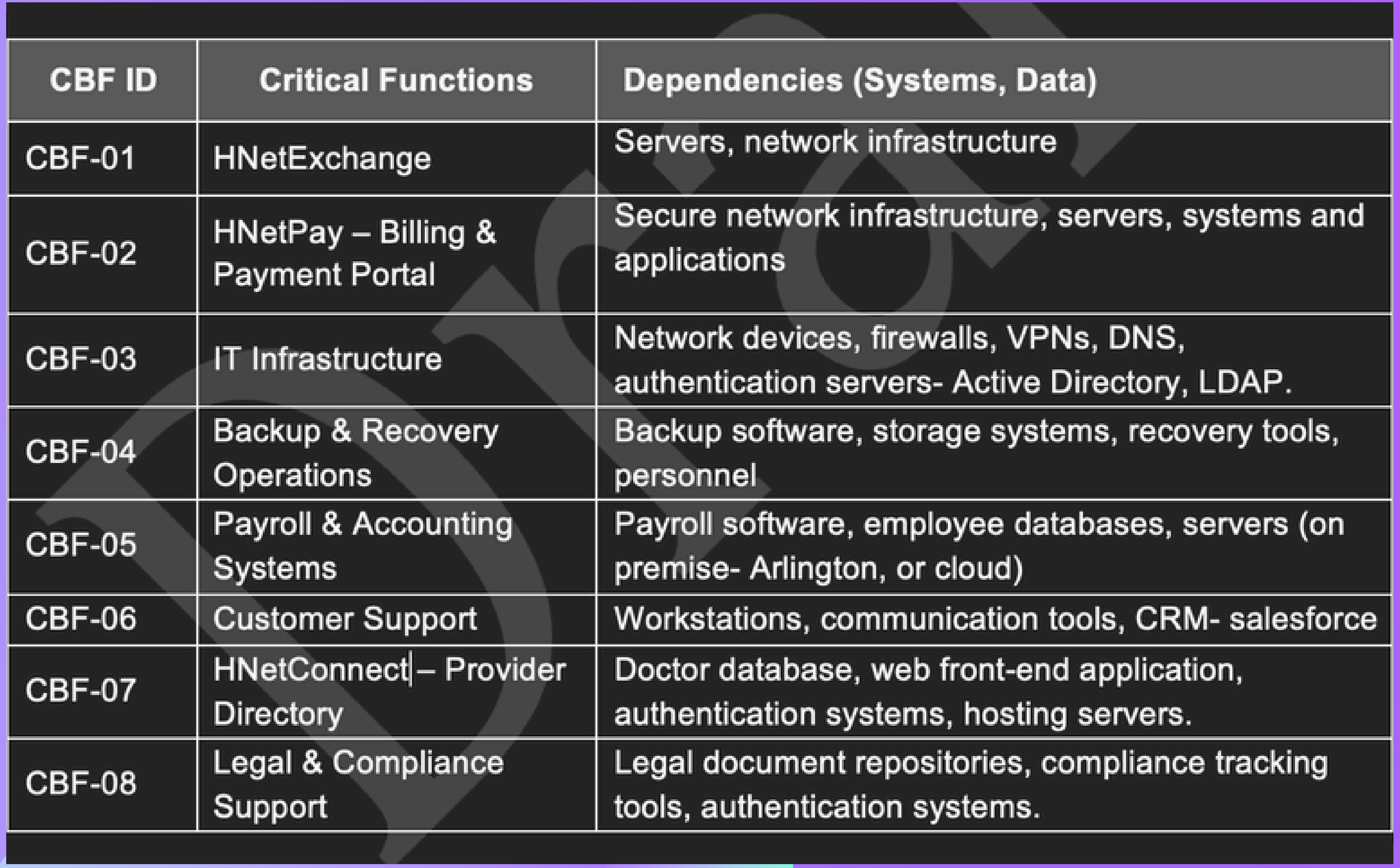
What Was Covered

- Core business applications
- IT infrastructure and data centers
- Privacy-sensitive data (PHI, PII)
- Payroll, customer support, legal & compliance functions

