Kunal Malhotra

Cybersecurity & Technology Risk Professional

099107 08715 | kunalmalhotra@gmx.com | New Delhi, Delhi, India

PROFESSIONAL SUMMARY

I am a results-driven leader who thrives in high-pressure environments & inspires teams with a “never-give-up, get-it-done” attitude. With over 12 years of experience in cybersecurity, technology risk, & governance, I have built a reputation for fostering collaboration & motivating teams to tackle complex challenges head-on. Whether developing strategies, leading initiatives, or managing risk, I maintain a relentless focus on delivering impactful outcomes. For details on my projects and the sectors I've worked in, please visit my website.

SKILLS

Risk Transformation | IT Audit & Assurance | Security Architecture | Strategy & Governance | Threat Risk Assessments | Data Privacy & Compliance | Cyber Maturity Assessments | Business Continuity Planning | Third Party Risk Management

STANDARDS

Regulations & Acts	GDPR | CCPA | PIPEDA | HIPAA | COPPA | SOX 404 | GLBA | FISMA | CISA | RBI | NESA | FFIEC | OCC
Industry Standards & Frameworks	ISO 27001 | PCI DSS | NIST CSF | SOC | COBIT | COSO | CIS | HITRUST | ITIL

EDUCATION

POST GRADUATION IN CYBERSECURITY

Massachusetts Institute of Technology, 2023

BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE

Bharat Institute of Technology, 2012

EXPERIENCE

DIRECTOR - CYBERSECURITY & TECHNOLOGY RISK

CYTERICO — August 2023 - Present

- Leading a start-up venture, demonstrating an entrepreneurial spirit, overseeing initial operations, implementing strategic plans, setting up a team, managing resources, & establishing key partnerships.
- Spearheading the development & execution of a comprehensive cybersecurity & technology risk management practice across multiple sectors, aligning risk strategies with organizational goals to enhance operational resilience.

- Driving the development of an AI-powered solution that transforms business processes for enterprises & professional services, leveraging autonomous AI agents to enhance accuracy, reduce costs, & shorten timelines.
- Developing & implementing tailored ERM frameworks for clients, ensuring compliance with international standards & driving risk culture within client organizations.

MANAGER - CYBERSECURITY STRATEGY & GOVERNANCE

KPMG Canada — December 2022 - May 2023

- Delivered an engagement focused on data privacy & vendor risk mitigation for an airport authority, ensuring PIPEDA compliance & enhancing data governance by classifying sensitive data, evaluating vendor security, & implementing a risk-based approach to prevent future breaches.
- Built & maintained strong relationships with the clients to understand their cyber security needs and challenges & provided them with expert advice & solutions.
- Led a cyber maturity benchmark for education sector institutions, comparing their security posture against peers within the same country, province, & city, and provided insights to help the client align with NIST CSF standards and enhance their governance framework.
- Led a cybersecurity enhancement project for critical OT systems in the energy sector, assessing maturity, identifying risks, & validating security controls against NERC CIP, NIST CSF, & ISO 27001 standards.
- Conducted a security architecture assessment for state infrastructure, identifying gaps in the current posture and providing a roadmap to implement controls that would strengthen critical infrastructure & enhance overall security resilience.
- Contributed to the development & execution of cyber security go-to-market strategy, including developing marketing materials, participating in client pitches, & building relationships with potential clients.
- Spearheaded resource allocation & developed key performance indicators to effectively monitor team performance. Led weekly partner meetings to review team outcomes, & drive discussions around career progression & promotion cycle.

MANGER | OFFSHORE LEAD - GOVERNANCE, RISK & COMPLIANCE

HCL Technologies — October 2021 - September 2022

- Offshore leader leading a team of consultants and managers in the GRC consulting practice, delivering engagements for global clients. Oversaw offshore operations, ensured high-quality outcomes, client satisfaction, & effective project execution, while mentoring team members & driving continuous improvements in service delivery.
- Collaborated with the executive team onshore to create proposals & submit bids for new business opportunities, contributing to business growth & ensuring alignment with client needs.
- Delivered a TPRM engagement for a major UK pharmaceutical client using Process Unity as the GRC tool. Assessed third-party vendor risks, conducted due diligence, & identified compliance gaps related to GDPR & NIST frameworks, providing actionable recommendations to mitigate risks & ensure vendor compliance with industry standards.
- Led an engagement for a major US bank to assess IT controls for SOX 404 compliance. Focused on testing the effectiveness of controls related to financial reporting & supported the IT transformation by updating the internal control framework to align with new IT processes & regulatory requirements.

