

# CVEQ Resilience Scorecards Guidebook



**CVEQ™**

**Cybercare** 

Simple • Effective • Affordable



## **CVEQ Resilience Scorecards Guidebook**

*From System Assurance to Decision Assurance: Measuring Resilience in the AI Age*

**"Resilience is the new currency of trust."**



© 2025 Serianu Limited. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission from Serianu Limited.

This guidebook has been developed under the Cybercare® and CVEQ® frameworks.

For inquiries:

**Serianu Limited**

[www.serianu.com](http://www.serianu.com) | [info@serianu.com](mailto:info@serianu.com)

# Table of Contents

Foreword	1
The Changing Technology Landscape	3
The Evolution of Assurance	6
The Six CVEQ Indicators	9
The Four Loss Scenario Categories	12
The 24 Loss Scenario Events	15
The 20 Control Design Capabilities (CDC)	18
The 25 Threat Detection Capabilities (TDC)	21
How to Interpret the Scorecards	24
Using the Scorecards Across Stakeholders	27
Sample CDC and TDC Scorecards	30
The Future of Resilience Measurement	33
Annexures	36





---

# Chapter 1: Foreword

The digital economy has reached a decisive moment. Technology no longer just processes data or runs systems — it now powers the decisions that drive financial markets, healthcare outcomes, government services, and customer experiences.

With this shift comes a new challenge: ensuring those decisions remain trustworthy, resilient, and explainable, even when disruption strikes.

Past assurance models no longer suffice:

- **System Assurance** → Was the server patched?
- **Digital Assurance** → Is the ecosystem reliable?
- **Decision Assurance** → Can we trust the outcomes themselves?

This is the context in which the CVEQ Resilience Scorecards are being launched.

They represent a new language of resilience — bridging technical operations and non-technical oversight, aligning both to a single truth:

Resilience is the new currency of trust.





---

## Chapter 2: The Changing Technology Landscape

Technology has always shaped how organizations create value — and how they build trust. To understand the need for resilience scorecards, we must trace how the use of technology has evolved, and how each stage shifted the definition of assurance.

## 2.1 The Data Era – Human-Centered Trust

- **Flow:** Data → Human Analysis → Decision → Outcome.
- Decisions were made by managers and leaders using reports, spreadsheets, and judgment.
- **Assurance focus:** Trust resided in the individual's ethics, competence, and accountability.

## 2.2 The System Era – Trust in IT Systems

- **Flow:** Data → Standalone System → Human Oversight → Decision → Outcome.
- As organizations automated business processes, trust shifted from people to systems.
- **Assurance focus:** *System assurance* — confirming that IT systems were patched, configured securely, and free of known flaws.
- **Limitation:** Assurance was **siloed**. Each system could be secure in isolation, but organizations lacked visibility across the bigger picture.

## 2.3 The Digital Era – Trust Across Networks

- **Flow:** Data → Interconnected Systems → Human Oversight → Decision → Outcome.
- With cloud computing, APIs, and third-party integrations, trust had to extend beyond individual systems.
- **Assurance focus:** *Digital assurance* — ensuring data remained accurate, available, and secure across distributed ecosystems.

- **Limitation:** Organizations could monitor flows and compliance, but not the **integrity of the decisions** those flows enabled.

## 2.4 The Analytics Era – Trust in AI-Augmented Decisions

- **Flow:** Data → Systems + AI Models → Human Oversight → Decision → Outcome.
- Machine learning models began influencing key decisions: credit scoring, fraud detection, customer targeting.
- **Assurance focus:** Ensuring AI outputs were explainable, unbiased, and effective.
- **Limitation:** Oversight lagged behind adoption. Many organizations lacked consistent metrics to prove AI trustworthiness.

## 2.5 The Autonomous AI Era – Trust in Decisions Themselves

- **Flow:** Data → Systems + Autonomous AI → Limited Human Oversight → Decision → Outcome.
- Today, AI models often make decisions directly: approving transactions, routing logistics, diagnosing conditions.
- **Assurance focus:** *Decision assurance* — proving that decisions are reliable, resilient, and fair, even under stress.
- **Implication:** Failures now stem not just from weak systems, but from compromised decision logic itself (e.g., bias, manipulation, outages, mistrust).



## 2.6 Why This Evolution Matters

Each era expanded the surface of trust:

- From **people** → **systems** → **networks** → **models** → **decisions**.
- Each stage brought new opportunities — and new risks.
- With each shift, assurance had to evolve.

- This is where the **CVEQ Resilience Scorecards** fit in: they provide a practical way to measure whether organizations can not only secure systems and data, but also ensure that **decisions themselves remain resilient in the face of disruption**.





## Chapter 3: The Evolution of Assurance

As technology has advanced, so too has the way organizations prove trust. What began as a focus on individual systems has grown into a mandate to assure entire decision ecosystems.

### 3.1 System Assurance – The IT-Centric Lens

- **Focus:** Are our IT systems secure, patched, and compliant?
- **Key activities:** Vulnerability scans, patching, system hardening.
- **Typical output:** Compliance checklists, audit certifications.
- **Limitation:** Assurance was siloed — proving a server was secure didn't mean the business process or decision it supported was resilient.

### 3.2 Digital Assurance – The Ecosystem Lens

- **Focus:** Is our digital ecosystem — spanning cloud platforms, partners, APIs, and networks — reliable, available, and compliant?
- **Key activities:** Data integrity checks, continuity planning, cross-platform monitoring.
- **Typical output:** Posture reports, SLA monitoring dashboards.
- **Limitation:** Assurance was still infrastructure-centric — it validated flows and uptime but not the integrity of decisions flowing through those digital channels.

### 3.3 Decision Assurance – The Future Lens

- **Focus:** Can we trust the decisions — human or AI-driven — that shape outcomes in finance, healthcare, government, and commerce?
- **Key activities:** Measuring resilience against fraud, bias, manipulation, outages, and mistrust.

- **Typical output: Resilience Scorecards** — simple grades (A–D) and percentages that reflect decision integrity.
- **Strength:** Decision assurance is **outcome-centric** — it validates not just systems or data, but the **trustworthiness of choices** made under disruption.

### 3.4 The Role of Indicators

Every era of assurance relied on **indicators** — measurable signals of trust.

- **System Assurance Indicators:** Patch status, vulnerability counts, audit results.
- **Digital Assurance Indicators:** Availability percentages, SLA adherence, data loss rates.
- **Decision Assurance Indicators (CVEQ):**
  1. **Profile Indicators** → define what matters most (critical processes, assets, and data).
  2. **Maturity Indicators** → show how structured and advanced the organization's risk and resilience programs are.
  3. **Visibility Indicators** → reveal whether blind spots exist across risks, controls, and exposures.
  4. **Exposure Indicators** → measure potential vulnerabilities and disruption scenarios.
  5. **Compliance Indicators** → confirm adherence to regulatory, contractual, and policy requirements.
  6. **Resilience Indicators** → quantify the ability to withstand financial, service, data, and trust loss scenarios.