What Was Not Covered

- Clinical decision-making
- Medical treatment workflow

Critical Business Functions Identified



CBF ID	Critical Functions	Dependencies (Systems, Data)
CBF-01	HNetExchange	Servers, network infrastructure
CBF-02	HNetPay – Billing & Payment Portal	Secure network infrastructure, servers, systems and applications
CBF-03	IT Infrastructure	Network devices, firewalls, VPNs, DNS, authentication servers- Active Directory, LDAP.
CBF-04	Backup & Recovery Operations	Backup software, storage systems, recovery tools, personnel
CBF-05	Payroll & Accounting Systems	Payroll software, employee databases, servers (on premise- Arlington, or cloud)
CBF-06	Customer Support	Workstations, communication tools, CRM- salesforce
CBF-07	HNetConnect – Provider Directory	Doctor database, web front-end application, authentication systems, hosting servers.
CBF-08	Legal & Compliance Support	Legal document repositories, compliance tracking tools, authentication systems.

Key Systems Analyzed

- Secure medical messaging platform
- Billing & payment portal
- Provider directory system
- IT infrastructure & authentication services
- Payroll, customer support, and compliance operations

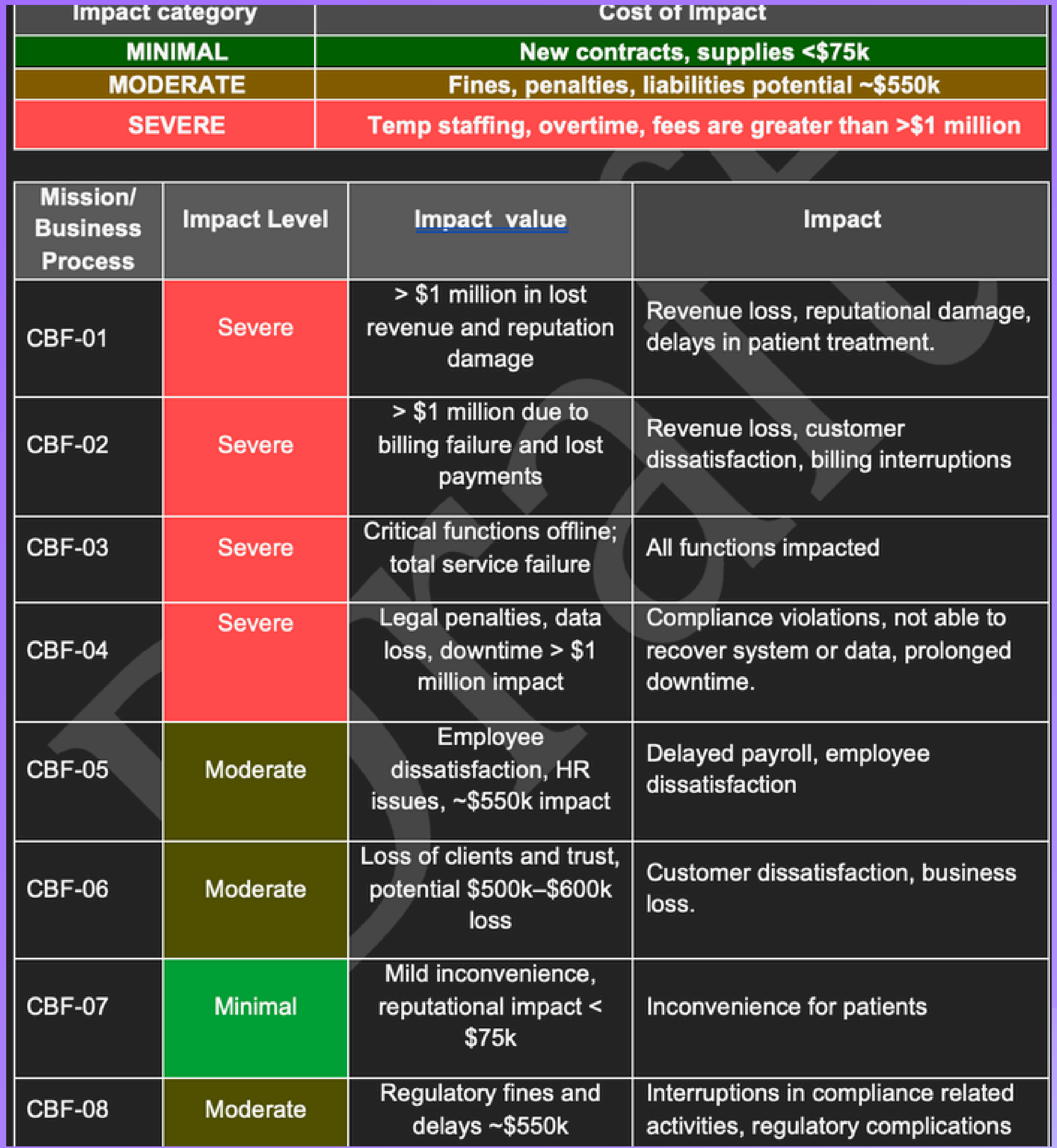
Impact Analysis

Impact Categories Evaluated

- Financial impact
- Legal & regulatory impact
- Reputational impact
- Service delivery impact

Key Findings

