# KARISHMA NEOLE

**Cybersecurity Professional**

📱 +91 9825045310/ +91 7984478768    ✉ karishma.neole12@gmail.com    🔗 linkedin.com/Karishmaneole

## 📑 Core Competencies

- Data Protection
  - Data Loss Prevention (DLP)
  - Digital Rights Management
  - Data Classification
  - Cloud Access Security Broker
  - Mobile Device Management
- Secure Access Service Edge (SASE)
- Zero Trust Network Access (ZTNA)
- Incident Response
- Web Application Security
  - PenetrationTesting (Web/API)
- Vulnerability Assessment
- Third-Party Risk Management
- Governance Risk Compliance
  - Audit Readiness (ISO 27001,SOC 2)
  - ITGC evaluations
  - Privacy (GDPR,DPDP)
- Security Awareness Training
- Security Monitoring & Reporting

## ⚙ Tools

- Microsoft Purview (MIP, DLP, IRM, eDiscovery)
- Microsoft Compliance Center
- Microsoft Defender Suite
- Forcepoint DLP
- Forcepoint ONE
- IRM (Seclore, Blackberry)
- Zscaler, Palo Alto Prisma
- CASB(Netskope)
- MDM (Microsoft Intune, BlackbBerry UEM)
- RSA Archer, ServiceNow GRC and JIRA
- Burp Suite, Metasploit, Nmap, Acunetix, AppScan,Linux
- PowerBI
- Trend Micro PhishSight

## 👤 Profile Summary

Cybersecurity professional with **6.5+ years of experience**, having delivered **data protection and compliance solutions** for **various Fortune 500 clients across sectors like Oil & Gas, Manufacturing, Agrochemical, Education, and Technology**. Successfully deployed **DLP, DRM, CASB, and MDM**, resulting in significant reduction in data leakage incidents, and **automating governance workflows** to enhance policy enforcement. Skilled in designing security programs aligned with **ISO 27001, SOC 2, HIPAA, GDPR**, achieving **near-continuous audit readiness and conducting ITGC reviews. Automated third-party risk assessments** via ServiceNow and RSA Archer**, cutting processing time by 60% and exceptions by 30%. Led cybersecurity awareness programs for 3,000+ users**, driving a 40% drop in phishing incidents. Delivered **executive dashboards** using Power BI and ServiceNow GRC, providing **real-time compliance insights**. Developed and enforce security policies and controls across cloud and on-premises environments. Lead penetration testing initiatives, conducting in-depth **risk assessments**, and implementing cloud security best practices to proactively identify, assess, and mitigate security threat. Strategic contributor to **Privacy by Design** and ongoing risk reduction efforts.

## 🎓 Education

- **2018: M.Tech. in Information and Network Security** (NIRMA University, Ahmedabad, Gujarat)
- **2016: B. Tech. in Information Security** (Gujarat Technical University Anand, Gujarat)

## 💼 Work Experience and Roles

| Times Internet (Times of India Group) Aug 2022 – Dec 2024, Delhi | Ernst & Young (EY LLP) May 2018 – Jul 2022, Mumbai | Oracle Pvt. Ltd (RGBU) May 2017–Apr 2018, Bengaluru |
|---|---|---|
| Application security Specialist | Senior Cybersecurity Consultant | Intern |
| Vulnerability management Application security ISO, SOC 2 Audit Readiness Third Party RiskAssessment Security Compliance | Data Protection Application security ISO SOC2 Audit compliance End user Awareness GRC & Incidence Response | Tool Development Batch Automation Database migration Data Validation Customer Support |

## 🎗 Certifications

- EC Council - Certified Ethical Hacker (CEHv10)
- Microsoft 365 Security Administrator (MS-500)
- EC Council – Certified Security Analyst (ECSAv10)
- ISO 27701

## 🏆 Achievements

- Recipient of the "Kudos Award" at Ernst & Young for outstanding contributions to project success and team excellence.
- Honored with the EY Exceptional Award in recognition of delivering exceptional performance and exceeding organizational expectations.
- Received Client Appreciation Letter for delivering exceptional project results and consistently surpassing client expectations.

# 🎯 Key Result Areas

**Data Protection Strategy**:
- Evaluated and deployed data protection strategies tailored to client-specific risks and compliance mandates (GDPR, HIPAA, ISO 27001), enhancing overall data control posture.
- Designed and implemented data classification frameworks and metadata tagging policy-based automation, reducing manual intervention by 60% & audit traceability.
- Collaborated with Legal, Privacy, Risk, and Business Units to align data protection governance models and ownership responsibilities.