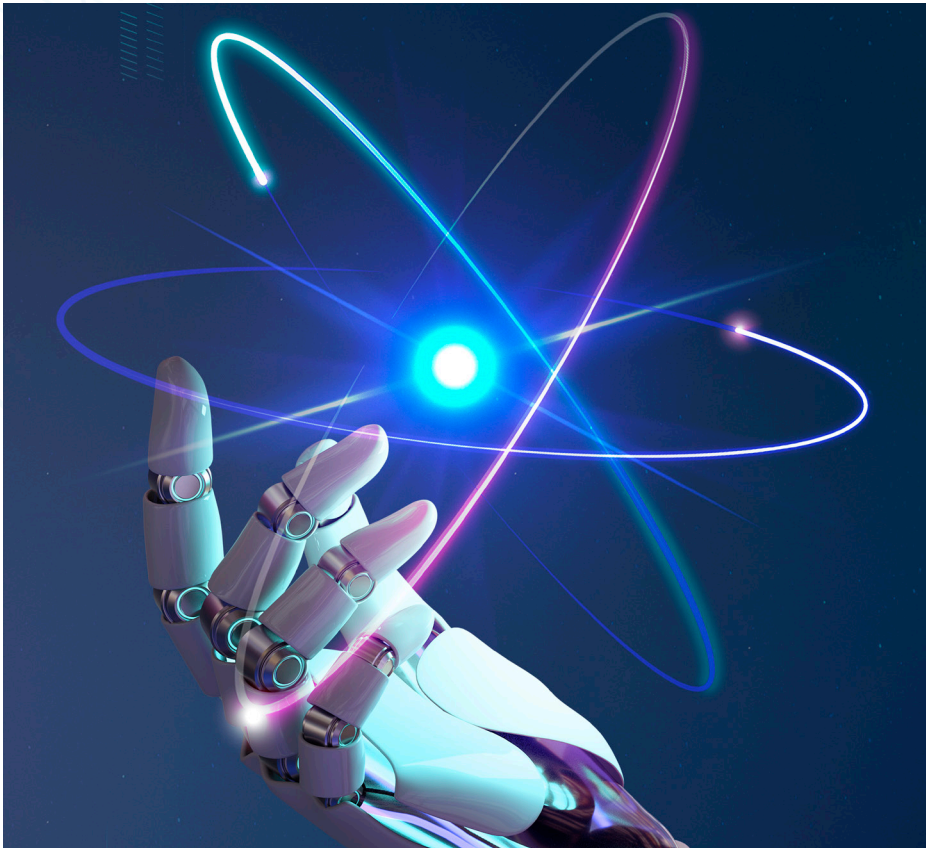
Together, these six indicators act as the health signals of the decision ecosystem — much like financial ratios act as health signals of corporate performance.

### 3.5 Why This Matters

Decision assurance is not a replacement for system or digital assurance — it is their logical progression.

- System assurance kept individual servers safe.
- Digital assurance kept networks and ecosystems reliable.
- Decision assurance ensures that outcomes remain resilient when disruption strikes.

- The **CVEQ Resilience Scorecards** embody this progression by giving organizations a unified way to measure resilience, benchmark performance, and communicate results across both technical and non-technical audiences.







## Chapter 4: The Six CVEQ Indicators

Decisions, whether made by humans or AI, must be trusted. To build and maintain that trust, organizations rely on indicators — measurable signals that reveal the health of the decision ecosystem.

Just as financial metrics (profit margin, liquidity ratio, debt-to-equity) give confidence in corporate performance, CVEQ indicators provide confidence in digital resilience.

## 4.1 Six Families of Indicators

The CVEQ Framework organizes indicators into six families:

- **Profile Indicators** – Define what matters most: critical processes, data, assets, and risks.
- **Maturity Indicators** – Show how structured and advanced the organization's governance and risk programs are.
- **Visibility Indicators** – Ensure there are no blind spots across systems, assets, controls, and exposures.
- **Exposure Indicators** – Show real-time exposure to vulnerabilities, incidents, and potential disruption scenarios.
- **Compliance Indicators** – Confirm whether obligations, regulations, and policies are being met.
- **Resilience Indicators** – Demonstrate the ability to withstand disruption across financial, service, data, and trust loss scenarios.

## 4.2 How Indicators Connect

- **Profile** tells us what matters most — the critical processes, data, assets, and risks.

- **Maturity** tells us whether governance and risk programs are structured and effective.
- **Visibility** tells us whether we can see across the full risk landscape without blind spots.
- **Exposure** tells us our real-time cyber-risk posture – vulnerabilities, threats and others.
- **Compliance** tells us whether obligations, regulations, and policies are being met.
- **Resilience** tells us whether we can withstand and recover from disruption.

## 4.3 Where Resilience Scorecards Fit

Resilience Scorecards sit within the Resilience Indicators family, but they are tightly linked to the other five. They:

- Quantify resilience across the four loss categories (Financial, Service, Data, Trust).
- Convert complex technical assessments (CDC & TDC scores) into a single percentage and grade (A–D).
- Provide a language that executives, regulators, and boards can understand, while remaining detailed enough for technical teams.

➤ Scorecards transform evidence into **insight**, bridging the gap between operational data and strategic oversight.

## 4.4 Example – Boardroom Perspective

When a board reviews indicators, they might see:

- **Profile:** Payments and customer data are identified as the most critical processes and assets.
- **Maturity:** Risk governance is structured but not yet optimized for advanced resilience.
- **Visibility:** Most third-party and internal risks are mapped, though some blind spots remain.
- **Exposure:** Real-time exposure shows data theft and fraud scenarios as high risk, with active vulnerabilities still unresolved.
- **Compliance:** Aligned with regulatory requirements, but lagging in ISO adoption and broader industry standards.

- **Resilience (via Scorecards):** Current resilience is **32% (C)** — indicating that disruption in data or service scenarios would cause significant business and reputational damage.

That single insight shifts the conversation from compliance checklists to decision readiness.

## 4.5 Why Indicators Matter in the AI Age

In the era of **autonomous AI**, indicators are no longer optional:

- They provide evidence that models, systems, and processes are fit for trust.
- They expose where AI-driven decisions may fail under stress (e.g., model manipulation, outages, mistrust).
- They allow regulators to benchmark resilience systemically across industries.

- Indicators are the **new language of assurance**. Resilience Scorecards are one of the most critical of these indicators — translating technical health signals into clear business insight.



## **Chapter 5: The Four Loss Scenario Categories**

At the heart of the CVEQ Resilience Scorecards are four universal categories of loss scenarios. No matter the industry, size, or geography of an organization, disruption ultimately manifests in one or more of these dimensions.



## 5.1 Financial Breach

- **Definition:** Direct loss of money or value through fraud, theft, or manipulation.
- **Example Scenario Events:**
  - » Payment fraud
  - » Card fraud
  - » Online fraud
  - » Email fraud
  - » Mobile fraud
  - » Model fraud
- **Why it matters:** Financial breaches strike at the core of organizational survival and directly impact profitability.