- Several systems had severe financial and compliance impact
- Some outages exceeded $1M in potential losses
- Infrastructure downtime affected all business functions



Impact category	Cost of Impact
MINIMAL	New contracts, supplies <$75k
MODERATE	Fines, penalties, liabilities potential ~$550k
SEVERE	Temp staffing, overtime, fees are greater than >$1 million

Mission/ Business Process	Impact Level	Impact value	Impact
CBF-01	Severe	> $1 million in lost revenue and reputation damage	Revenue loss, reputational damage, delays in patient treatment.
CBF-02	Severe	> $1 million due to billing failure and lost payments	Revenue loss, customer dissatisfaction, billing interruptions
CBF-03	Severe	Critical functions offline; total service failure	All functions impacted
CBF-04	Severe	Legal penalties, data loss, downtime > $1 million impact	Compliance violations, not able to recover system or data, prolonged downtime.
CBF-05	Moderate	Employee dissatisfaction, HR issues, ~$550k impact	Delayed payroll, employee dissatisfaction
CBF-06	Moderate	Loss of clients and trust, potential $500k–$600k loss	Customer dissatisfaction, business loss.
CBF-07	Minimal	Mild inconvenience, reputational impact < $75k	Inconvenience for patients
CBF-08	Moderate	Regulatory fines and delays ~$550k	Interruptions in compliance related activities, regulatory complications

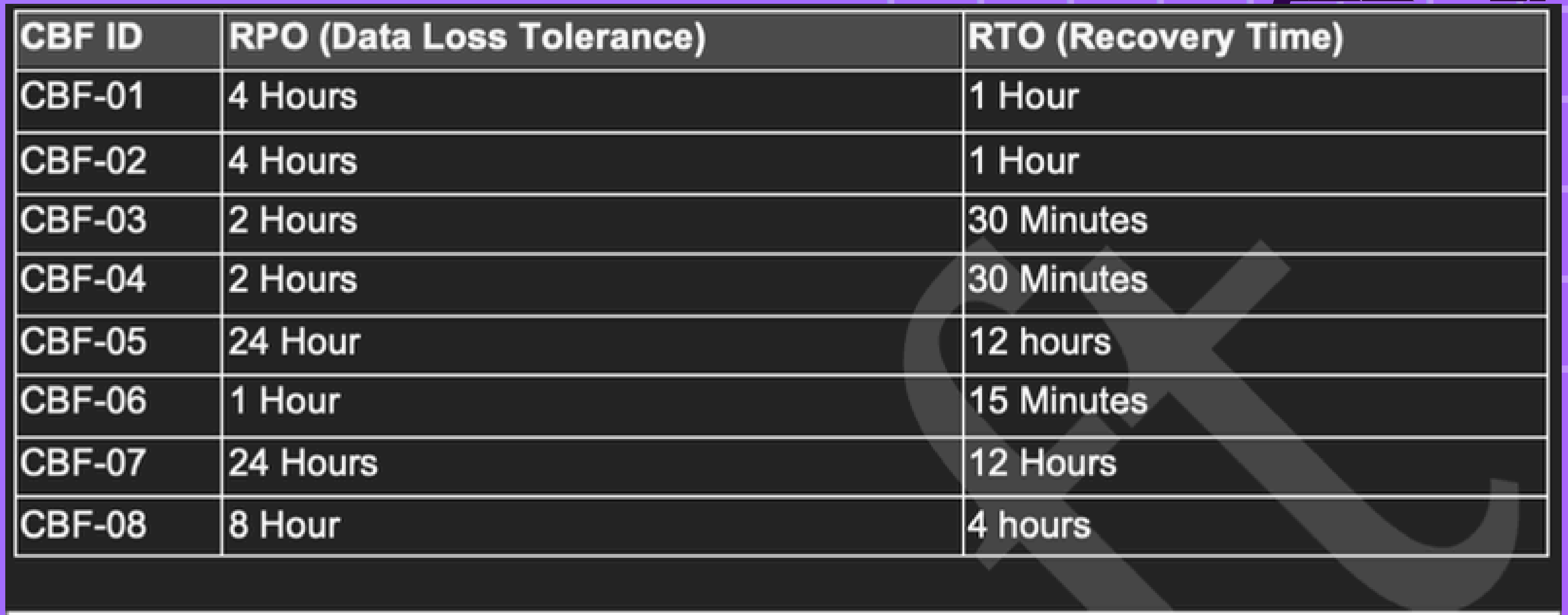
Downtime Tolerance & Recovery Objectives