SENIOR CONSULTANT - CYBERSECURITY

EY India — July 2019 - October 2021

- Led multiple projects with banks across India & internationally to conduct gap assessments in compliance with the Reserve Bank of India's Master Direction on Digital Payment Security Controls, ensuring alignment with regulatory standards.
- Redesigned Program Governance frameworks for a GCC client in India, which is a top-tier bank in the US, to enhance risk management, oversight, & operational efficiency, driving compliance & fostering sustainable growth in digital banking operations.
- Conducted a TPRM benchmarking assessment for a financial services client, evaluating processes against OCC guidelines, NIST CSF, ISO 27001, & industry peers, identifying compliance gaps & inefficiencies, & delivering a roadmap with actionable recommendations to enhance TPRM maturity & mitigate third-party risks.
- Advised one of the largest Investment Funds in the UAE on strengthening business continuity & resilience frameworks, conducting risk assessments, & aligning disaster recovery & crisis response strategies with global best practices.
- Reviewed & redesigned policies & procedures for clients across multiple regions, ensuring compliance with local regulations & industry best practices. Streamlined processes to improve efficiency, mitigate risks, & support long-term business growth.
- Designed & implemented a comprehensive set of Security Metrics, KRIs, & KPIs for a leading bank in the UAE, enhancing

cybersecurity monitoring, risk assessment, & regulatory compliance, while improving incident response times & aligning security.

- Conducted BIA interviews & documented BIA reports for a client, defining high-level recovery strategy principles & identifying key recovery strategies.
- Reviewed existing processes, current automation, environment, controls, & governance, providing short- term & medium-term improvement recommendations for one of the UK's largest banks. Collaborated with a London based consulting team to redesign their cybersecurity framework, drafting EPICs & user stories to support the transformation.
- Led end-to-end IT audits for multiple small finance banks in India, assessing the effectiveness of internal controls, risk management processes, & IT governance to ensure compliance with industry regulations & standards.
- Conducted comprehensive data center audits for banks, evaluating infrastructure security, disaster recovery protocols, & data integrity to ensure optimal performance & regulatory adherence.
- Engaged in a consulting project for a Fortune 500 bank in the GCC region, based in India, acting as the BIRO to assess & enhance data governance, risk management, & compliance frameworks, ensuring alignment with global standards & regulatory requirements.
- Worked on various proposals in diversified verticals for clients in the financial services sector, created POVs for CXO leadership workshops with senior executives from several GCCs participating, & submitted bids in person by traveling to different cities for multiple clients.

HEAD OF IT AUDIT - RISK & COMPLIANCE

axio August 2018 - June 2019

- As Head of Risk & Compliance, led the design & deployment of the Internal Audit & governance framework, establishing robust audit & security processes across all IT operations within the organization.
- Formulated the Risk Register for all critical applications & products, conducted gap analyses, & designed an Internal Controls Framework, ensuring the identification & mitigation of control deficiencies.
- Established audit frequency & risk assessment protocols for the IT environment, including applications, databases, & infrastructure, to ensure ongoing compliance & risk management.
- Directed both in-house & outsourced resources in audit planning & execution, reviewed audit findings, & collaborated with the Chief Risk Officer to finalize reports with actionable mitigation recommendations.

DEPUTY MANAGER - FINANCIAL REPORTING & ACCOUNTING

AXA XL October 2016 - July 2018

- Played a key role in aligning internal controls with the newly implemented IT architecture as part of the organization's IT transformation, ensuring compliance with SOX 404 & evolving regulatory standards.
- Managed & executed controls testing for financial reporting systems, ensuring compliance with SOX 404 regulations, & designed & implemented control procedures to assess the effectiveness of IT controls in safeguarding financial data.
- Collaborated with stakeholders across Finance, IT, Risk, Underwriting, Claims, & Internal Audit to gather inputs, align departmental goals, & streamline control assessment & testing processes.
- Conducted comprehensive risk assessments of financial data processing systems to identify control gaps & implemented mitigation plans to address weaknesses in design & operational effectiveness of financial & IT controls.
- Maintained a comprehensive RACM to assess & document potential risks, including financial, operational, IT, fraud, regulatory, & reputational, & mapped corresponding control measures to ensure effective risk mitigation.
- Tested the design & operational effectiveness of critical controls, including user access management, change management, data integrity, & reconciliation processes.
- Reconciled financial transactions across systems & the General Ledger, ensuring data accuracy & completeness, while conducting code reviews to verify the reporting tool's accuracy and ensure data from MDM aligned with the financial records.
- Coordinated with external auditors PwC & the internal audit team to ensure alignment on control testing & minimize redundancies, providing real-time support during audit processes, including testing & documentation review.
- Updated control documentation to reflect changes in business processes, regulatory requirements, & the IT transformation, ensuring internal controls were designed in accordance with best practices & compliance standards.
- Conducted interviews & walkthroughs with key business stakeholders to understand control implementation & operationalization, providing guidance & training to internal teams on SOX compliance & effective control management.
- Managed both automated & manual testing of controls, including system-generated reports & reconciliation processes, ensuring data accuracy & consistency across financial systems.
- Prepared detailed reports for senior management & the MCO, outlining testing results, control effectiveness, & any recommended actions for strengthening internal controls.

