Shaswat Manoj Jha

CEHv12 | ISO 27001 Lead Auditor

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

Professional Synopsis:

A Certified Ethical Hacker **(CEH), ISO 27001 Lead Auditor** and an experienced information security professional, specializing in **GRC (IT Governance, Technology Risk Management, and Regulatory Compliance)** audits. Successfully executed projects involving **ISMS**, **ITGC**, **ITAC**, **Segregation of Duty (SOD)**, **Data Leak Prevention (DLP)**, and regulatory compliance based on **Digital Personal Data Protection Act (DPDP) 2023, NIST 800-53,** and **ISO 27001**. Possess a comprehensive understanding of principles and requirements in **NIST RMF 800-37, PCI-DSS**, **ISO 22301** and **ISO 31000** frameworks.

Proactive problem solver dedicated to strengthening security measures in alignment with organizational security objectives to protect critical assets. Skilled in conducting audits, identifying risks, and providing actionable recommendations to ensure compliance with regulatory and industry standards.

I possess a strong understanding of client requirements and preferences, which has enabled me to tailor excellent service and maintain exceptional client satisfaction. Some of the major clients served include Niva Bupa Health Insurance, Max Life Insurance, Aditya Birla Health Insurance, IIFL Home Loans, Alliance Insurance Brokers and VFS Global.

Proficient in drafting information security policies and concluding audits/ assessments with detailed documentation with recommendations for remediation, contributing to the overall enhancement of IT security posture and compliance adherence. Driven by a commitment to continuous improvement, I am competent in Database Management System (DBMS), SQL, Data Science, configuring/maintaining SIEM systems and possess basic knowledge of PowerBI & programming languages like PHP, Python, C, and C++.

Career Objective:

I aim to leverage my interpersonal, management and technical skills to make a meaningful and high-quality contribution to the success of my organization. I'm seeking a vibrant and supportive work environment, where positivity thrives, challenges are embraced, and growth is a constant priority.

I firmly believe that my quick learning ability and consistent curiosity propels me forward in the field of Information Security and I'm looking for an organization that can provide me with ample opportunities to channel my skills allowing me to contribute to the advancement of the industry.

Work Experience:

➢ **Consultant 2 – IT Internal Audit** **June 2023 – Present**
at Protiviti

ITGC, Network Security, Cloud Security and Disaster Recovery Assessment:

- ✓ Conducted comprehensive IT security and compliance assessments across multiple domains, ensuring alignment with industry standards and regulatory requirements.
- ✓ Evaluated IT General Controls (ITGC) for critical applications, focusing on areas such as user access management, change management, backup management, incident management, and batch job monitoring.
- ✓ Enhanced data security measures through the implementation of data identification and classification policies, maintenance of data inventories, and controls over data at rest and in motion.
- ✓ Ensured system security through robust endpoint inventory maintenance, baselining of security configurations, antivirus controls, privileged identity management, and vulnerability management.
- ✓ Implemented cloud security frameworks, including identity and access management, cloud asset management, and vulnerability management, to safeguard data hosted on cloud platforms.
- ✓ Reviewed and enhanced the Business Continuity and IT Disaster Recovery (DR) plans, assessing their adequacy and conducting drills, simulations, and tabletop exercises to validate their effectiveness.

- ✓ Provided detailed documentation of assessment findings and recommendations for remediation, contributing to the overall enhancement of IT security posture and compliance adherence.

PII Assessment based on Indian Digital Personal Data Protection (DPDP) Act, 2023:

- ✓ Reviewed 120+ applications and APIs including their front-end, logs and reports for presence and accessibility of 62 different types of Personally Identifiable Information (PII).
- ✓ Plotted the availability of PIIs into a tabular matrix for a quick overview of PIIs in applications.
- ✓ **Validated generic accounts** for privileged access, ensuring necessary permissions and providing recommendations to avoid excessive privileges.
- ✓ Assessed employee endpoint systems for data leakage avenues, safeguarding sensitive PII from unauthorized extraction.

IT General Controls (ITGC), IT Application Controls (ITAC) and Information Security audit:

- ✓ Reviewed organization's adherence to **IT policies and procedures**.
- ✓ Reviewed vendor management and compliance to ensure service level agreements (SLAs) are met.
- ✓ Conducted **IT General Controls (ITGC)** review to assess information security and ensure compliance with industry standards and regulations.
- ✓ Evaluated IT operations, covering aspects like **backup management**, scalability, **patch management**, **change management**, antivirus controls, **data leak prevention (DLP)**, and **privileged user access management**.
- ✓ Assessed **IT Application Controls (ITAC)** for **user access management**, **change management**, software **functionality testing**, **business continuity** plan, **disaster recovery** plan, closure of past VAPT reports, customer data **(PII) security**, and log management/monitoring.

➢ **Senior Analyst** **June 2022 – June 2023**
at Nangia and Co.