Key Metrics Defined

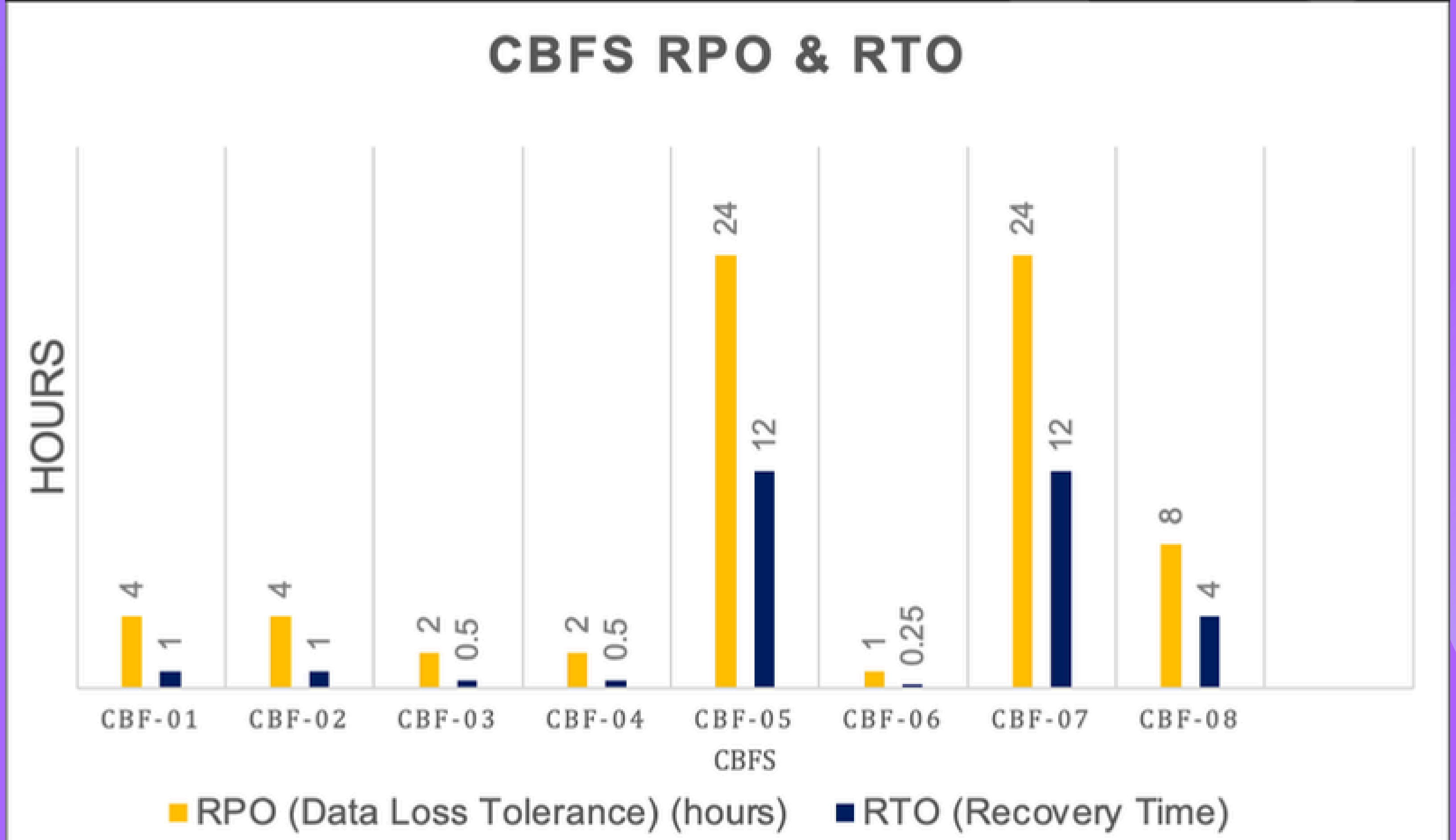
- MAO (Maximum Acceptable Outage)
- RTO (Recovery Time Objective)
- RPO (Recovery Point Objective)

