Shaswat Manoj Jha

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

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

Professional Synopsis:

A **Certified Ethical Hacker (CEH)** and **ISO/IEC 27001 Lead Auditor** with over **3 years of experience** in **Information Security**, specializing in **IT Internal & Integrated Audits** and **GRC (Governance, Risk Management & Compliance)**. Adept at executing engagements involving **ISMS**, **IT General Controls (ITGC)**, **IT Application Controls (ITAC)**, **Endpoint Data Leak Prevention (DLP)**, and **regulatory compliance** aligned with the **Digital Personal Data Protection Act (DPDP) 2023**, **NIST Cybersecurity Framework (CSF)**, and **ISO/IEC 27001**.

Possess a strong grasp of **cybersecurity principles**, **privacy regulations**, and frameworks such as **NIST RMF 800-37**, **PCI-DSS**, **ISO 22301**, and **ISO 31000**. **Known for a keen analytical eye and meticulous attention to control design, documentation, and policy drafting**, ensuring effective governance and risk mitigation across technology and business environments.

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.

Adept at developing **winning proposals, RFPs, comprehensive reports**, **audit documentation**, and **insightful presentations** that communicate technical findings with clarity. Passionate about continuous learning and innovation, with proficiency in **Generative AI**, **Web Application Penetration Testing**, **Power BI**, **Visio**, **Data Science**, **Big Data**, **SQL**, and working knowledge of **PHP**, **Python**, and **C++**.

Certifications:

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

Work Experience: Completed 3 Years on June '25

Full Time at	**Designation**	**From**	**To**
EY (Ernst & Young)	Consultant – Tech Risk Advisory	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

IT General Controls (ITGC) and Risk Management:

- ✓ Led **ITGC reviews** across **IAM**, **Change Management**, **IT Operations** (including **Backup & Recovery**) and **Physical Security**, executing **Test of Design (ToD)** and **Test of Operating Effectiveness (ToE)** to validate **control design and operating effectiveness** under **NIST CSF 2.0**, **SOX**, and **NIST SP 800-53**. Leveraged **Azure Active Directory**, **SailPoint**, **SIEM (Splunk)**, and **ITSM (ServiceNow)** to evidence **control design**, **operating effectiveness**, and **remediation**.
- ✓ Performed **integrated audits** mapping **IT controls** to **business processes** and **financial assertions**; documented **walkthroughs**, **control narratives**, **RACM**, **test scripts**, **sampling**, and **audit evidence** to support assurance conclusions.
- ✓ Reviewed and Improved **ISMS policies (User Access, Change, Acceptable Use, Asset Management, Incident Response, Business Continuity Policy (BCP), Disaster Recovery (DR), Cyber Crisis**

Management) with document control, versioning, and approval records, ensuring alignment to **ISO/IEC 27001:2022** and organizational objectives.

- ✓ Assessed **RPA** environments for **governance**, **credential vaulting**, **segregation of duties (SoD)**, **bot account** management, **logging, monitoring**, and **exception handling** for **ITGC compliance** and **change governance**.
- ✓ Assessed cloud security using **CIS Benchmarks**, validating **IAM, encryption, logging, segmentation, backup and DR per NIST CSF 2.0**.
- ✓ Established security governance through monthly **SteerCo** reviews by tracking key risk and performance indicators (**KRIs/KPIs**) and driving timely issue resolution achieving over 95% on-time closure.
- ✓ Conducted **gap analyses** against **NIST SP 800-53**, producing **maturity assessments**, **risk heatmaps** and **closure evidence** for prioritized **remediation**.

IT Application Controls (ITAC):

- ✓ Assessed **application controls** across **interfaces**, **input and edit checks**, **master data**, **report integrity**, **configurable parameters**, and **SoD** to ensure **accuracy**, **completeness**, and **authorized processing** (**C&A** assurance).
- ✓ Identified risks of **unauthorized data modification**; implemented **preventive and detective** measures (e.g., **maker–checker**, **field validation**, **audit trails**, **immutability**, **reconciliations**), and validated **parameter security** and **access restrictions**.
- ✓ Evaluated **automated controls** and **system configurations**; recommended design changes to reduce **manual intervention**, lower **control failure** probability, improve change management and strengthen the Software Development Lifecycle **(SDLC)**.
- ✓ Evaluated input fields to verify that critical data inputs are governed by appropriate validations and checks, ensuring data integrity and completeness.

Regulatory & Framework Compliance (RBI, IRDA, SAMA, DPDP etc.) and Internal Policy Adherence:

- ✓ Aligned **ISO/IEC 27001** implementations with **IRDAI and RBI** expectations; mapped controls to **NIST CSF 2.0** and **NIST SP 800-53** to demonstrate **regulatory coverage** and identify **residual risk**.
- ✓ Performed **SAMA Cybersecurity Framework (SAMA CSF) gap assessments** across **cybersecurity** and **IT governance** policies; tracked **remediation** to closure with **audit evidence** and **management sign-off**.
- ✓ Reviewed **applications and APIs** for **PII** exposure across **UI**, **logs**, and **reports**; verified compliance with **IRDAI** guidance and **India Digital Data Protection Act (DPDP 2023)** (e.g., **purpose limitation**, **data minimization**, **consent**, **retention**).
- ✓ Strengthened **BCP/DR** programs for **asset coverage**, **RTO/RPO** alignment, **backup and restore validation**, and periodic **drills and tabletop exercises**; captured **lessons learned** and **plan updates**.
- ✓ Operationalized policy adherence by converting policies into **testable checklists**, **sampling plans**, and **evidence requirements**; recorded **non-conformities** and **corrective actions** for **compliance** reporting.