## 5.2 Service Breach

- **Definition:** Disruption to critical services or operations.
- **Example Scenario Events:**
  - » Third-party outages
  - » System downtime
  - » Network failures
  - » Website crashes
  - » Application failures
  - » Model outages
- **Why it matters:** Service breaches erode customer confidence and can cripple operations, sometimes with cascading effects across sectors.

## 5.3 Data Breach

- **Definition:** Compromise of data confidentiality, integrity, or availability.

### ➤ Example Scenario Events:

- » Data theft
- » PII breaches
- » Unauthorized disclosure
- » Malicious encryption (e.g., ransomware)
- » Data manipulation
- » Model manipulation

- **Why it matters:** Data breaches undermine compliance, privacy, and trust, and often attract regulatory fines.

## 5.4 Trust Breach

- **Definition:** Loss of stakeholder confidence in the organization's ability to operate reliably and ethically.
- **Example Scenario Events:**
  - » Regulatory violations
  - » Contractual breaches
  - » Policy violations
  - » Model mistrust
  - » Online defacement
  - » Brand abuse
- **Why it matters:** Trust breaches cut deeper than immediate financial or service losses. They can trigger regulatory penalties, reputational damage, and long-term erosion of customer relationships.

➤ These **Loss Scenario Categories** are the foundation for the **24 Loss Scenario Events** detailed in the next chapter. They ensure resilience measurement covers not just technical failures, but the full spectrum of outcomes that matter to business survival and trust.





## Chapter 6: The 24 Loss Scenario Events

The CVEQ Framework translates the four universal Loss Scenario Categories into 24 specific scenario events. These scenarios form the columns of the Resilience Scorecards and represent the real-world disruptions every organization must prepare for.

## 6.1 Financial Breach Scenarios

1. **Payment Fraud** – Unauthorized manipulation of payment processes to divert funds.
2. **Online Fraud** – Exploitation of online platforms or digital identities for fraudulent gain.
3. **Email Fraud** – Business Email Compromise (BEC) or phishing-driven financial loss.
4. **Mobile Fraud** – Fraud through SIM swaps, mobile app exploits, or OTP interception.
5. **Card Fraud** – Skimming, cloning, or unauthorized use of debit/credit cards.
6. **Model Fraud** – Manipulation of AI/ML models to approve or trigger fraudulent transactions. Unlike traditional fraud, this stems directly from tampering with autonomous model logic.

## 6.2 Service Breach Scenarios

7. **Third-Party Outage** – Disruption caused by downtime or failure of a critical vendor or service provider.
8. **System Outage** – Failure of internal IT systems disrupting operations.
9. **Network Outage** – Internet or connectivity disruption affecting services.
10. **Website Outage** – Public-facing websites or portals going offline.
11. **Application Outage** – Downtime of critical business applications.
12. **Model Outage** – Disruption of AI/ML models causing decision failures.

## 6.3 Data Breach Scenarios

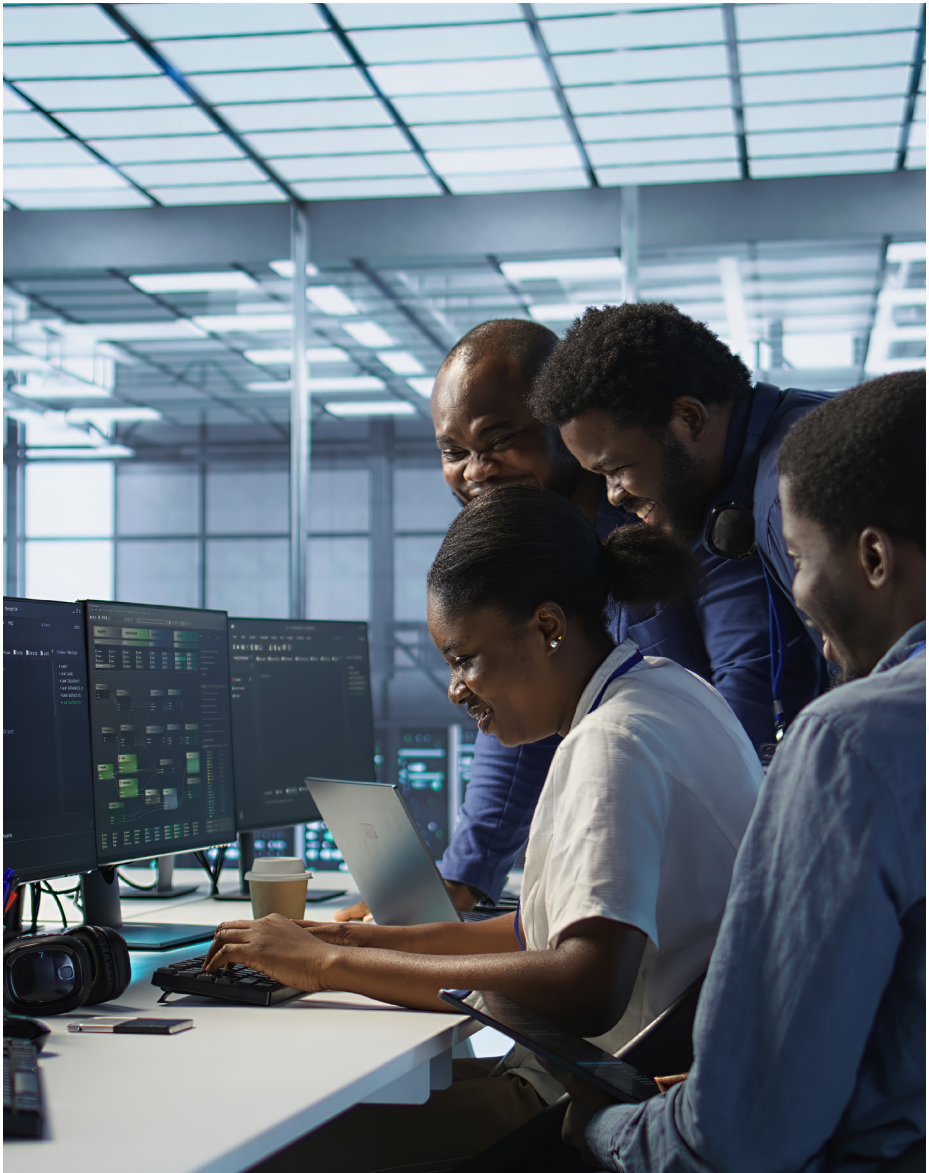
13. **Data Theft** – Unauthorized exfiltration of confidential or sensitive data.
14. **PII Breach** – Unauthorized exposure of personally identifiable information.
15. **Data Disclosure** – Leakage or unauthorized publication of protected information.
16. **Data Encryption** – Malicious encryption of data (e.g., ransomware).
17. **Data Manipulation** – Unauthorized alteration of data records.
18. **Model Manipulation** – Corruption of AI/ML training data or model parameters to bias outcomes.