Why This Matters

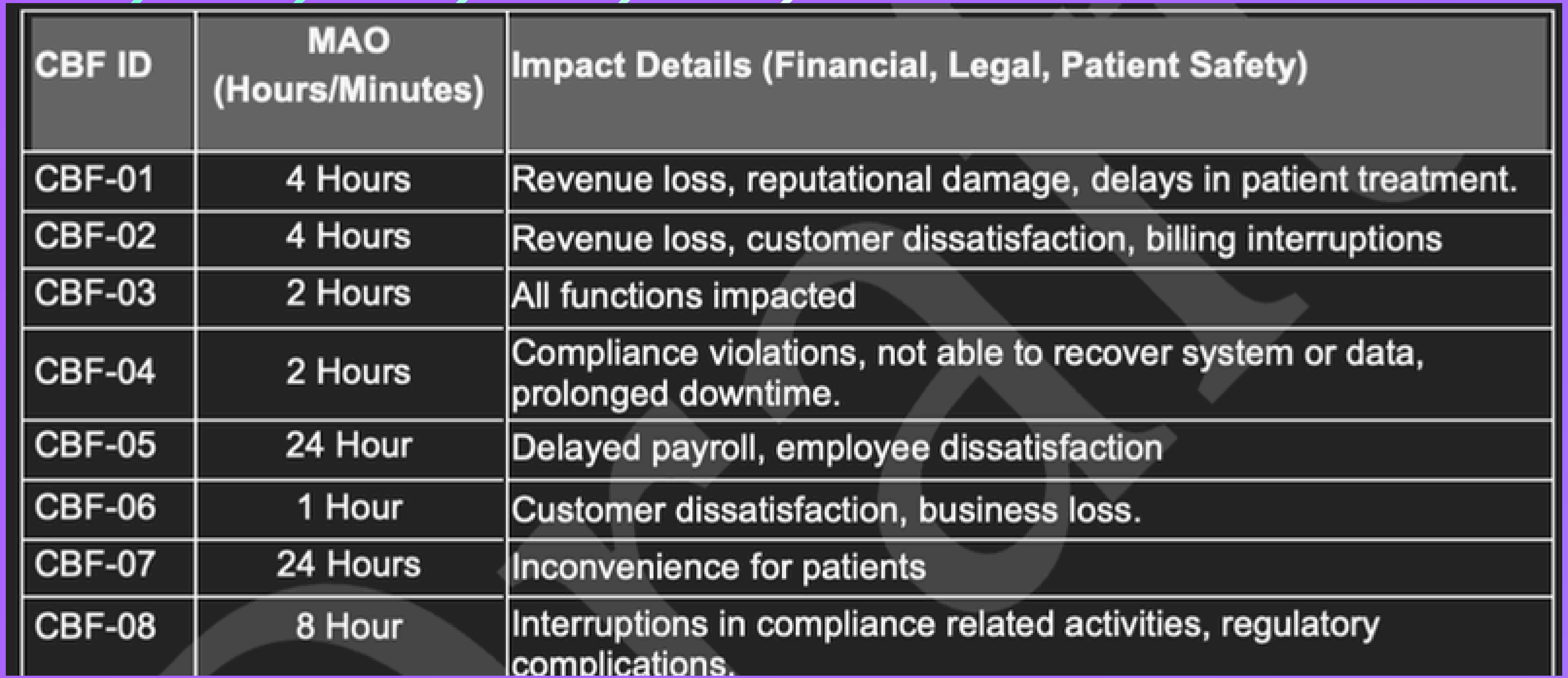
- Guides recovery sequencing
- Aligns IT recovery with business tolerance
- Supports audit and compliance expectations



