Shaswat Manoj Jha

ISO 27001 & ISO 42001 Lead Auditor | CEHv12 | B.Tech (CSE) | MBA (IT)

(+91) 9234567699 | shaswatmanojjha@gmail.com | www.shaswatmanojjha.com

Professional Synopsis:

IT Risk & Compliance Professional with nearly 4 years of experience specializing in **Information Security Audits** including **ITGC & ITAC**, and evaluating security configurations across local and public cloud platforms. Adept at analysing digital environments and mapping controls to governance frameworks, including **NIST CSF**, **ISO 27001 and ISO 42001**. Proven track record of conducting integrated audits, collaborating with cross-functional teams within the financial services sector to identify control gaps, provide actionable insights, and deliver stakeholder-focused recommendations that enhance operational resilience and audit efficiency.

Passionate about continuous learning and innovation. Possess a strong grasp of information security principles, privacy regulations, and frameworks such as **NIST RMF 800-37**, **PCI-DSS**, **ISO 22301**, and **ISO 31000**. In the team, often known for a **keen analytical eye** and **meticulous attention** to detail.

With extensive exposure to the **insurance** and **financial services** sectors, have collaborated with leading **global and Indian organizations** to deliver **tailored, stakeholder-focused solutions** that enhance compliance maturity, operational resilience, and audit efficiency.

Experienced at developing **winning proposals, RFPs, reports**, **audit documentation (RACM, Workpapers, Evidence etc)**, and **insightful presentations** that communicate technical findings with clarity.

Certifications:

- ISO/IEC 27001 (Information Security Management System) Lead Auditor – IRCA
- ISO/IEC 42001 (Artificial Intelligence Management System) Lead Auditor – Exemplar Global
- Certified Ethical Hacker :: CEHv12 – EC Council (Score - 92%)
- ISEA Certified Cyber Hygiene Practitioner – Ministry of Electronics & IT (MeitY), Govt. of India

Work Experience: (4 Years)

Full Time at	Designation	From	To
EY (Ernst & Young)	Consultant – IS Audit & Risk	August 2024	**Present**
Protiviti	Consultant 3 – IT Audit	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

Education:

Degree / Program	Institution	Year
MBA – Information Technology and Financial Management	Swami Vivekananda Subharti University, Meerut (Distance)	2022 – 2024
B. Tech – Computer Science and Engineering (81%)	Madhyanchal Professional University, Bhopal (Full-Time)	2018 – 2022

Soft Skills:

- Detail Oriented
- Selling & Negotiation
- Self-Directed
- Critical Thinking
- Proactive Initiator
- Innovative
- Googling (Dorks)
- Project Ownership

Familiar Technologies & Expertise:

- **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

- **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) & CAIQ, SAMA CSF, DPDP Act 2023, IRDAI Information Security Guidelines, OWASP Top 10

- **Tools & Technologies:**
  GRC & Audit Management: AuditBoard, ServiceNow, RSA Archer, RPA, GitHub
  Data Analytics & Visualization: PowerBI, Microsoft Visio, Advanced Excel
  Scripting & Programming: Python, SQL
  Identity & Cloud Access: AWS, Microsoft Azure, SailPoint, Active Directory, CyberArk

Detailed Work Experience:

IT General Controls (ITGC) and Cloud Security:

- ✓ Led end-to-end ITGC audits, executing Test of Design (ToD) and Test of Operating Effectiveness (ToE) across IAM, Incident/Change Management, IT Operations, DR, and Physical Security, ensuring compliance with **SOX, NIST CSF 2.0, and NIST SP 800-53**.
- ✓ Evaluated cloud infrastructure security configurations against **CIS Benchmarks**, validating IAM, encryption, network segmentation, and Disaster Recovery readiness.
- ✓ Assessed cloud vendor risk and compliance posture using the **CSA Cloud Controls Matrix (CCM)** and **CAIQ**, enforcing strict alignment with the Shared Responsibility Model.
- ✓ Executed **integrated audits** by mapping IT controls directly to key business processes and financial assertions.
- ✓ 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** and models to mitigate unauthorized code modification and ensure responsible usage.

ISMS Governance & Policy Review:

- ✓ Reviewed and improved **ISMS policies (IAM, BCP/DR, Cyber Crisis, Change, Incident, Acceptable Use, Asset Management)** driving alignment with **ISO 27001:2022** and broader organizational objectives.
- ✓ Drove ISMS policy adherence by developing **testing checklists** and **sampling plans**, to identify **non-conformities** and designed **corrective actions plans** for compliance reporting.