## 6.4 Trust Breach Scenarios

19. **Regulatory Violation** – Breach of compliance with legal or regulatory requirements.
20. **Contractual Violation** – Failure to meet contractual or SLA obligations.
21. **Policy Violation** – Breach of internal organizational policies.
22. **Model Mistrust** – Decline in stakeholder confidence in AI-driven decisions due to bias, opacity, or explainability gaps.
23. **Online Defacement** – Unauthorized modification of public-facing websites or platforms.
24. **Brand Abuse** – Misuse, impersonation, or phishing campaigns targeting the brand's reputation.



- These **24 scenario events** define the disruption universe against which resilience is measured. They provide a structured way to model exposures across financial, service, data, and trust dimensions — ensuring no blind spots in resilience measurement.





## Chapter 7: The 20 Control Design Capabilities (CDC)

The CVEQ Framework defines 20 Control Design Capabilities (CDCs). These capabilities represent the essential building blocks of organizational resilience. They ensure that controls are designed, documented, and embedded into the organization's governance, technology, and processes.

The CDCs are grouped into five categories: Oversight, Asset, User, Incident, and Continuity.

## 7.1 Oversight CDCs (1-7)

1. **Data Assessment** – Identifying, classifying, and prioritizing critical data assets based on sensitivity and business value.
2. **Risk Assessment** – Evaluating risks across business processes, data, and loss scenarios to inform decision-making.
3. **Risk Governance** – Establishing accountability, oversight structures, and decision rights for managing risks.
4. **Risk Reporting** – Communicating risks and resilience levels to leadership, regulators, and stakeholders.
5. **Policy Management** – Defining, approving, and enforcing organizational policies to guide behavior and control use.
6. **Control Management** – Documenting, monitoring, and validating that controls are implemented and functioning effectively.
7. **Third-Party Management** – Assessing, monitoring, and mitigating risks arising from vendors, partners, and service providers.

## 7.2 Asset CDCs (8-12)

8. **Asset Inventory** – Maintaining a comprehensive register of IT, OT, and digital assets across the enterprise.
9. **Malware Defences** – Designing layered defences to prevent, detect, and block malicious software.
10. **Vulnerability Patching** – Ensuring timely remediation of known weaknesses through structured patching processes.

11. **Network Security** – Designing secure networks, including segmentation, monitoring, and perimeter defences.

12. **Data Protection** – Safeguarding data confidentiality, integrity, and availability through encryption, masking, and access controls.

## 7.3 User CDCs (13-15)

13. **User Access Controls** – Enforcing authentication, authorization, and least-privilege principles for all user accounts.
14. **Privilege Access Controls** – Governing administrative and elevated accounts to prevent misuse or compromise.
15. **User Awareness** – Designing training programs and awareness campaigns to equip users to recognize and resist threats.

## 7.4 Incident CDCs (16-18)

16. **Threat Monitoring** – Establishing monitoring mechanisms to detect anomalies, intrusions, or signs of compromise.
17. **Incident Response** – Building structured response capabilities, including playbooks, teams, and escalation paths.
18. **Transaction Monitoring** – Detecting anomalies in financial and business transactions that may indicate fraud or manipulation.

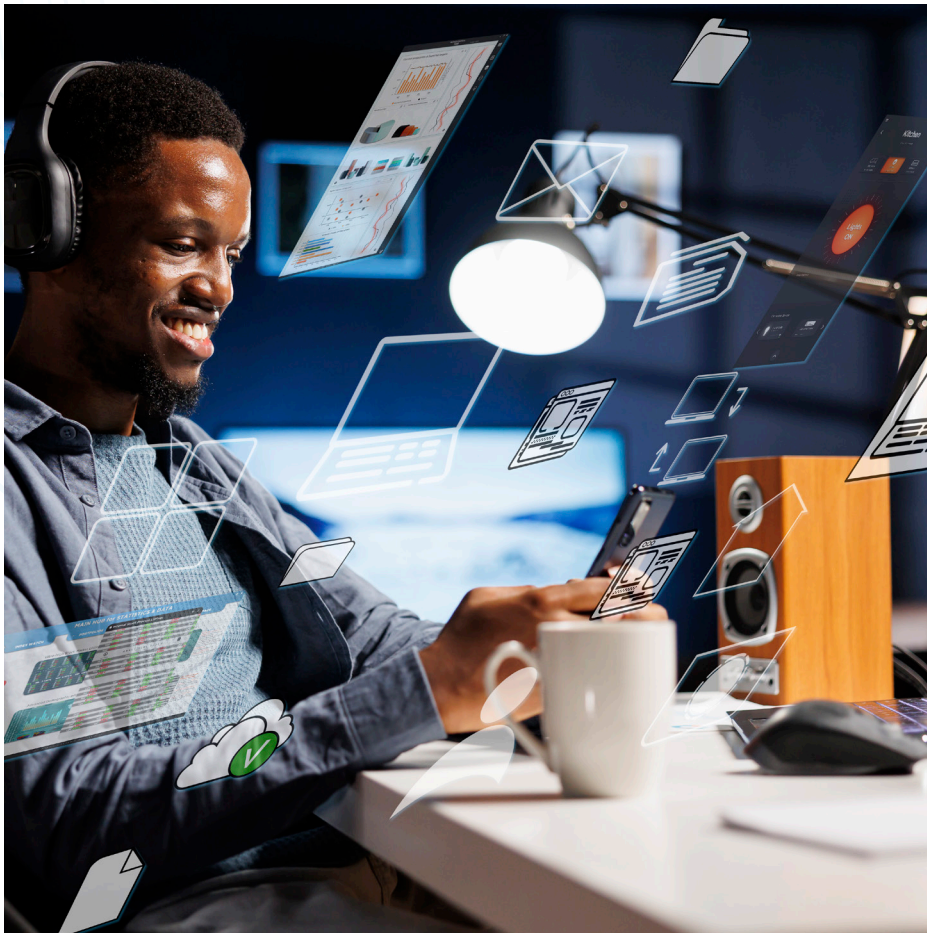


## 7.5 Continuity CDCs (19–20)

**19. Data Recovery** – Designing and testing processes to restore lost or corrupted data within acceptable timelines.

**20. Service Availability** – Embedding resilience, redundancy, and failover into critical services to ensure continuity.

➤ Together, these **20 Control Design Capabilities** represent the foundation of the **CDC Resilience Scorecards**. They allow organizations to measure the strength of their **control design layer**, linking governance, assets, users, incidents, and continuity to resilience outcomes.





## Chapter 8: The 25 Threat Detection Capabilities (TDC)

The CVEQ Framework defines **25 Threat Detection Capabilities (TDCs)**. These capabilities measure how well an organization can identify, detect, and respond to threats in real time.

They represent the **operational detection layer** of resilience and are grouped into **four categories**: Asset, User, Incident, and Continuity.



