Shaswat Manoj Jha, CISA

CISA | ISO 27001 Lead Auditor | ISO 42001 Lead Auditor | CEH
MBA (IT) | B.Tech (CSE)
Technology Risk & IT Audit | SOX ITGC/ITAC, Cloud, Cyber & AI Governance

(+91) 9234567699
hello@shaswatmanojjha.com
shaswatmanojjha.com

// Professional Synopsis:

CISA-certified IT Risk & Compliance Professional with **4+ years** of experience delivering Information Security Audits across Cloud, **ITGC** and **ITAC** environments, and evaluating complex security configurations across on-premises and public cloud environments. In the team, known for a strong analytical judgement, structured problem solving, and meticulous attention to detail in audit documentation. Skilled at analysing digital infrastructures and mapping technical controls to rigorous global frameworks **(NIST, ISO)** and regional guidelines **(IRDAI, SAMA, SOX, DPDP)**. Possesses a strong grasp of information security principles, data privacy regulations, operational resilience and risk management standards **(NIST RMF, ISO 22301, ISO 42001, ISO 31000)**.

With extensive exposure to the financial services and insurance sectors, specialized in collaborating with cross-functional teams for integrated audits across global and Indian organizations to deliver tailored, stakeholder-focused solutions.

Experienced in managing the **full audit lifecycle**, from developing client **proposals** to efficiently executing the audit fieldwork with defensible documentation, and delivering insightful executive reports translating technical findings into actionable insights on compliance maturity and operational resilience.

// Certifications:

- **CISA (Certified Information Systems Auditor)** – *ISACA*
- **ISO/IEC 27001 Lead Auditor** *(Information Security Management System) – IRCA*
- **ISO/IEC 42001 Lead Auditor** *(Artificial Intelligence Management System) – Exemplar Global*
- **Certified Ethical Hacker (CEHv12)** – *EC Council (Score: 92.8%)*
- **ISEA Certified Cyber Hygiene Practitioner** – *Ministry of Electronics & IT (MeitY), Govt. of India*

// Core Competencies & Technical Stack:

- **Audit & IT Governance:**
  ITGC (IAM, Incident, Change, BCP/DR), ITAC, Third Party Risk Management, ToD and ToE for IT Controls, Integrated Audits, Policy Review, IT Governance, RFPs.
- **Cloud Security & Identity:**
  AWS, Microsoft Azure, SailPoint, Active Directory, Cloud Security Posture Management (CSPM), CyberArk (PAM), Splunk (SIEM), DLP, Endpoint Detection and Response (EDR).
- **Frameworks & Regulations:**
  Sarbanes-Oxley (SOX), ISO 27001, ISO 31000, ISO 42001, NIST CSF 2.0, NIST SP 800-53, CIS Benchmarks, CSA Cloud Controls Matrix (CCM), SAMA CSF, DPDP Act 2023, IRDAI IS Guidelines, OWASP Top 10.
- **Tools & Technologies:**

GRC & Audit Management:	AuditBoard, ServiceNow, RSA Archer, GitHub
Data Analytics & Visualization:	Power BI, Microsoft Visio, Advanced Excel
Scripting & Programming:	Python, SQL
Identity & Cloud Access:	AWS, Microsoft Azure, SailPoint, Active Directory, CyberArk

// Professional Competencies:

- **Executive Communication**
- **Proactive & Self-Directed**
- **Stakeholder Management**
- **Technical Storytelling**
- **Accountability & Ownership**
- **Continuous Learning**

// Employment History:

Full Time at	**Designation**	**From**	**To**
EY (Ernst & Young)	Consultant – IS Audit & Risk	August 2024	**Present**
Protiviti	Consultant 3 – IT Audit & Tech Risk	June 2023	July 2024
Nangia and Co LLP	Senior Analyst – Cybersecurity	June 2022	June 2023
Internship at	**Designation**	**From**	**To**
Tata Consultancy Services	Intern – Advanced DAST	June 2020	August 2020

// Work Experience:

