Cyber Audit / Digital Audit

Make your system safe and auditable

Introduction to Cyber Audit (Policy Perspective)

- Cyber Auditing is the systematic review of digital systems, data, and controls
- Focuses on governance, accountability, risk, and compliance
- It does not require technical skills or coding knowledge
- It answers a simple question:
- “Are our digital systems safe, controlled, and accountable?”

Cyber Audit vs Traditional Audit

- Traditional Audit
  - Paper files and physical records
  - Manual approvals and signatures
  - Visible fraud and errors
- Cyber / Digital Audit
  - Online systems and databases
  - Automated decisions and transactions
  - Hidden risks (data misuse, access abuse)

Cyber Auditing is a Policy Issue (Not an IT Issue)

- Digital systems directly affect:
  - Citizen services
  - Public funds
  - National reputation
- Cyber failures lead to:
  - Data leaks
  - Service disruption
  - Loss of public trust

Cyber risk is a governance and leadership responsibility

What Cyber Auditing Looks At (High Level)

- Cyber Auditing reviews:
  - Who can access systems and data
  - How citizen data is protected
  - Whether vendors are properly controlled
  - How incidents are handled
  - Whether policies are implemented in practice

No technical testing required

Government Digital Assets

- Citizen Data
  - NID, birth registration, social safety net data
- Government Systems
  - Ministry portals, service platforms, databases
- Financial Systems
  - e-GP, digital payments, allowance distribution
- Infrastructure
  - Data centers, government cloud, networks
- Third-Party Assets
  - Vendor-managed systems and outsourced platforms

Government Threat Landscape (Policy View)

- Unauthorized access by staff or vendors
- Data leakage due to poor access control
- Weak passwords and shared user accounts
- System downtime and service disruption
- Vendor negligence or lack of accountability

Threats are not only hackers, they often arise from weak management and controls.

Cyber Laws

- Protect citizen data and digital services
- Define responsibilities for government and vendors
- Ensure accountability in case of cyber incidents
- Support legal action against misuse or negligence

Key Cyber Laws & Policies in Bangladesh

- Cyber Security Ordinance, 2025
- Personal Data Protection Ordinance, 2025
- Information and Communication Technology (ICT) Act, 2006

Cyber Security Ordinance, 2025

Category (Ordinance 2025)	Legal Sanction
Online Gambling	Up to 2 years jail or Tk 1 crore fine or both
Cyber Fraud / Financial Deception	Up to 2–5 years jail + significant fines
Cyber Deception / Forgery	Up to 5 years jail + fines
Sexual Harassment & Exploitation Content	Increased penalties with special protection for children and women
Repealed Offences	Cases under old sections are void and dismissed

Access Control & Identity Audit

- What is Access Control?
  - Access control defines who can use which system or data and what they can do.
  - Ensures that only authorized users access sensitive information.
  - Key for protecting citizen data, financial systems, and critical infrastructure.

What is Identity Audit?

- A systematic review of user accounts, roles, and permissions.
- Checks if:
  - Old accounts are disabled after staff leave or transfer
  - Users have appropriate access levels for their role
  - Vendor or third-party access is controlled and monitored

Common Gaps in Government Systems

- Shared login credentials among staff and senior officer
- Shared login credentials among previous officer
- Excessive privileges for vendors or temporary users
- No periodic access review
- Lack of accountability for misuse

Audit Questions for Officials and Identity

- Who has access to this system today?
- Is access reviewed and updated regularly?
- Are vendors monitored for compliance?
- What happens if an account is compromised?

Data Audit

- What is Data Audit?
  - A systematic review of data collection, storage, usage, and protection in government systems.
  - Ensures data is accurate, secure, and compliant with laws and policies.
  - Focuses on citizen data, financial records, and operational databases.

Key Audit Questions

- Is data classified correctly (sensitive vs routine)?
- Who owns and is responsible for the data?
- Are there controls for integrity, confidentiality, and availability?
- How is data shared with vendors or other departments?
- Is there a data retention and disposal policy?

Vendor & Outsourced IT Audit

- A Vendor / Outsourced IT Audit is the review of systems, processes, and services managed by external providers.
- Ensures that outsourced IT activities comply with laws, policies, and government standards.
- Outsourced systems still carry government data and citizen information.
- Weak vendor management can lead to data breaches, service disruption, and legal liability.
- **Senior officials** remain accountable for governance, even if IT is outsourced.

Key Audit Focus Areas for Vendors

- Contractual Compliance
  - Are security and data protection responsibilities clearly defined?
  - Are penalties and SLAs (Service Level Agreements) included?
- Access Management
  - Do vendors have limited and monitored access?
  - Are vendor accounts regularly reviewed and revoked when unnecessary?

Key Audit Focus Areas for Vendors

- Data Handling & Security
  - Is sensitive data encrypted, backed up, and classified?
  - Are vendors following data retention and disposal policies?
- Incident Reporting
  - Are vendors required to report breaches or suspicious activities immediately?
  - Are response procedures tested and documented?

Practical Audit Questions & Policy for Vendors

- Who owns the data vs who manages it?
- Does the vendor comply with legal and policy obligations?
- Are there regular audits or reports from the vendor?
- What controls ensure accountability for service failures?