## 8.1 Asset TDCs (1–7)

- 1. Hardware Asset Integrity**  
– Validating that devices are genuine, uncompromised, and properly monitored.
- 2. Software Inventory Integrity**  
– Ensuring all installed software is legitimate, authorized, and up to date.
- 3. Malware Presence** – Detecting malicious software activity across systems, endpoints, and networks.
- 4. Files and Services Abuse**  
– Monitoring for misuse or suspicious activity within files, processes, or services.
- 5. Vulnerabilities and Exploits** – Detecting attempts to exploit known or unknown weaknesses.
- 6. Configuration Integrity** – Identifying unauthorized or risky configuration changes across systems.
- 7. Sensitive Data Integrity** – Detecting unauthorized access, modification, or movement of sensitive or critical data.

## 8.2 User TDCs (8–13)

- 8. User Account Integrity** – Identifying abnormal account creation, privilege escalation, or misuse.
- 9. User Access Activity** – Monitoring unusual or suspicious user activity patterns.
- 10. Privilege Account Integrity**  
– Detecting compromise or misuse of privileged accounts.
- 11. Privilege Access Activity**  
– Tracking and analyzing privileged user actions for risky behavior.

## 12. Social Engineering Attack –

Detecting phishing, vishing, and other attempts to exploit human behavior.

## 13. User Awareness Training

– Measuring user readiness through phishing simulations, tests, and awareness campaigns.

## 8.3 Incident TDCs (14–19)

### 14. Incident Detection Capability

– Ability to recognize incidents early, triage, and escalate effectively.

### 15. Incident Resolution Capability

– Ability to contain and remediate incidents quickly and efficiently.

### 16. Transactional Data Integrity

– Detecting tampering or corruption of financial or operational transaction data.

### 17. Transaction Anomaly

**Detection** – Identifying unusual transaction patterns that may signal fraud or manipulation.

### 18. Network Time Integrity

– Ensuring system clocks and timestamps remain synchronized and uncompromised.

### 19. Log Data Integrity

– Detecting tampering, deletion, or gaps in logs that support investigations and compliance.

## 8.4 Continuity TDCs (20–25)

### 20. System Performance –

Monitoring for anomalies in system health, capacity, or performance degradation.

### 21. System Availability

– Detecting service disruptions, outages, or downtime.

**22. Data Backup Capability**

– Ensuring backups are completed, validated, and available for restoration.

**23. Data Restoration Capability**

– Verifying that backups can be restored successfully within required timelines.

**24. Offline Backup Capability –**

Ensuring critical backups exist in offline, immutable storage to protect against ransomware.

**25. Threat Intelligence Capability**

– Leveraging internal and external intelligence sources to detect and anticipate emerging threats.

➤ These **25 Threat Detection Capabilities** underpin the **TDC Resilience Scorecards**. They measure an organization's **detection strength** against the 24 loss scenario events, highlighting blind spots and operational weaknesses that could undermine resilience.





## Chapter 9: How to Interpret the Scorecards

Resilience Scorecards translate complex technical assessments into simple, comparable outputs. They serve as a bridge between technical operations teams and non-technical oversight stakeholders such as executives, boards, and regulators.

This chapter explains how to read and interpret the scorecards, including percentage scores, letter grades, capability variances, and resilience trends.

## 9.1 Scorecard Components

Each scorecard includes:

- **Organization Name and Date** – To contextualize results.
- **CVEQ Domain** – Either Risk Reduction (CDC) or Threat Detection (TDC).
- **Resilience Score** – Percentage score across all loss scenarios.
- **Overall Rating** – Letter grade (A–D, with “+” or “–”) derived from the score.
- **Loss Scenario Categories** – Financial, Service, Data, and Trust breaches.
- **Loss Scenario Events** – The 24 scenario events across categories.
- **Capabilities** – Either 20 CDCs or 25 TDCs, depending on the scorecard.

- **Current vs. Optimal Levels** – Showing actual performance against benchmark expectations.

## 9.2 Scoring Methodology

- **Resilience Score (%)**: Reflects the organization’s aggregate resilience across all loss scenarios.
- **Overall Rating (A–D)**: A grade derived from the resilience percentage using the standard CVEQ grading scale.
- **Capability Scores**: Each CDC or TDC is assigned a performance percentage, reflecting its effectiveness against loss scenarios.
- **Variance Levels**: Gap between current resilience and optimal resilience, expressed in percentage points.

## 9.3 Grading Scale


The grading scale is consistent across CDC and TDC scorecards:



Resilience Percentage	Grade	Interpretation
91–100%	<b>A (Very High Resilience)</b>	Organization is fully resilient; negligible gaps remain.
76–90%	<b>A- (High Resilience)</b>	Strong resilience posture; only minor improvements needed.
61–75%	<b>B (Medium-High Resilience)</b>	Above-average resilience; targeted gaps must be closed.
46–60%	<b>B- (Medium Resilience)</b>	Acceptable but fragile resilience; multiple weaknesses exist.
31–45%	<b>C (Medium-Low Resilience)</b>	Below average resilience; organization at risk in high-severity scenarios.
16–30%	<b>C- (Low Resilience)</b>	Weak resilience posture; significant vulnerabilities present.
0–15%	<b>D (Very Low Resilience)</b>	Critically low resilience; urgent remediation is required.

## 9.4 Reading the Scorecards

1. **Start with the Overall Rating:** Provides a quick benchmark of resilience maturity.
2. **Examine Loss Categories:** See whether gaps are concentrated in Financial, Service, Data, or Trust scenarios.
3. **Review Individual Capabilities:** Identify which CDCs or TDCs are underperforming.
4. **Check Variance:** Focus on the largest gaps between current and optimal resilience.
5. **Prioritize Actions:** Use results to drive remediation planning and resource allocation.

## 9.5 Example Interpretations

-  **Case A – Low Resilience (32%, Grade C-):**  
The bank has a weak resilience posture, underperforming particularly in Service Breach scenarios. Large gaps in incident response and system availability expose it to disruption.

-  **Case B – Medium Resilience (51%, Grade B-):**  
The telco shows acceptable but fragile resilience. Strong user controls and detection are offset by weaknesses in data recovery and third-party oversight.
-  **Case C – High Resilience (80%, Grade A-):**  
The insurer has invested heavily in both CDCs and TDCs, achieving strong resilience across Financial and Data categories. Minor continuity gaps remain but the organization is generally well-prepared.

## 9.6 Why Interpretation Matters

Scorecards are not just technical dashboards — they are decision tools:

- **For executives:** They simplify complex resilience into an accessible benchmark.
- **For risk teams:** They highlight specific control and detection gaps.
- **For regulators:** They provide a consistent way to benchmark resilience across organizations.
- **For AI governance:** They explicitly capture model-related risks (fraud, outages, manipulation, mistrust).

- Interpretation transforms scorecards from measurement instruments into **strategic enablers** for cyber risk management and decision assurance.





# Chapter 10: Using the Scorecards Across Stakeholders

CVEQ Resilience Scorecards are designed to be meaningful not only to cyber and risk teams, but also to **executives, boards, regulators, and AI governance groups**. This chapter highlights how each group can interpret and apply the scorecards in their role.

