MOORE

THREAT DETECTION PREVENTION AND RESPONSE

Transform your business to withstand the challenges of modern threat landscape

Vulnerability assessment and penetration testing (VAPT)

In today's rapidly evolving digital landscape, organisations face an ever-expanding array of cyber threats that can compromise their critical assets, operations, and reputation. As cyber attackers become increasingly sophisticated, traditional security measures are no longer sufficient to protect against potential vulnerabilities and exploits.

What is vulnerability assessment and penetration testing (VAPT)?

Vulnerability and penetration assessment is a comprehensive approach to identifying, evaluating, and addressing potential weaknesses in an organisation's IT infrastructure, applications, and networks. This process involves two key components:

1. **Vulnerability assessment (VA):** A systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and often recommends steps to address them.
2. **Penetration testing (PT):** Also known as "ethical hacking," this is an authorised simulated cyberattack on a computer system, performed to evaluate the security of the system. The goal is not just to find vulnerabilities, but to actively exploit them to determine the potential real-world impact.

How VAPT enhances security posture?

By incorporating regular vulnerability and penetration assessments into your cybersecurity strategy, you can significantly enhance your organisation's security posture:

1. **Proactive threat identification:** Detect potential vulnerabilities before malicious actors can exploit them.
2. **Risk prioritisation:** Understand which vulnerabilities pose the greatest risk, allowing for efficient allocation of security resources.
3. **Security control validation:** Verify the effectiveness of existing security measures and identify areas for improvement.
4. **Compliance support:** Meet regulatory requirements and industry standards for security assessments.
5. **Security awareness:** Increase organisational understanding of potential security weaknesses and attack vectors.

Why is VAPT important?

In an era of increasing cyber threats, vulnerability and penetration assessment has become crucial for several reasons:

1. **Evolving threat landscape:** As cyber threats become more sophisticated, regular assessments help organisations stay ahead of potential attackers.
2. **Cost-effective security:** Identifying and addressing vulnerabilities early is far less costly than dealing with the aftermath of a successful cyberattack.
3. **Maintaining stakeholder trust:** Demonstrating a proactive approach to cybersecurity helps maintain the confidence of customers, partners, and regulators.
4. **Continuous improvement:** Regular assessments provide insights that drive ongoing enhancements to an organisation's security posture.

The rising tide of cyber threats

Recent years have witnessed a surge in high-profile cyberattacks, underscoring the critical importance of robust vulnerability management:

- In 2022, the uber data breach facilitated by social engineering tactics, compromised the company's internal systems and exposed sensitive financial data, highlighting the importance of comprehensive security assessments that include human factors.
- In 2021, the colonial pipeline ransomware attack disrupted fuel supplies across the eastern United States, highlighting the potential for cyber incidents to impact critical infrastructure.
- In 2020, the SolarWinds supply chain attack compromised numerous government agencies and private sector organisations, demonstrating the far-reaching consequences of sophisticated cyber espionage campaigns.

These incidents serve as stark reminders of the potential consequences of unaddressed vulnerabilities in organisational IT ecosystems.

Market trends and statistics

The global vulnerability assessment market is experiencing rapid growth, reflecting the increasing recognition of its importance:

- The vulnerability assessment market is projected to reach $18.7 billion by 2026, growing at a compound annual growth rate of 6.3% from 2021 to 2026.
- According to a study by Ponemon Institute, organisations that conduct regular VAPT are 40% less likely to experience unplanned downtime compared to those that did not.