CBF ID	RPO (Data Loss Tolerance)	RTO (Recovery Time)
CBF-01	4 Hours	1 Hour
CBF-02	4 Hours	1 Hour
CBF-03	2 Hours	30 Minutes
CBF-04	2 Hours	30 Minutes
CBF-05	24 Hour	12 hours
CBF-06	1 Hour	15 Minutes
CBF-07	24 Hours	12 Hours
CBF-08	8 Hour	4 hours



Resource Dependency Mapping



CBF ID	MAO (Hours/Minutes)	Impact Details (Financial, Legal, Patient Safety)
CBF-01	4 Hours	Revenue loss, reputational damage, delays in patient treatment.
CBF-02	4 Hours	Revenue loss, customer dissatisfaction, billing interruptions
CBF-03	2 Hours	All functions impacted
CBF-04	2 Hours	Compliance violations, not able to recover system or data, prolonged downtime.
CBF-05	24 Hour	Delayed payroll, employee dissatisfaction
CBF-06	1 Hour	Customer dissatisfaction, business loss.
CBF-07	24 Hours	Inconvenience for patients
CBF-08	8 Hour	Interruptions in compliance related activities, regulatory complications.

Critical Resources Identified

- Application servers
- Databases
- VPN & network infrastructure
- Backup systems
- End-user devices
- Sensitive data repositories (PHI/PII)

Outcome

- Clear understanding of what must be restored first
- Reduced recovery ambiguity during incidents

Business Continuity Strategy

Continuity Approach

- Alternate data center / cloud recovery
- Hot-site or mirrored systems
- Secure VPN-based remote operations
- Interim operations for finance and compliance teams