CONSULTANT – INFORMATION PROTECTION & BUSINESS RESILIENCE

KPMG Global Services January 2016 - October 2016

- Conducted IT compliance assessments & issues remediation for Information Security, Business Resilience, & ITGC control testing, performing gap assessments for major clients, & recommending the implementation of ISO 27001:2013, NIST 800-53, FFIEC, & GLBA controls through mapping to meet business security requirements.
- Performed control mapping & gap analysis using industry-standard HIPAA for a large pharmaceutical client, reviewing IT policies & procedures to ensure alignment with best practices. Documented test plans, gap logs, & evidence in work papers.
- Led the development of secure software guidelines, database monitoring, & data masking strategies, evaluating technologies, processes, & vendors. Assessed service contracts (SOW & SLA) & identified optimal value propositions for clients.
- Researched & documented security recommendations, designed risk control matrices based on control objectives, & performed control testing.
- Conducted meetings with client & service organizations to discuss gaps, findings, & recommended actions for remediation. Conducted SOX 404 testing for the design & effectiveness of controls for a leading UK bank using the Archer tool, ensuring compliance with regulatory requirements & identifying control deficiencies for remediation.

IT SERVICE DELIVERY ANALYST – INFORMATION SECURITY & RISK MANAGEMENT

Xerox Technology January 2015 - December 2015

- Led SOX 404 audit program through an offshore delivery center, building a high-performing team & enhancing vulnerability management across technology areas.
- Supported ISO 27001-aligned risk management practices, overseeing Patch Management for Xerox applications, databases, & servers, while managing third-party supplier access controls.
- Conducted BIA, tracked End-of-Life IT assets, & supported disaster recovery drills to ensure continuity of critical systems & compliance with corporate security standards.
- Monitored & ensured regulatory compliance for ESAP systems by conducting weekly user account & access reviews & publishing monthly reports for the governance team on key business initiatives.
- Managed incident response & vendor assessments, mentored new associates, & collaborated with cyber intelligence analysts & IT professionals to address security risks & optimize threat mitigation efforts.

SENIOR BUSINESS ANALYST

300 Plus Consultant July 2012 - January 2015

- Under the capacity of a Project Manager for a publishing client, I led & managed critical information security assessments. Ensured alignment with security goals & regulatory standards, while overseeing timelines, deliverables, & scope.
- Consolidated application & infrastructure vulnerabilities into a unified, risk-focused view to guide senior management's decision-making on risk mitigation & remediation strategies.
- Reviewed threat & vulnerability assessments for one of the largest Human Capital & Reinsurance Solutions clients in the UK.
- Oversaw daily operations of client data centres, ensuring optimal uptime, efficient resource utilization, & effective capacity planning.
- Collaborated with the client to implement disaster recovery & business continuity strategies, ensuring secure & efficient data management practices tailored to client-specific needs.
- Utilized advanced statistical & database management skills to create detailed reports & analyze financial statements, market conditions, & regulatory limits (e.g., SEC filings such as DEF 14A, 8-K, & 10-K) for a global consulting & market research client.
- Conducted secondary market research, scanning financial market updates & industry analyses, & worked with client counterparts to enhance studies & publications.
- Ensured that research outcomes directly informed & influenced client business strategies by providing actionable insights based on ongoing market monitoring.
- Developed & enhanced client-facing web applications, writing JSP & Servlets to add functionality based on customer requirements.
- Created user interfaces using JSP, JavaScript, HTML, & CSS, leveraging J2EE design patterns for business logic, delivering both new & enhanced applications tailored to client specifications.