Our approach to VAPT

Our IT & Cybersecurity team offers a comprehensive approach to vulnerability and penetration assessment, leveraging cutting-edge tools and methodologies to fortify your digital defences:

Scope definition and planning

- Collaborate with stakeholders to define assessment objectives
- Identify critical assets and systems for evaluation
- Develop a tailored assessment strategy aligned with your risk profile

Vulnerability scanning

- Utilise advanced scanning tools to identify potential vulnerabilities
- Assess network devices, servers, applications, and cloud infrastructure
- Prioritise vulnerabilities based on severity and potential impact

Penetration testing and exploitation

- Conduct in-depth manual testing to validate and expand upon automated scan results
- Attempt to exploit identified vulnerabilities to determine real-world risk
- Assess the effectiveness of existing security controls

Social engineering assessment

- Evaluate human-centric vulnerabilities through simulated phishing campaigns
- Assess employee awareness and adherence to security policies

Reporting and remediation planning

- Provide detailed reports outlining identified vulnerabilities and their potential impact
- Offer prioritised remediation recommendations and actionable insights
- Collaborate on developing a comprehensive remediation roadmap

Continuous monitoring and re-assessment

- Implement ongoing vulnerability management processes
- Conduct regular re-assessments to ensure continued resilience against evolving threats

Benefits of our vulnerability assessment and penetration testing (VAPT) services

By partnering with our team, your organisation can:

- Gain a comprehensive understanding of your current security posture
- Identify and address critical vulnerabilities before they can be exploited
- Enhance compliance with industry regulations and standards
- Strengthen your overall cybersecurity strategy and resilience
- Demonstrate a proactive approach to security, bolstering stakeholder confidence

In an era where cyber threats are constantly evolving, vulnerability and penetration assessments have become an essential component of a robust cybersecurity strategy. By leveraging our expertise and advanced methodologies, your organisation can stay one step ahead of potential attackers, safeguarding your critical assets and maintaining the trust of your stakeholders.

Phishing simulation

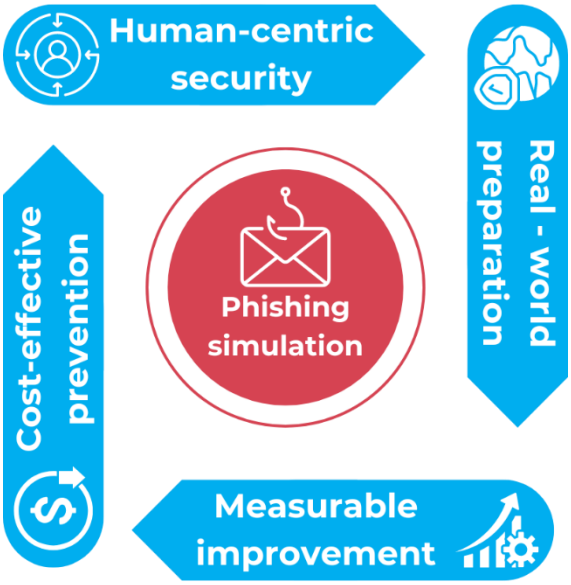
In today's interconnected digital landscape, phishing attacks have emerged as one of the most pervasive and damaging cyber threats facing organisations. These sophisticated social engineering tactics exploit human vulnerabilities, bypassing even the most robust technical defences. As cyber criminals refine their techniques, organisations must adopt proactive measures to strengthen their first line of defence – their employees.

Understanding phishing simulation

Phishing simulation is a controlled, ethical exercise that mimics real-world phishing attempts to assess and improve an organisation's resilience against social engineering attacks. By simulating various phishing scenarios, organisations can

- Evaluate employee awareness and susceptibility to phishing attempts;
- Identify vulnerabilities in existing security protocols; and
- Provide targeted training to enhance overall cybersecurity posture.

Why phishing simulation matters



1. **Human-centric security:** While technical defences are crucial, humans remain the most vulnerable link in the security chain. With 95% of cybersecurity breaches caused by human error, phishing simulations address this critical aspect of cybersecurity.
2. **Real-world preparation:** By exposing employees to realistic phishing scenarios in a controlled environment, organisations better prepare their workforce for actual attacks. This is crucial as 97% of people cannot identify a sophisticated phishing email.
3. **Measurable improvement:** Regular simulations provide quantifiable data on an organisation's improving resilience against social engineering tactics. Studies show that phishing simulation training can reduce click rates on malicious links by up to 50%.
4. **Cost-effective prevention:** The cost of conducting phishing simulations and awareness training is significantly lower than the potential financial and reputational damage of a successful phishing attack, which can average $4.91 million per incident.