*Data protection roadmap | Data Classification Policy & framework | RACI Matrix for Data Protection | DLP Exception SOP & Approval Workflow |Data Protection Maturity Benchmarks | Data Loss Prevention KPI metrics*

**Technology Deployment:**
- End-to-end deployment of enterprise-grade DLP, CASB, DRM, and MDM solutions across hybrid environments spanning APAC, India, AMEA, and Asia, securing sensitive data against insider threats, cloud misconfigurations, and endpoint leakage.
- Enabled CASB integrations (Netskope, Microsoft Defender for Cloud Apps) to monitor and control unsanctioned SaaS usage, reducing shadow IT exposure by 60% and enforcing inline controls across platforms such as OneDrive, Slack, and Google Drive.
- Deployed MDM policies (Intune, Blackberry UEM) to enforce encryption, secure containerization, and remote wipe capabilities across 100% of mobile endpoints.
- Delivered tailored CSPM recommendations, aligning DLP and CASB with AWS and Azure native controls, achieving near-complete encryption-at-rest compliance.
- Conducted UAT, policy tuning, to ensure seamless adoption with minimal false positives.
- Integrated deployed controls with GRC platforms (ServiceNow, JIRA) for real-time compliance visibility and reported key metrics, incident trends, and roadmap performance to executive steering committees.

*Implementation plan & Deployment Runbooks (per tool) |Tool Assessment Report | Policy approval workflow | Use Case-to-Policy Mapping | Policy Enforcement Dashboard | Shadow IT discovery and app risk scoring | MDM Enrollment SOP | BYOD Policy | End-User DRM Training | Real-time Metrics Dashboard | Incidence Response Playbook | Compliance monitoring*

**Governance, Risk Assessment & Compliance Oversight**:
- Conducted comprehensive data flow and risk assessments across 126 departments globally, identifying vulnerabilities through configuration reviews, policy assessments, and ITGC evaluations.
- Performed current vs. desired state assessments, identifying and mapping control gaps against ISO 27001, NIST CSF, GDPR, and SOC 2 requirements.
- Led pre-audit readiness for ISO 27001 and SOC 2, covering all 14 ISO control domains and SOC 2 Trust Criteria, driving risk remediation and compliance alignment.
- Coordinated with 10+ control owners to streamline evidence collection, reducing documentation gaps by >90% and improving audit SLA adherence from 70% to 98% via ServiceNow GRC automation.

*Compliance Mapping Reports | Risk register | Audit readiness status dashboards | Control Implementation Plans | audit-ready documentation (policy,SOPs) | Automated Evidence Collection | Automated TPRA workflow | Data Flow Analysis |Asset Inventory*

**Vulnerability Management & Penetration testing:**
- Led manual web application and API penetration testing, identifying and validating high-risk vulnerabilities aligned with OWASP Top 10 and CVE benchmarks, leveraging tools such as Burp Suite, Nmap, Acunetix, AppScan, ZAP, and Wireshark.
- Delivered comprehensive vulnerability assessment reports with critical risk insights, custom remediation guidance,directly contributing to improved security posture and compliance readiness.
- Collaborated cross-functionally with engineering and infrastructure teams to track, prioritize, and remediate findings via centralized dashboards, improving remediation SLA adherence and reducing the open vulnerability backlog by over 50% within two quarters.

*vulnerability assessment report | Vulnerability Remediation Tracker (Excel/JIRA/ServiceNow) | Monthly Progress Dashboards*

**Security Awareness and Training Programs:**
- Designed and led enterprise-wide cybersecurity awareness programs covering over 3,000 users across APAC, AMEA, and India, customized by department, role, and risk profile.
- Developed interactive training modules and deployed simulated phishing exercises using TrendMicro Phish Insight, resulting in a 40% reduction in phishing click rates within two quarters.
- Created awareness dashboards and end user training compliance reports, achieving a >95% completion rate across all business units within defined compliance timelines.
- Integrated cybersecurity awareness into onboarding programs and annual compliance training, ensuring 100% coverage of new hires and re-certifications.
- Launched ongoing "Secure Work Culture" campaigns, including posters, infographics, quizzes, and mailers, driving user engagement and reinforcing secure behaviors across business functions.
- Delivered role-based training across 126 departments to support the enterprise rollout of Data Classification, MDM, and DRM solutions, ensuring seamless adoption with minimal business disruption.
- Conducted post-training knowledge assessments, identified awareness gaps, and deployed targeted re-training programs, improving knowledge retention scores by 20%

*Training Schedule, Campaign Plan | Phishing Campaign Report | Training Dashboard (Power BI / Excel) | BU-wise Compliance Tracker*

**Executive Reporting:**
- Developed and delivered interactive, executive-level security dashboards, providing real-time visibility into risk posture, policy performance, and compliance KPIs for senior leadership decision-making.