- **IT General Controls (ITGC) and Cloud Security:**
  - ✓ Led end-to-end **integrated audits** by mapping technical controls to key business processes and risks. Executed Test of Design (**ToD**) and Operating Effectiveness (**ToE**) across **IAM**, **IT Operations, Incident/Change Management**, and **BCP/DR**, ensuring compliance with **SOX, IRDAI & ISO 27001**.
  - ✓ Assessed cloud infrastructure and vendor risk by evaluating security configurations against **CIS Benchmarks** (IAM, encryption, network segmentation, DR) and utilizing **CSA Cloud Controls Matrix (CCM)** and **CAIQ** to enforce strict alignment with the **Shared Responsibility Model**.
  - ✓ Audited **Robotic Process Automation (RPA)** environments for ITGC compliance, focusing on bot account management, credential vaulting, Segregation of Duties (SoD), and exception handling.
  - ✓ Assessed **GitHub** environments to validate IAM, privileged access monitoring, and secure repository configurations, enforcing strict governance over integrated **AI tools** to ensure responsible usage and mitigate unauthorized code modification.
- **ISMS Governance & Policy Review:**
  - ✓ Reviewed and improved **ISMS policies (IAM, BCP/DR, Cyber Crisis, Change, Incident, Acceptable Use, Asset Management)** to align with organizational objectives and **ISO 27001:2022** standards.
  - ✓ Drove ISMS policy adherence by developing **testing checklists** and **sampling plans**, to identify non-conformities and defined corrective action plans for resolution.
- **IT Application Controls (ITAC):**
  - ✓ Tested **IT application controls** (interfaces, edit checks, master data, report integrity) and unauthorized data modification risks (maker-checker workflows, audit trails, input sanitization) to provide assurance on **data accuracy, completeness**, and **authorized processing**.
  - ✓ Recommended SDLC and system configuration improvements to automate controls, significantly reducing manual intervention and lowering control failure probabilities.
- **Regulatory Compliance (IRDAI, SAMA, DPDP etc.) and Policy Adherence:**
  - ✓ Aligned **ISO 27001** implementations with **IRDAI** guidelines, cross-mapping controls to **NIST CSF 2.0** and **NIST SP 800-53** by performing gap analyses to identify and mitigate residual risk.
  - ✓ Performed gap assessments against **SAMA Cybersecurity Framework (SAMA CSF)** across IT governance policies, steering remediation efforts to successful closure.
  - ✓ Conducted data privacy assessments aligned with **Digital Personal Data Protection Act (DPDP 2023)**, assessing applications and APIs for **PII exposure** across application front ends, system logs, reports and data exports. Developed strategies driven by data minimization, hashing, consent management and retention**.**
- **Vendor / Third Party Risk Management:**
  - ✓ Executed **Third-Party Risk Management (TPRM)** assessments, evaluating **SLA compliance**, **logical access controls, physical security** and **data protection standards.**
  - ✓ Performed **on-site vendor assessments** targeting **social-engineering exposure**, endpoint DLP, data **handling**, and **access provisioning** to mitigate **insider threats** and **data leakage**.
- **Data Security, Endpoint Review and DLP Testing:**
  - ✓ Mapped **sensitive enterprise data flows** across users, processes and IT systems on **Microsoft Visio,** to systematically identify potential data leakage points and operational risks.
  - ✓ Strengthened **enterprise endpoint security** by identifying **DLP control** gaps and enforcing asset hygiene through asset inventory, patch management, DLP rulesets, and **Endpoint Detection and Response (EDR)** updates, while tracking compliance and exceptions via custom Power BI dashboards.
- **Cybersecurity, Dynamic Application Security and Penetration Testing (DAST):**
  - ✓ Performed **automated** and **manual DAST** using Burp Suite, OWASP ZAP, and SQLMap to identify **OWASP Top 10** issues (SQLi, XSS, IDOR, Broken Authentication, Security Misconfiguration).
  - ✓ Captured Proof of Concepts (PoCs) and assigned **CVSS risk ratings,** collaborated with IT to implement secure defaults (least privilege, rate limiting, input sanitization), and verify vulnerability remediation.
- **Proposals, Reports and Documentation:**
  - ✓ Scoped client **proposals** by defining methodologies, effort estimates and acceptance criteria to secure high-value audit engagements.

- ✓ Developed comprehensive audit documentation including Risk and Control Matrices (**RACM**), detailed workpapers, and evidence repositories, to maintain strict quality standards and provide clear defensibility of audit conclusions.
- ✓ Developed **executive-ready reports** with **Power BI dashboards,** translating complex technical risks into prioritized, actionable remediation roadmaps for C-suite stakeholders.

// Notable Audit Automation & Technical Initiatives:

- Developed a **PII scanner script** in Python using regular expressions to analyse 1,000+ unstructured files, including system logs, PDF reports and spreadsheets (.txt, .pdf, .xlsx) to automatically identify sensitive data exposure, drastically accelerating the audit timeline from **weeks to days**.
- Identified and responsibly disclosed a critical authorization bypass vulnerability (Broken Access Control) in a major SaaS platform that allowed unauthorized access to premium features without upgrading. Collaborated with the vendor on remediation and was formally acknowledged and **rewarded for the disclosure**.
- Developed a PowerShell automation script to extract, and reconcile Active Directory (AD) user list against HR termination lists, **reducing the manual effort required** to test the operating effectiveness of quarterly User Access Reviews.
- Executed a comprehensive **VAPT** assessment on a dummy eCommerce platform using Nessus, Nmap and Burp Suite. Successfully exploited SQL Injection, XSS, IDOR vulnerabilities and delivering a 126-page VAPT report. **[View Project]**
- Developed "Admission Guardian", a web-based directory for students, featuring 19,000+ institutions, exams, courses and more with complex database schema and application logic.

// Education:

Degree / Program	Institution	Score	Year
MBA – Information Technology and Finance	Swami Vivekananda Subharti University, Meerut (Distance)	70%	2022 – 24
B. Tech – Computer Science and Engineering	Madhyanchal Professional University, Bhopal (Full-Time)	81%	2018 – 22

// Trainings:

Training	Certification Body
Data Privacy – Bronze Learning (2026)	Ernst and Young
Applied AI – Bronze Learning (2025)	Ernst and Young
IBM Specialization on Generative AI for Cybersecurity Professionals	from IBM via Coursera
Information Systems Audit, Controls and Assurance	from The Hong Kong University via Coursera
Cybersecurity Management (5 Weeks)	Charles Sturt University
Additional certifications and training: shaswatmanojjha.com/certifications	

// Key Achievements:

- Recognized with the "**Client Extraordinaire**" award by Ernst & Young (EY) for serving as a trusted business advisor and creating value for the client.
- Achieved a high-distinction score of **92.8%** on the EC-Council CEH (Certified Ethical Hacker) exam.

// Personal Information:

- **Current Address** – Pune, Maharashtra
- **Preferred Location** – Remote / Kolkata / Delhi / Gurugram
- **Linguistic Abilities** – English, Hindi & Maithili

"Combining together technology risk and audit experience, technical expertise, process automation, and business-focused reporting to deliver defensible assurance and practical remediation."