SecureZaidi
CYBERSECURITY & COMPLIANCE

COMPLIANCE GUIDE 04 / 04

Cybersecurity Risk Assessment Guide: From Identification to Board Reporting

A practical guide to conducting structured cybersecurity risk assessments using NIST and ISO frameworks — including how to communicate risk to your board.

Produced by	SecureZaidi Limited
Website	securezaidi.com
Email	info@securezaidi.com
Phone	+254 700 000 000
Edition	2026 Edition — For East African Organisations

Contents

1. Why Risk Assessment Matters

Cybersecurity risk assessment is the structured process of identifying, analysing, and evaluating the information security risks facing your organisation — so that you can make informed decisions about where to invest in security controls and what level of residual risk is acceptable.

Without a risk assessment, security spending is driven by vendor sales pitches, compliance checklists, or the last incident rather than by a clear understanding of your actual threat landscape and risk priorities. Organisations that manage security through risk make smarter investments, suffer fewer surprises, and are better prepared when incidents occur.

Risk assessment is also a regulatory requirement. The Kenya DPA requires organisations to implement appropriate technical and organisational measures proportionate to the risk. ISO 27001 makes risk assessment the centrepiece of the entire ISMS. NIST, PCI DSS, and most other frameworks also mandate it.

Key principle The goal of risk assessment is not to eliminate all risk — that is neither possible nor economically sensible. The goal is to understand your risks clearly enough to make rational decisions about which to reduce, transfer, or accept.

2. Common Risk Assessment Frameworks

Several frameworks are commonly used for cybersecurity risk assessment. You do not need to adopt one rigidly — a hybrid approach drawing on multiple frameworks is common and often most practical.

Framework	Description	Best suited for
NIST CSF	Organises risk management around five functions: Identify, Protect, Detect, Respond, Recover. The 2.0 version adds Govern.	First risk assessments; board-level framing; organisations wanting a US/international standard.
ISO 27005	The ISO risk management standard designed as a companion to ISO 27001. Asset-based approach.	Organisations pursuing ISO 27001 certification.
FAIR	Factor Analysis of Information Risk — a quantitative model that expresses risk in financial terms (loss exceedance curves).	Board reporting; cyber insurance; ROI calculations for security investments.
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation — a self-directed, team-based approach.	Smaller organisations without dedicated security teams.

3. Defining Scope and Objectives

Before starting, define clearly what the risk assessment covers and what it is intended to achieve. Scoping prevents the assessment from becoming unwieldy and ensures the results are actionable.

Scope questions to answer:

- Which systems, applications, and data are included?
- Which locations or business units are covered?
- Are third-party systems and suppliers in scope?
- What is the assessment time horizon (e.g. current state, or forward-looking 12 months)?

Objectives questions to answer:

- Is this assessment for internal risk management, regulatory compliance, board reporting, or ISO 27001?
- What decisions will the results inform — budget allocation, control selection, insurance purchase?
- Who are the primary consumers of the output — CIO, board, ODPC?

4. Step 1: Asset Inventory

You cannot assess risk to things you don't know about. A comprehensive asset inventory is the foundation of every risk assessment. Assets are broader than just IT hardware — they include any resource that has value to the organisation and that, if compromised, would cause harm.

Asset category	Examples
Information assets	Customer databases, HR records, financial data, contracts, intellectual property, emails.
Software assets	Core business applications, ERP, CRM, payroll systems, mobile apps, cloud services.
Hardware assets	Servers, laptops, workstations, mobile devices, networking equipment, printers, CCTV.
Service assets	Internet connectivity, electricity supply, third-party cloud services, payment processing.
People assets	Key staff with unique knowledge, administrators with privileged access, third-party contractors.
Intangible assets	Brand reputation, regulatory licences, customer trust, competitive intelligence.

Assign each asset an owner — an individual responsible for assessing risk to that asset and ensuring appropriate controls are in place. Ownerless assets are consistently under-protected.

5. Step 2: Threat Identification

A threat is any potential event that could harm an asset. Threats are not hypothetical — they should be grounded in the actual threat landscape facing organisations in your sector, geography, and size.

Relevant threats for East African organisations (2025):

Threat	Category
Business Email Compromise (BEC)	Human / Social engineering
Phishing and spear phishing	Human / Social engineering
SIM swap fraud	Human / Social engineering
Ransomware	Malware
Credential stuffing / brute force	Technical attack
Insider data theft or fraud	Insider threat
Supply chain compromise	Third-party risk
DDoS attack on web services	Technical attack
Accidental data disclosure	Human error
Cloud misconfiguration	Technical / Human error
Physical theft of devices	Physical threat
Power outage / infrastructure failure	Environmental

6. Step 3: Vulnerability Identification

A vulnerability is a weakness that could be exploited by a threat. Vulnerabilities exist in technology, processes, and people. Common methods for identifying vulnerabilities include:

- Automated vulnerability scanning tools (Nessus, Qualys, OpenVAS) run against internal and external-facing systems.
- Penetration testing — authorised simulated attacks that actively attempt to exploit weaknesses.

- Configuration reviews — checking that systems are hardened against known insecure defaults.
- Policy and process reviews — identifying gaps in procedures, training, access controls, and monitoring.
- Threat intelligence — using knowledge of how current attackers operate to identify specific weaknesses in your environment that are being actively exploited in the wild.

CVE monitoring	Subscribe to vulnerability feeds (CISA KEV catalogue, NVD) and ensure your patch management process can respond to critical CVEs within 48–72 hours of disclosure for internet-facing systems.

7. Step 4: Likelihood and Impact Scoring

For each identified risk (a combination of an asset, threat, and vulnerability), assign a likelihood score and an impact score. The product of these gives the overall risk level.