Risks of outsourcing IT systems

- Data Security & Privacy
  - Sensitive citizen data may be exposed or misused.
  - Weak vendor access control or poor encryption can cause breaches.
- Loss of Control
  - Government loses direct oversight of critical systems.
  - Operational decisions may depend on vendor priorities.
- Compliance & Legal Liability
  - Vendors may fail to follow cyber laws or policies.
  - Government remains accountable for legal violations.
- Service Disruption
  - Downtime or delays in vendor support can halt citizen services.

Cyber Incident & Breach Audit

- A Breach Audit assesses whether an organization handles cyber incidents and data breaches according to laws, policies, and best practices.
- Focuses on risk mitigation, reporting, and prevention, ensuring leadership accountability.
- Assess Response Procedures
  - Was there a formal incident response plan?
  - Were roles and responsibilities clearly defined and followed?
- Check Reporting Compliance
  - Were breaches reported to senior management, regulatory authorities, or affected citizens as required?

Digital Financial Systems & Fraud Audit

- What is Digital Financial Systems Audit?
  - A review of online payment platforms, e-GP systems, digital disbursements, and financial databases.
  - Ensures accuracy, integrity, and compliance of financial operations.
- What is Fraud Audit?
  - Systematic check for fraud, misappropriation, or unauthorized transactions in digital financial systems.
  - Focuses on controls, monitoring, and accountability, not technical coding.
- Data Integrity & Security
  - Is financial data protected from unauthorized changes?
  - Are backups and encryption implemented and tested?

Audit Reporting & Executive Decision-Making

- Summarizes findings from cyber, data, or financial audits.
- Highlights risks, gaps, and compliance issues in a clear, actionable way.
- Designed for decision-makers, not technical staff.
- Provides a snapshot of risks and operational vulnerabilities.
- Helps prioritize actions and allocate resources efficiently.
- Supports policy compliance and governance oversight.

IT Audit Report Template

- Executive Summary
  - Audit Title:
  - Department / System:
  - Audit Period:
  - Auditors:
  - Overall Assessment: (e.g., Compliant / Needs Improvement / High Risk)
  - Key Highlights: 3–5 bullet points summarizing major findings or risks.

IT Audit Report Template

- Objectives
  - Purpose of the audit (e.g., review cyber controls, data integrity, digital financial systems, vendor management).
- Scope
  - Systems, applications, and processes reviewed.
  - In-scope vs out-of-scope items.
- Methodology
  - Review of policies, contracts, logs, and access records.
  - Interviews with system owners and staff.
  - Review of incident reports, audit trails, and compliance documents.

IT Audit Report Template

- Key Findings

Finding No.	Issue / Gap Identified	Risk Level (High/Medium/Low)	Evidence / Observation	Impact (Operational / Financial / Reputational)
1				
2				
3				

IT Audit Report Template

- Recommendations

Finding No.	Recommendation	Responsible Party	Priority (Immediate / Short-Term / Long-Term)	Target Completion
1				
2				
3				

Executive Decisions / Action Taken

- Decisions made based on audit findings.
- Policies approved, resources allocated, or corrective measures mandated.
- Responsible authorities identified.

Bangladesh Government Digital Ecosystem

- National web portals (ministry portals, service portals)
- Citizen databases (NID, birth registration, social safety nets)
- Financial systems (e-GP, digital payments, subsidies)
- Cloud and data centers (National Data Center, government cloud)
- Outsourced and vendor-managed systems

Bangladesh Government Digital Ecosystem

- Audit Focus
  - Who owns the system?
  - Who controls the data?
  - Who is accountable when something fails?

Common Cyber Risks in BD Public Sector

- Data leaks due to weak access control
- Poor password and account management
- Over-dependence on third-party vendors
- Lack of regular system audit and monitoring
- Limited cyber awareness among staff

Legal & Policy Framework (Audit Perspective)

- Digital Security Act & relevant ICT laws
- Data protection obligations of government agencies
- National ICT Policy and e-Governance guidelines
- Internal government circulars and compliance instructions

Typical Audit Weaknesses Observed in Government Projects

- No clear data classification (everything treated the same)
- Excessive system access for staff and vendors
- No exit process when officials are transferred
- Incident handling done informally
- Cyber audit treated as IT issue, not management issue

Outsourcing & Vendor Risks in Bangladesh

- Most government systems are developed and maintained by vendors
- Contracts focus on delivery, not security
- Limited vendor accountability after system deployment
- Audit Questions
  - Does the contract define data ownership?
  - Are security responsibilities clearly stated?
  - Is there an exit and handover plan?

Mini Case Study (Bangladesh-Style Scenario)

- Background of the Project

As part of the Digital Bangladesh / Smart Bangladesh initiative, a government department launched an online citizen service portal to issue certificates and manage benefit-related applications. The objective was to reduce physical visits, improve transparency, and speed up service delivery.

The system was:

- Developed by a local private IT vendor
- Hosted on a government-approved data center
- Used nationwide by district and field-level offices
- Accessible to both government officials and outsourced support staff

Thank You