## 10.1 Boards and Executives

- » **Objective:** To make informed investment and governance decisions.
- » **Use of Scorecards:**
  - » Review the overall resilience grade (A–D) as a benchmark.
  - » Understand where loss categories (Financial, Service, Data, Trust) are most vulnerable.
  - » Align resilience targets with business strategy and appetite for risk.
- » **Value:** Provides a clear, comparable metric to prioritize where to invest in resilience.

## 10.2 Cyber and Risk Teams

- » **Objective:** To diagnose and remediate technical and operational weaknesses.
- » **Use of Scorecards:**
  - » Analyze CDC and TDC capability scores to identify weak points.
  - » Map variance levels to remediation plans.
  - » Monitor resilience trends over time to validate improvements.
- » **Value:** Provides a structured way to link technical controls with real-world loss scenarios.

## 10.3 Regulators and Supervisors

- » **Objective:** To ensure systemic resilience across industries and sectors.
- » **Use of Scorecards:**
  - » Benchmark organizations in a sector or region against consistent resilience criteria.

- » Identify systemic weaknesses (e.g., third-party dependence, data breaches).
- » Use as evidence of resilience **beyond compliance checklists.**

- » **Value:** Provides a sector-wide resilience snapshot, enabling regulators to track improvements and emerging risks.

## 10.4 AI Governance and Model Risk Teams

- » **Objective:** To manage risks from AI models and autonomous decision-making.
- » **Use of Scorecards:**
  - » Focus on model-related loss scenarios (Model Fraud, Model Outage, Model Manipulation, Model Mistrust).
  - » Validate whether detection and control capabilities adequately address AI-driven risks.
  - » Use resilience metrics to build trust in AI decisions among stakeholders.
- » **Value:** Scorecards integrate AI-specific risks into the broader resilience framework, ensuring model governance is not isolated.

## 10.5 Sectoral and Industry Bodies

- » **Objective:** To promote resilience standards and best practices across industries.
- » **Use of Scorecards:**
  - » Compare member organizations' resilience maturity.
  - » Develop sectoral benchmarks and guidance.

- » Highlight industry-level resilience trends and gaps.
- » **Value:** Provides a standardized resilience language to foster collaboration and industry-wide progress.
- » By tailoring outputs to these diverse audiences, Resilience Scorecards ensure that resilience measurement is **not just technical** but **strategic, systemic, and sectoral**.







# Chapter 11: Sample CDC and TDC Scorecards

To help organizations understand how to apply CVEQ Resilience Scorecards, this chapter provides sample scorecards for both Control Design Capabilities (CDC) and Threat Detection Capabilities (TDC). These are illustrative examples based on anonymized organizations.

## 11.1 Sample CDC Loss Scenario Scorecard

**Organization Name:** Mega Africa

**CVEQ Domain:** Risk Reduction – Control Design

**Date:** As at August 2025

**Resilience Score:** 51%

**Overall Rating:** B-

Capability Category	Example CDCs	Current Resilience	Optimal Level	Variance
Oversight (1–7)	Data Assessment, Risk Governance, Policy Management	48–70%	100%	-30 to -52%
Asset (8–12)	Asset Inventory, Malware Defences, Network Security	41–78%	100%	-22 to -59%
User (13–15)	User Access Controls, Privilege Access Controls, User Awareness	44–48%	100%	-52 to -56%
Incident (16–18)	Threat Monitoring, Incident Response, Transaction Monitoring	33–77%	100%	-23 to -67%
Continuity (19–20)	Data Recovery, Service Availability	15–59%	100%	-41 to -85%

### Interpretation:

- Strong performance in Policy Management and Incident Response.
- Weaknesses in Service Availability and Third-Party Management drag overall resilience down.
- Recommended focus: strengthening continuity and oversight to close systemic gaps.

## 11.2 Sample TDC Loss Scenario Scorecard

**Organization Name:** Mega Africa

**CVEQ Domain:** Threat Detection – Threat Detection Capabilities

**Date:** As at 31-August-2025

**Resilience Score:** 32%

**Overall Rating:** C



Capability Category	Example TDCs	Current Resilience	Optimal Level	Variance
Asset (1–7)	Hardware Asset Integrity, Vulnerabilities & Exploits, Sensitive Data Integrity	22–44%	100%	-56 to -78%
User (8–13)	User Access Activity, Privilege Account Integrity, Social Engineering Attack	10–66%	100%	-34 to -90%
Incident (14–19)	Incident Detection, Resolution, Transaction Anomaly Detection, Log Integrity	23–55%	100%	-45 to -77%
Continuity (20–25)	System Availability, Data Restoration, Threat Intelligence	12–54%	100%	-46 to -88%

### Interpretation:

- Critical weaknesses in User Account Integrity and Continuity Capabilities (offline backups, restoration).
- Transaction Anomaly Detection is underperforming despite its importance in fraud prevention.
- Recommended focus: strengthening detection depth in user behavior monitoring and data continuity.

## 11.3 What These Examples Show

- CDC Scorecards highlight whether control design is robust enough to withstand disruption.
- TDC Scorecards reveal whether threats are being actively detected and responded to in real time.
- Taken together, they provide a complete resilience picture — spanning both prevention (CDC) and detection (TDC).



## Chapter 12: The Future of Resilience Measurement

The launch of the CVEQ Resilience Scorecards marks a major milestone in the evolution of cyber risk and resilience management. Yet, this is only the beginning. The future will bring new challenges, new expectations, and new ways of measuring resilience.

## 12.1 From Technical to Strategic

- **Yesterday:** Measurement focused on whether systems were patched and compliant.
- **Today:** Resilience is measured across loss scenarios that matter to business survival and trust.
- **Tomorrow:** Scorecards will evolve into strategic tools for shaping investment, regulation, and decision assurance at the highest levels of organizations.

## 12.2 Integration with Decision Assurance

As organizations shift into the **autonomous AI era**, resilience measurement must adapt:

- AI models introduce new loss scenarios (Model Fraud, Model Manipulation, Model Outage, Model Mistrust).
- Resilience indicators must capture not just system health, but decision integrity.
- Scorecards will become central to decision assurance, offering evidence that AI-driven choices are fair, explainable, and resilient.

## 12.3 Sector and Ecosystem Resilience

- Regulators and industry bodies will increasingly use scorecards to measure systemic resilience across industries.
- Sector-wide resilience reporting will allow governments and regulators to spot common weaknesses (e.g., overreliance on third parties).

- Cross-sector benchmarking will establish minimum resilience thresholds, just as financial ratios do in capital adequacy.

## 12.4 Real-Time Resilience Dashboards

The future of resilience is not static scorecards but dynamic dashboards:

- Continuous monitoring of CDC and TDC performance.
- Automated updates to resilience scores as controls are implemented or threats evolve.
- Integration with threat intelligence feeds and incident data to maintain real-time visibility.