IT Application Controls (ITAC):

- ✓ Tested **IT application controls** (interfaces, edit checks, master data, report integrity, and **SoD**) to provide assurance on **data accuracy, completeness**, and authorized processing.
- ✓ Mitigated **unauthorized data modification** risks by validating **preventative and detective** controls including maker–checker workflows, audit trails, and parameter security.
- ✓ Recommended SDLC and system configuration improvements to automate controls, significantly reducing manual intervention and lowering control failure probabilities.

Regulatory Compliance (RBI, IRDA, 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 with management sign-off.
- ✓ Conducted data privacy assessments aligned with **Digital Data Protection Act (DPDP 2023)** by assessing applications and APIs for **PII exposure** across frontend, logs and exports. Provided remediation recommendations based on minimization, hashing, consent and retention principles.

Vendor / Third Party Risk Management:

- ✓ Executed **Third-Party Risk Management (TPRM)** assessments covering **SLA compliance**, **logical and physical security** & **data protection.**
- ✓ 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, systems and apps** on **Microsoft Visio,** and evaluated various processes to identify potential data **leakage points and vulnerabilities**.
- ✓ Strengthened **enterprise endpoint security** by identifying **DLP control** gaps and centralizing hygiene, including asset inventory, patch management, targeted 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 and validate **OWASP Top 10** issues (**SQLi**, **XSS**, **IDOR**, **Broken Authentication**, **Security Misconfiguration**, **Sensitive Data Exposure**).
- ✓ 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 **executive-ready reports** with **PowerBI dashboards,** translating complex technical risks into prioritized, actionable remediation roadmaps for C-suite stakeholders.

Notable Trainings:

Training	Certification Body	Completion
Data Privacy - Bronze Learning (2026)	Ernst and Young	Feb 2026
Applied AI - Bronze Learning (2025)	Ernst and Young	Jan 2025
IBM Specialization on Generative AI for Cybersecurity Professionals	from IBM via Coursera	Jan 2025
Information Systems Audit, Controls and Assurance	from The Hong Kong University of Science and Technology via Coursera	Apr 2024
Cybersecurity Management (5 Weeks)	Charles Sturt University	Apr 2023
View More at: shaswatmanojjha.com/#certifications		

Notable Audit Automation & Technical Initiatives:

- ➢ Developed a **PII scanner script** in Python utilizing RegEx to parse tens of gigabytes of unstructured client data (.txt, .pdf, .xlsx). Automated the identification of sensitive data exposures, drastically accelerating the privacy assessment timeline from **several weeks to a few 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, format, and reconcile Active Directory (AD) user group memberships against HR termination lists, **reducing the manual effort** required for quarterly User Access Reviews (UAR).
- Executed a comprehensive **Vulnerability Assessment and Penetration Test (VAPT)** on a dummy eCommerce platform using Nmap, Burp Suite, SQL Map, and OWASP ZAP. **Successfully exploited vulnerabilities** such as SQL Injection, XSS & IDOR and drafted a 126-page Vulnerability Assessment & Penetration Testing (VAPT) report. **[View Project]**
- Developed a web platform "College Finder", a data-driven web application (Python, PHP, SQL) featuring a centralized database of 14,000+ institutions. Utilized **BeautifulSoup** and **Pandas** for large-scale data scraping and preprocessing, implementing complex querying for geospatial and course-based filtering.

Key Achievements:

- Completed Internshala's Ethical Hacking Training with a perfect examination score of **100%** securing the title of **Top Performer**.
- Achieved a high-distinction score of **92.8%** on the EC-Council Certified Ethical Hacker examination.
- Managed a team of 15 freelancers to refine and enhance the data accuracy and reliability of the data scraped via "BeautifulSoup" for the "College Finder" project.
- Scored **195 out of 200** in the "Cyber Crime Awareness" exam, under Mission Shakti, UP Government.
- Successfully delivered the Advanced Dynamic Application Security Testing (DAST) project with high distinction (84%) during the **Tata Consultancy Services** internship. **[View Project]**

Personal Information:

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

Lead Auditor by discipline and certified ethical hacker by mindset - integrating governance, risk, and assurance to deliver secure, compliant, and resilient enterprises.

* * *