Audit Based on NIST Cybersecurity Framework for IRDAI Compliance:

- ✓ Collaborated with the Chief Information Security Officer (CISO) to review the implementation of **ISO 27001** and tuned systems and controls to align the IT security with **IRDAI** guidelines.
- ✓ Enhanced the **Information Security Management System (ISMS)** by implementing controls such as system hardening, incident logging, capacity monitoring, multi-factor authentication, **password management** and **user access management**.
- ✓ Conducted endpoint reviews and tabletop exercises for incident management & disaster recovery.
- ✓ Drafted new and refined existing information security policies such as **Cyber Crisis Management**, **Disaster Recovery**, **Business Continuity**, **Change Management**, **Acceptable Use**, **Asset Management,** and **Incident Response** to meet regulatory (IRDAI) requirements.
- ✓ Conducted **Business Impact Analysis (BIA)** and designed frameworks such as risk register, software inventory, asset inventory, lessons learnt tracker and endpoint security testing template for enhanced security state of the organization.

Data Security Assessment, Endpoint Review and DLP Testing:

- ✓ Conducted a comprehensive review of internal applications, understanding the flow of data and identifying potential data leakage points.
- ✓ Identified procedural gaps through collaboration with department heads and ground staff to identify and mitigate risks of customer personally identifiable information (PII) leakage.
- ✓ Designed data flow diagrams in **Microsoft Visio**, visualizing end-to-end flow of customer PII across staff, systems, and applications, based on practical discussions with all departments.
- ✓ Physically inspected the telesales floor to identify social engineering vulnerabilities and other physical data leakage avenues.
- ✓ Assessed endpoint security on employee PCs, identifying several gaps in **Data Leak Prevention (DLP)** rulesets. Further, provided recommendations to prevent unauthorized data extraction.
- ✓ Conducted an on-site **vendor risk management** exercise, identifying significant gaps in the client's data security at the vendor.

IT General Controls (ITGC) and Segregation of Duty (SOD) audit:

- ✓ Identified gaps in **user access management** to mitigate risks of unauthorized access to critical internal applications and provided recommendations to enhance the design and effectiveness of existing **IT policies and controls**.
- ✓ Conducted internal audit of **change management**, **patch management**, **incident management**, **User Access Management (UAM)** and **Segregation of Duty (SOD)** controls.

➢ **Advanced Dynamic Application Security Testing Intern** **June 2020 to August 2020**
at Tata Consultancy Services (TCS)

- ✓ Worked on various manual Dynamic Application Security Testing (DAST) techniques and automated tools such as Burp Suite, SQL Map and OWASP Zap, to successfully identify and address security vulnerabilities in various web applications.
- ✓ Identified vulnerabilities such as SQL Injection, XSS, Broken Authentication, Broken Access Control, Security Misconfiguration, and Sensitive Data Exposure.
- ✓ Secured 84% marks in the final internship project assessment. **[View Project]**

Achievements:

- ➢ Scored **100%** marks and received the title of "**Top Performer**" in Internshala's Ethical Hacking Training.
- ➢ In pursuit of completing the "College Finder" project, managed a team of 15 freelancers to refine the data scraped via BeautifulSoup and enhance its accuracy and reliability.
- ➢ Scored **195 out of 200** in the "Cyber Crime Awareness" exam, under Mission Shakti, UP Government.

Notable Personal Projects:

- ➢ While working on a PII assessment engagement, created a PII Scanner script on Python. This automated tool was designed for scanning terabytes of text files including TXT, PDF, and Excel files, utilizes regular expression (RegEx) patterns to identify potential personally identifiable information (PII) in individual lines. The implementation of this script significantly reduced the weeks of work required for scanning application logs and reports by completing these scans within a few hours.
- ➢ Using tools such as Nmap, Burp Suite, SQL Map, Nikto and OWASP ZAP, tested an eCommerce website for vulnerabilities such as SQL Injection, XSS, IDOR & CSRF and drafted an industry-standard Vulnerability Assessment and Penetration Testing (VAPT) report of 126 pages. **[View Project]**
- ➢ Using Python, BeautifulSoup, Pandas, SQL and PHP, created a web platform "College Finder" which provides complete details of over 14000 colleges including complicated data such as distance from nearby colleges, list of colleges offering similar courses and other calculative data. **[View Project]**

Education:

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

Notable Trainings:

Training	Institution	Date
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

Certifications:

- Certified Ethical Hacker :: CEHv12 – EC Council (Score - 92%)
- ISO/IEC 27001 Lead Auditor – IRCA
- ISO/IEC 20000 IT Service Management Associate – SkillFront
- ISEA Certified Cyber Hygiene Practitioner – Ministry of Electronics & IT (MeitY), Govt. of India

Soft Skills:

- Team Leadership
- Self-Directed
- Proactive Initiator
- Googling Expert
- Selling & Negotiation
- Critical Thinking
- Innovative
- Accountable

Personal Information:

D.O.B – 22nd November 2000
Current Address – Kandivali, Mumbai, Maharashtra
Linguistic Abilities – English, Hindi & Maithili

* * *