## 12.5 Expanding Beyond Cybersecurity

Resilience scorecards will expand into other domains of risk:

- **Operational Resilience** – ensuring services withstand natural disasters, geopolitical instability, and supply chain shocks.
- **Digital Trust** – integrating privacy, ethics, and AI explainability into resilience metrics.
- **Sustainability and ESG** – aligning resilience with environmental, social, and governance priorities.

## 12.6 Why This Matters

The future of resilience measurement will redefine how organizations communicate trust:

- Boards and executives will expect resilience scores alongside financial metrics.

- Regulators will mandate sectoral reporting of resilience levels.
  - Customers, investors, and partners will see resilience as a precondition for trust.
- CVEQ Resilience Scorecards are not the end state — they are the **foundation for a new era of resilience measurement**, one that aligns technology, risk, and trust in the age of autonomous AI.





## Annex A: Glossary of Key Terms

- **Assurance** – Confidence that systems, processes, and decisions maintain integrity and reliability.
- **Decision Assurance** – Trust that AI-enabled and human decisions are reliable, explainable, and fair.
- **CVEQ Framework** – Cyber-risk Visibility & Exposure Quantification framework underpinning Cybercare.
- **Resilience** – The ability to withstand, adapt to, and recover from disruption.
- **Loss Scenario Event** – A specific disruption (e.g., fraud, outage, breach) modeled under CVEQ.
- **Control Design Capabilities (CDC)** – The 20 foundational controls that ensure risk prevention and governance.
- **Threat Detection Capabilities (TDC)** – The 25 detection and response capabilities that ensure threat visibility.
- **Resilience Scorecard** – A standardized output translating technical evidence into resilience percentages and letter grades.

## Annex B: Loss Scenario Events

The **24 Loss Scenario Events** grouped under four categories:

- **Financial Breach:** Payment Fraud, Online Fraud, Email Fraud, Mobile Fraud, Card Fraud, Model Fraud.
- **Service Breach:** Third-Party Outage, System Outage, Network Outage, Website Outage, Application Outage, Model Outage.
- **Data Breach:** Data Theft, PII Breach, Data Disclosure, Data Encryption, Data Manipulation, Model Manipulation.
- **Trust Breach:** Regulatory Violation, Contractual Violation, Policy Violation, Model Mistrust, Online Defacement, Brand Abuse.

## Annex C: Control Design Capabilities (CDC)

Grouped into five categories:

- **Oversight (1–7):** Data Assessment, Risk Assessment, Risk Governance, Risk Reporting, Policy Management, Control Management, Third-Party Management.
- **Asset (8–12):** Asset Inventory, Malware Defences, Vulnerability Patching, Network Security, Data Protection.
- **User (13–15):** User Access Controls, Privilege Access Controls, User Awareness.

- **Incident (16–18):** Threat Monitoring, Incident Response, Transaction Monitoring.
- **Continuity (19–20):** Data Recovery, Service Availability.

## Annex D: Threat Detection Capabilities (TDC)

Grouped into four categories:

- **Asset (1–7):** Hardware Asset Integrity, Software Inventory Integrity, Malware Presence, Files & Services Abuse, Vulnerabilities & Exploits, Configuration Integrity, Sensitive Data Integrity.
- **User (8–13):** User Account Integrity, User Access Activity, Privilege Account Integrity, Privilege Access Activity, Social Engineering Attack, User Awareness Training.
- **Incident (14–19):** Incident Detection Capability, Incident Resolution Capability, Transactional Data Integrity, Transaction Anomaly Detection, Network Time Integrity, Log Data Integrity.
- **Continuity (20–25):** System Performance, System Availability, Data Backup Capability, Data Restoration Capability, Offline Backup Capability, Threat Intelligence Capability.

## Annex E: Sample Scorecards

CDC Example – Mega Africa (March 2024):

- Overall Resilience: **51% (B-)**
- Strengths: Policy Management, Incident Response.
- Weaknesses: Service Availability, Third-Party Management.

TDC Example – Mega Africa (August 2025):

- Overall Resilience: **32% (C)**
- Strengths: Malware Detection, Sensitive Data Integrity.
- Weaknesses: Transaction Anomaly Detection, Continuity Capabilities.

## Annex F: Grading Scale

The grading scale provides a standardized way to interpret resilience percentages across both CDC and TDC scorecards.

Resilience Percentage	Grade	Interpretation
91–100%	<b>A (Very High Resilience)</b>	Organization is fully resilient; negligible gaps remain.
76–90%	<b>A- (High Resilience)</b>	Strong resilience posture; only minor improvements needed.
61–75%	<b>B (Medium-High Resilience)</b>	Above-average resilience; targeted gaps must be closed.
46–60%	<b>B- (Medium Resilience)</b>	Acceptable but fragile resilience; multiple weaknesses exist.
31–45%	<b>C (Medium-Low Resilience)</b>	Below average resilience; organization at risk in high-severity scenarios.
16–30%	<b>C- (Low Resilience)</b>	Weak resilience posture; significant vulnerabilities present.
0–15%	<b>D (Very Low Resilience)</b>	Critically low resilience; urgent remediation is required.

## Annex G: Sample Resilience Report

This annex illustrates how resilience scores are broken down by category and scenario event, with control and detection capabilities driving the results.

### 1. CDC Resilience Snapshot – Mega Africa (As at 31-August-2025)

**Overall Resilience:** 51% (B-)

**Domain:** Risk Reduction – Control Design

Loss Scenario Category	Scenario Events	Event Scores	Strong CDC Capabilities	Weak CDC Capabilities
<b>Financial Breach (58%)</b>	Payment Fraud	61%	Transaction Monitoring	Risk Assessment
	Online Fraud	58%	Policy Management	User Awareness
	Email Fraud	55%	Data Protection	User Awareness
	Mobile Fraud	49%	Risk Governance	Control Management
	Card Fraud	54%	Privilege Access Controls	Risk Assessment
	Model Fraud	42%	Policy Management	Data Assessment

Loss Scenario Category	Scenario Events	Event Scores	Strong CDC Capabilities	Weak CDC Capabilities
<b>Service Breach (44%)</b>	Third-Party Outage	39%	Risk Reporting	Third-Party Management
	System Outage	42%	Incident Response	Service Availability
	Network Outage	46%	Network Security	Data Recovery
	Website Outage	44%	Malware Defences	Service Availability
	Application Outage	45%	Incident Response	Control Management
	Model Outage	41%	Policy Management	Asset Inventory
<b>Data Breach (52%)</b>	Data Theft	53%	Data Protection	Asset Inventory
	PII Breach	52%	Data Assessment	User Awareness
	Data Disclosure	50%	Risk Governance	Policy Management
	Data Encryption	48%	Data Protection	Data Recovery
	Data Manipulation	46%	Control Management	Transaction Monitoring
	Model Manipulation	44%	Policy Management	Risk Assessment
<b>Trust Breach (49%)</b>	Regulatory Violation	51%	Risk Reporting	Risk Governance
	Contractual Violation	49%	Policy Management	Third-Party Management
	Policy Violation	47%	Control Management	User Awareness
	Model Mistrust	45%	Risk Governance	Data Assessment
	Online Defacement	43%	Network Security	Malware Defences
	Brand Abuse	41%	Policy Management	User Awareness

### Interpretation:

- Financial breaches are partially controlled but model fraud remains a critical weak point.