Goal

- Maintain business services even during major disruptions

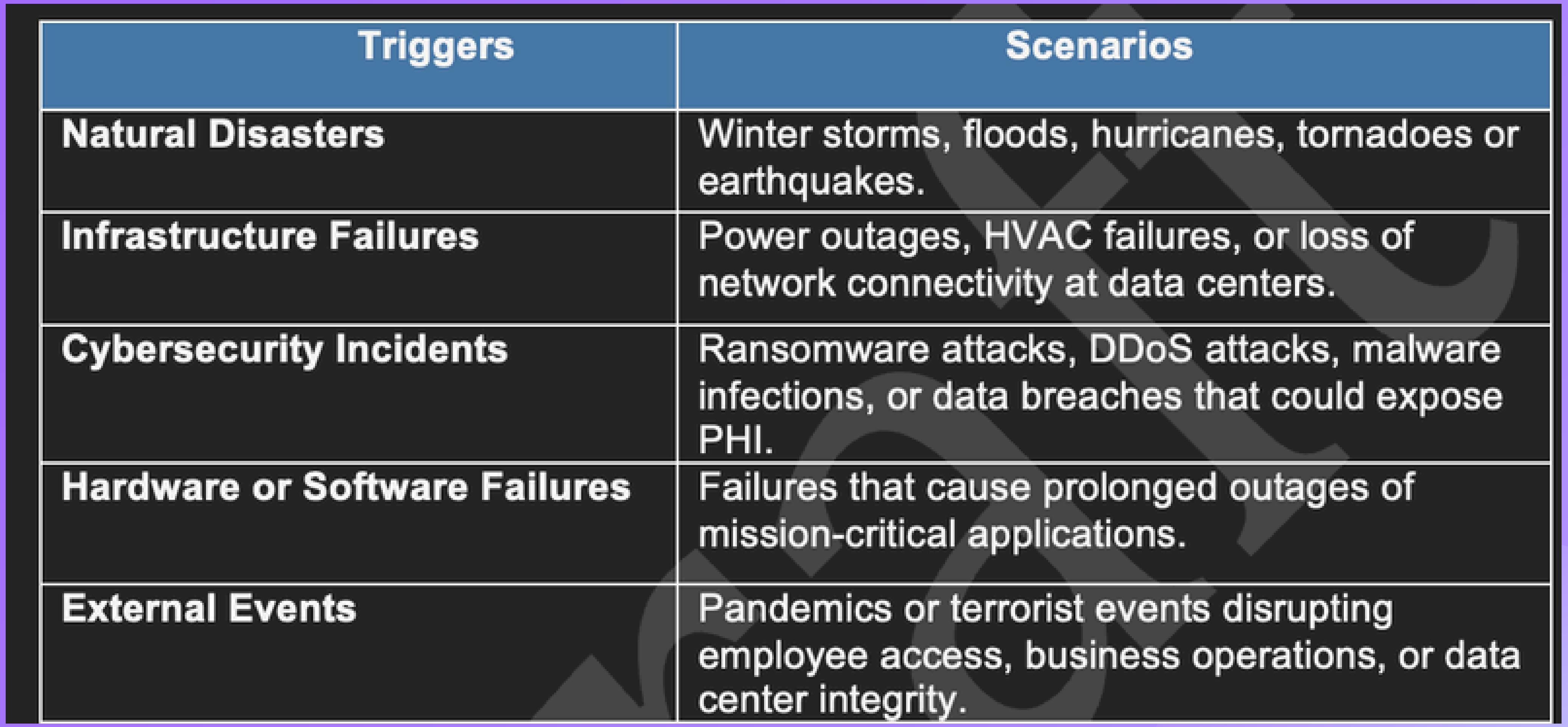
Incident Activation & Governance

Activation Triggers

- Cyberattacks (ransomware, data breach)
- Infrastructure failures
- Natural disasters
- External crises

Governance Model

- Defined incident commander
- Technical lead
- Compliance liaison
- Crisis communication team



Triggers	Scenarios
Natural Disasters	Winter storms, floods, hurricanes, tornadoes or earthquakes.
Infrastructure Failures	Power outages, HVAC failures, or loss of network connectivity at data centers.
Cybersecurity Incidents	Ransomware attacks, DDoS attacks, malware infections, or data breaches that could expose PHI.
Hardware or Software Failures	Failures that cause prolonged outages of mission-critical applications.
External Events	Pandemics or terrorist events disrupting employee access, business operations, or data center integrity.

Recovery Procedures (High Level)

Recovery Areas

- Data recovery (backups & integrity validation)
- System recovery (applications & servers)
- Network recovery (VPN, firewalls, DNS)

Security & Privacy Focus

- Encryption
- Secure access
- Validation before production cutover

Testing & Continuous Improvement

Testing Methods

- Desk check reviews
- Tabletop exercises
- Weekly simulations
- Annual full-scale drills

Why This Matters

- Ensures plan works in real life
- Builds staff confidence
- Meets regulatory expectations

Key Skills Demonstrated

This Project Demonstrates

- Privacy & compliance thinking
- Business risk analysis
- Documentation & governance
- Regulatory awareness
- Cross-functional communication
- Business-focused security planning

Why This Project Matters to Employers

- Shows real-world privacy & compliance capability
- Demonstrates business-aligned security thinking
- Applicable across healthcare, finance, and consulting roles

Use Case

- Resume attachment
- Portfolio showcase
- Interview discussion artifact

By Jacinta Izundu

Thank You Very Much

clemsjacy@gmail.com

+1 217 670 4436

http://linkedin.com/i n/jacinta-izundu-b36a2023