Security Audit Readiness Checklist

What to have ready before a scoped security assessment

Prepared by	Nazline Mwita, CompTIA Security+
Practice	HarLyn Digital Partners
Scope	Self-assessment starting point — not a substitute for a scoped audit

Scope & Access

- A clear list of in-scope hosts, applications, and environments is documented.
- Test accounts at each privilege level (admin, standard user, guest) are available for the auditor.
- An emergency contact and rollback plan exist for the testing window.

Infrastructure

- Cloud configuration (storage buckets, IAM roles, security groups) has a current inventory.
- Unused or forgotten environments (staging, demo, legacy) are identified before the audit, not discovered during it.
- Secrets management (env vars, key vaults) is documented — auditors shouldn't find hardcoded keys as a surprise.

Process & Policy

- An incident-response plan exists, even a lightweight one, with a named owner.
- Access reviews (who has admin rights, and why) happen on a cadence, not never.
- Previous audit findings (if any) have a documented remediation status.

After the Audit

- There's a plan to triage findings by severity within an agreed window, not “someday.”
- A retest pass is scheduled to confirm closed findings are actually closed.

How to use this checklist

This is a starting-point self-assessment, not a substitute for a scoped engagement. Items checked “no” or “unsure” are candidates for a Secure Digital Workflow Assessment.

Nazline Mwita, CompTIA Security+ certified Cybersecurity Assurance Lead and Co-Founder at HarLyn Digital Partners. Specializing in authorized web & API security assessments, KDPA compliance reviews, and defensive cloud architecture in Nairobi, Kenya.