- Service breaches highlight fragile continuity controls (Service Availability, Third-Party Management).
- Data breaches show structural weaknesses in Asset Inventory and Data Recovery.
- Trust breaches reveal governance and awareness gaps that threaten reputation and compliance.

## 2. TDC Resilience Snapshot – Mega Africa (As at 31-August-2025)

**Overall Resilience: 32% (C)**

**Domain: Threat Detection – Threat Detection Capabilities**

Loss Scenario Category	Scenario Events	Event Scores	Strong TDC Capabilities	Weak TDC Capabilities
<b>Financial Breach (35%)</b>	Payment Fraud	34%	Transactional Data Integrity	Transaction Anomaly Detection
	Online Fraud	33%	Malware Presence	User Account Integrity
	Email Fraud	36%	Social Engineering Detection	User Awareness Training
	Mobile Fraud	29%	Sensitive Data Integrity	Privilege Account Integrity
	Card Fraud	32%	Log Data Integrity	Transaction Anomaly Detection
	Model Fraud	28%	Threat Intelligence	Model-specific anomaly detection gaps
<b>Service Breach (28%)</b>	Third-Party Outage	26%	System Availability	Offline Backup Capability
	System Outage	30%	Incident Detection	System Performance
	Network Outage	27%	Network Time Integrity	Configuration Integrity
	Website Outage	25%	Threat Intelligence	System Availability
	Application Outage	29%	Incident Resolution	User Access Activity
	Model Outage	23%	Transactional Data Integrity	Privilege Access Activity

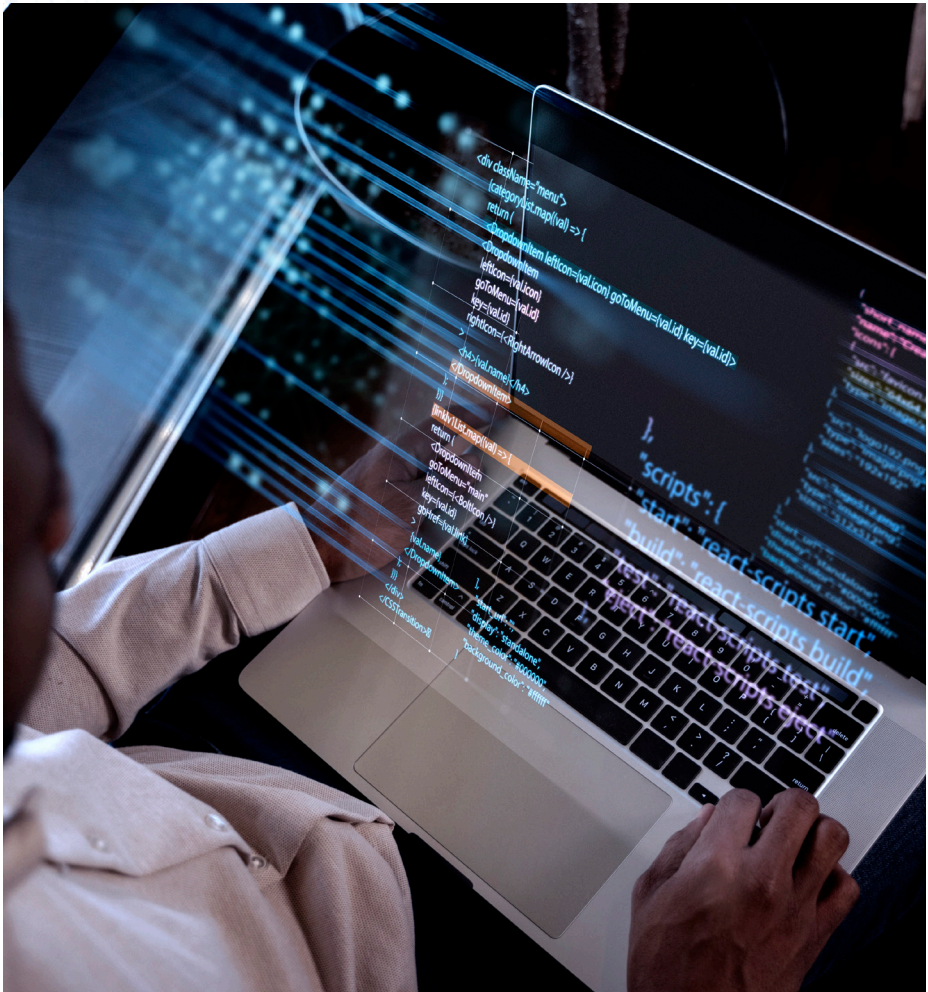
Loss Scenario Category	Scenario Events	Event Scores	Strong TDC Capabilities	Weak TDC Capabilities
<b>Data Breach (38%)</b>	Data Theft	39%	Sensitive Data Integrity	Log Data Integrity
	PII Breach	35%	User Awareness	User Account Integrity
	Data Disclosure	32%	Threat Intelligence	Configuration Integrity
	Data Encryption	31%	Malware Presence	Offline Backup Capability
	Data Manipulation	34%	Transaction Anomaly Detection	Sensitive Data Integrity
	Model Manipulation	27%	Threat Intelligence	User Access Monitoring
<b>Trust Breach (27%)</b>	Regulatory Violation	30%	Log Data Integrity	User Account Integrity
	Contractual Violation	28%	Threat Intelligence	Incident Resolution
	Policy Violation	29%	Social Engineering Detection	Privilege Account Integrity
	Model Mistrust	26%	Threat Intelligence	Sensitive Data Integrity
	Online Defacement	25%	Malware Detection	Network Monitoring
	Brand Abuse	23%	Threat Intelligence	User Awareness Training

### Interpretation:

- Financial breaches are especially vulnerable due to weak anomaly detection.
- Service breaches are the lowest scoring — outages, continuity, and performance issues dominate.
- Data breaches show some strength in Sensitive Data Integrity but weak log integrity and backup validation.
- Trust breaches show systemic failure in user monitoring and brand protection.

### 3. Key Lessons

- Breaking scores down by category and event shows where resilience gaps are concentrated.
- Boards and executives can see category averages (Financial, Service, Data, Trust).
- Risk and cyber teams can see event-level scores (e.g., Model Fraud = 28%), allowing them to target remediation directly.
- CDCs prevent disruption; TDCs detect and respond — resilience emerges when both layers reinforce each other.









## **Serianu Limited**

14 Chalbi Drive, Lavington,  
Nairobi, Kenya

### **Botswana Office:**

Plot 54349, Office Block B  
3rd Floor, CBD Gaborone



info@serianu.com



@serianultd



Africa Cyber Immersion Centre - ACIC



Serianu Limited



@africacyberimmersioncentre

[www.serianu.com](http://www.serianu.com)