Vendor / Third Party Risk Management:

- ✓ Executed **Third-Party Risk Management (TPRM)** assessments covering **SLA compliance**, **logical and physical security**, **data protection**, **incident notification**, and **sub-processor** oversight; identified **material gaps** and drove **remediation** with vendors.
- ✓ Conducted **on-site assessments** for **social-engineering exposure**, **media handling**, **endpoint DLP posture**, and **access provisioning and de-provisioning**, mitigating **data leakage** and **insider risk**.

PII Data Security, Endpoint Review and DLP Testing:

- ✓ Mapped **sensitive-data flows** across **users, systems and apps** on **Microsoft Visio**; evaluated **encryption in transit and at rest** (e.g., **TLS 1.2+**, **AES-256**, where applicable) and identified **leakage points** for targeted **controls**.
- ✓ Assessed **endpoint security** (laptops, desktops, thin clients), identified **DLP** control gaps, and recommended **policy/rule updates**, **device and port control**, **clipboard/print restrictions**, and **browser isolation**.

- ✓ Centralized endpoint hygiene via **asset inventory**, **patch management**, **DLP ruleset** deployment, and **Antivirus and Endpoint Detection and Response (EDR)** updates through **remote management**, with coverage and exception **dashboards** for **governance.**

Cybersecurity, Dynamic Application Security and Penetration Testing (DAST):

- ✓ Performed **automated and manual DAST** using **Burp Suite**, **OWASP ZAP**, and **SQLMap**; validated **OWASP Top 10** issues (**SQLi**, **XSS**, **IDOR**, **Broken Authentication, Access Control**, **Security Misconfiguration**, **Sensitive Data Exposure**) and captured **PoC** and **risk ratings (CVSS)**.
- ✓ Partnered with the IT team to **retest**, verify **fixes**, and implement **secure defaults** (**least privilege**, **CSRF protections**, **rate limiting**, **input sanitization**, **CSP and security headers**), updating **threat models** and the **risk register**.

Proposals, Reports and Documentation:

- ✓ Developed **client proposals** with **tailored scope**, **methodology**, **deliverables**, and **effort estimates**, leading to **awarded engagements** and clear **acceptance criteria**.
- ✓ Led **Business Impact Analyses (BIA)** and produced governance artifacts (**risk register**, **software and hardware asset inventories**, **lessons-learned log**, **endpoint testing templates**) to standardize **security operations**.
- ✓ Delivered **executive-ready reports with graphs and dashboards** (**PowerPoint**, **Power BI**) with **findings**, **risk ratings**, **prioritized recommendations**, and **roadmaps**, improving **stakeholder decision-making** and **remediation tracking**.

Trainings:

Training	Certification Body	Completion Date
Information Systems Audit, Controls and Assurance	The Hong Kong University of Science and Technology via Coursera	April 2024
Cybersecurity Management (5 Weeks)	Charles Sturt University	April 2023
Cybersecurity and Digital Forensics	Indian Institute of IT (IIT), Kota	November 2022
The Data Scientist's Toolbox	Johns Hopkins University via Coursera	August 2021
Cisco – Cybersecurity Essentials	Cisco Networking Academy	March 2021
Certified Network Security Specialist	International Cybersecurity Institute	February 2021
Ethical Hacking Training (8 Weeks)	Internshala Trainings	May 2020
Advanced Python Programming	College of Computer Ed., Jamshedpur	July 2019

Achievements:

- ➢ Achieved a perfect score of **100%** and got the title of "**Top Performer**" in Internshala's Hacking Training.
- ➢ Managed a team of 15 freelancers to refine and enhance the accuracy and reliability of the data scraped via "BeautifulSoup" for the "College Finder" project. (Described below in personal projects section)
- ➢ Scored **195 out of 200** in the "Cyber Crime Awareness" exam, under Mission Shakti, UP Government.
- ➢ Achieved 84% marks in the Advanced Dynamic Application Security Testing Internship project at Tata Consultancy Services. **[View Project]**

Notable Personal Projects:

- ➢ Developed a **PII scanner script** in Python during PII (Personally Identifiable Information) assessment for a client. This tool was designed to scan tens of gigabytes of logs and reports which included .txt, .pdf, and .xlsx files to find (PIIs) Personally Identifiable Information in them. It worked using regular expression (**RegEx**) patterns and the implementation of this script significantly **reduced the project timeline from weeks to days**.
- ➢ Conducted vulnerability testing on an eCommerce website using tools like Nmap, Burp Suite, SQL Map, and OWASP ZAP. Identified vulnerabilities such as SQL Injection, XSS & IDOR and drafted an industry-standard Vulnerability Assessment & Penetration Testing (VAPT) report with 126 pages. **[View Project]**

- Created a web platform "College Finder", using Python, BeautifulSoup, Pandas, SQL, and PHP. This platform provides complete details of over 14,000 colleges including complicated data such as distance from nearby colleges, list of colleges offering similar courses etc.
- Discovered a loophole in a popular resume builder website that allowed free users to access premium features like exporting resume. Reported the issue and was rewarded with a premium account.

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
- Self-Directed
- Proactive Initiator
- Googling Expert
- Selling & Negotiation
- Critical Thinking
- Innovative
- Project Ownership

Personal Information:

Date of Birth – 22nd November 2000
Current Address – Pune, Maharashtra
Preferred Location – Kolkata / Remote
Linguistic Abilities – English, Hindi & Maithili

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

* * *