5-point scoring scale:

Score	Likelihood definition	Impact definition
1 — Very Low	Unlikely to occur in 5 years; no known active exploitation.	Negligible financial or operational impact.
2 — Low	Could occur once every few years; low attacker motivation.	Minor disruption; easily recoverable; < KES 500K.
3 — Medium	Could occur in the next 12 months; moderate attacker capability.	Significant disruption; ODPC reportable; KES 500K–5M.
4 — High	Likely to occur in the next 6 months; active exploitation observed.	Major incident; regulatory action; KES 5M–50M impact.
5 — Critical	Already being actively exploited; imminent threat.	Catastrophic; existential risk to the organisation.

Risk Level = Likelihood × Impact. A risk scoring 4 × 4 = 16 (High) requires urgent treatment. A risk scoring 1 × 2 = 2 (Very Low) can be monitored or accepted. Establish risk appetite thresholds — e.g. any risk with a combined score above 12 must be actively treated.

8. Step 5: Risk Evaluation and Prioritisation

Risk evaluation compares the calculated risk levels against your organisation's risk appetite — the amount and type of risk the organisation is willing to accept in pursuit of its objectives. Risks that exceed the risk appetite require treatment. Risks within the risk appetite can be monitored or accepted.

Risk appetite should be formally defined by senior leadership and documented. Typical thresholds:

- Risks scoring 20–25 (Critical): require immediate executive action and urgent treatment.
- Risks scoring 12–19 (High): must be actively treated within the current planning period.
- Risks scoring 6–11 (Medium): treated in the medium term; tracked and reviewed quarterly.
- Risks scoring 1–5 (Low): accepted or monitored; reviewed annually.

9. Step 6: Risk Treatment Options

For every risk that exceeds your risk appetite, you must select a treatment approach:

Treatment	When to use it	Example
Reduce (Mitigate)	The risk can be lowered to an acceptable level by implementing additional controls at reasonable cost.	Deploy MFA to reduce the risk of account takeover from credential stuffing.
Transfer	The residual risk can be transferred to a third party — typically through cyber insurance or contractual liability transfer.	Purchase cyber insurance to cover the financial impact of a ransomware attack.
Avoid	The risk is unacceptable and the business activity causing it can be stopped or redesigned.	Stop storing sensitive customer data on local servers; migrate to encrypted, access-controlled cloud storage.
Accept	The risk is within risk appetite or the cost of treatment exceeds the expected loss. Must be formally documented and approved by an appropriate risk owner.	Accept the low risk of a disgruntled former employee with no system access causing reputational harm.

10. Maintaining the Risk Register

The risk register is the central document that records all identified risks, their scores, treatment decisions, owners, and status. It is a living document — not a one-time deliverable.

Risk register minimum fields:

- Risk ID and description
- Asset affected
- Threat and vulnerability
- Inherent likelihood and impact scores (before controls)
- Existing controls
- Residual likelihood and impact scores (after controls)
- Risk treatment decision and planned actions
- Risk owner (named individual)
- Review date

When to update the risk register:

- Scheduled quarterly or annual review.
- Following a security incident or near-miss.
- When new systems, services, or significant business changes are introduced.
- When the threat landscape changes materially (e.g. emergence of new attack techniques).

11. Communicating Risk to the Board

Board members and senior executives make better security investment decisions when risk is communicated in business terms — not technical jargon. The goal is to enable informed decision-making, not to demonstrate technical expertise.

Principles for board-level risk communication:

- Translate technical risk into business and financial terms: instead of 'we have 47 unpatched CVEs,' say 'our unpatched systems have a 40% chance of being exploited in the next 6 months, with an estimated financial impact of KES 15–50 million.'
- Use a heat map: a simple 5x5 risk heat map (likelihood on one axis, impact on the other) gives the board an instant visual picture of the risk landscape.
- Focus on top 5–10 risks: do not present every risk in the register. Present the highest-priority risks, proposed treatments, estimated cost of treatment, and the cost of not treating.
- Show trends: comparing this quarter's risk scores to the previous quarter shows whether the organisation's risk posture is improving or deteriorating.

- Connect to regulatory obligations: where a risk relates to a Kenya DPA or other regulatory requirement, make that connection explicit — board members respond to regulatory liability.
- End with decisions required: be explicit about what you need the board to approve — budget, policy changes, risk acceptance decisions. Avoid 'for information only' reports that require no action.

Board risk report structure	Executive summary (1 page) → Top risks heat map → Top 5 risks with treatment status → Incidents and near-misses this period → Security investments and their impact → Regulatory and compliance status → Decisions required.

How SecureZaidi Can Help

SecureZaidi is a Kenya-based cybersecurity and GRC consultancy specialising in helping East African organisations achieve and maintain compliance, reduce cyber risk, and build lasting security cultures. Our consultants bring deep, practical expertise in the Kenyan regulatory environment and the realities of doing business in the region.

Kenya DPA Compliance	ODPC registration, DPIA support, DPO-as-a-Service, policy development, and staff training.
ISO 27001 Certification	Gap analysis, ISMS implementation, internal audit support, and certification readiness preparation.
Security Awareness Training	Customised staff workshops, phishing simulation campaigns, and 12-month culture programmes.
GRC Advisory	Risk register development, threat modelling, board-level reporting, and policy frameworks.
vCISO Services	Fractional CISO leadership — strategy, oversight, and executive reporting without a full-time hire.
Penetration Testing	Authorised simulated attacks on networks, web applications, and cloud environments.

Ready to take the next step? Contact us today for a no-obligation consultation.

Email	info@securezaidi.com
Phone	+254 700 000 000
Website	securezaidi.com