The growing phishing threat

Recent incidents highlight the persistent and evolving nature of phishing attacks:

- In 2024, Arup, a multinational engineering firm, fell victim to a sophisticated deepfake phishing scam. Cybercriminals used AI-generated video and audio to impersonate a senior executive in a video call, convincing an employee to transfer $25 million to fraudulent accounts. This incident underscores the emerging threat of AI-enhanced social engineering attacks.
- In 2023, a major phishing campaign targeting Microsoft 365 users employed AI-generated voices in vishing (voice phishing) attacks, demonstrating the increasing sophistication of social engineering tactics.
- According to Trend Micro's 2023 report, over 30 million phishing URLs were detected globally, with the United States, Japan, and Brazil being the top targeted countries.
- A 2023 study revealed that 94% of organisations experienced at least one phishing attack, with 83% facing multiple attacks throughout them.

These incidents serve as stark reminders of the evolving nature of phishing threats and the critical importance of comprehensive security awareness training and advanced phishing simulations.

Market trends and statistics

The increasing recognition of phishing as a critical threat is reflected in market trends:

- Phishing attempts increased by 173% in the first half of 2023 compared to the same period in 2022.
- Business email compromise (BEC) attacks rose by 81% from 2022 to 2023, demonstrating the growing sophistication of targeted phishing campaigns.
- The top 10 most spoofed brands in phishing attacks include Microsoft, Google, Apple, highlighting the focus on impersonating trusted entities.
- The global security awareness training market, which includes phishing simulation, is projected to reach $10 billion by 2027, growing at a compound annual growth rate of 13% from 2020 to 2027.

Our phishing simulation approach

Our IT & Cybersecurity team offers a comprehensive phishing simulation service designed to strengthen your organisation's human firewall:

Assessment and planning

- Evaluate current security awareness levels
- Define simulation objectives and success metrics
- Design tailored phishing scenarios relevant to your industry and organisation

Campaign execution

- Deploy diverse phishing simulations (email, SMS, voice)
- Utilise advanced techniques mimicking real-world threats
- Monitor real-time employee responses and interactions

Analysis and reporting

- Compile detailed reports on simulation results
- Identify high-risk individuals and departments
- Analyse trends and patterns in employee behaviour

Targeted training

- Deliver immediate, contextual education for employees who interact with simulated phishing attempts
- Provide comprehensive security awareness training based on simulation results
- Offer role-specific training for high-risk positions

Continuous improvement

- Conduct regular simulations to reinforce learning
- Adjust scenarios based on emerging threats and previous results
- Track improvements in employee performance over time

Benefits of our phishing simulation services

By partnering with our team, your organisation can:

- Significantly reduce susceptibility to phishing and social engineering attacks
- Foster a culture of cybersecurity awareness throughout the organisation
- Comply with industry regulations requiring security awareness training
- Demonstrate a proactive approach to cybersecurity to stakeholders
- Continuously adapt to evolving phishing tactics and threats

In an era where a single click can compromise an entire organisation, phishing simulations have become an indispensable tool in the cybersecurity arsenal. By leveraging our expertise in phishing simulation, your organisation can transform its employees from potential vulnerabilities into a formidable human firewall, capable of recognising and thwarting even the most sophisticated social engineering attempts.

Cyber risk assessment

In an era where digital transformation drives business innovation, organisations face an ever-evolving landscape of cyber threats. A robust cyber risk assessment is no longer a luxury—it's a critical necessity for safeguarding your digital assets, maintaining operational continuity, and preserving stakeholder trust.

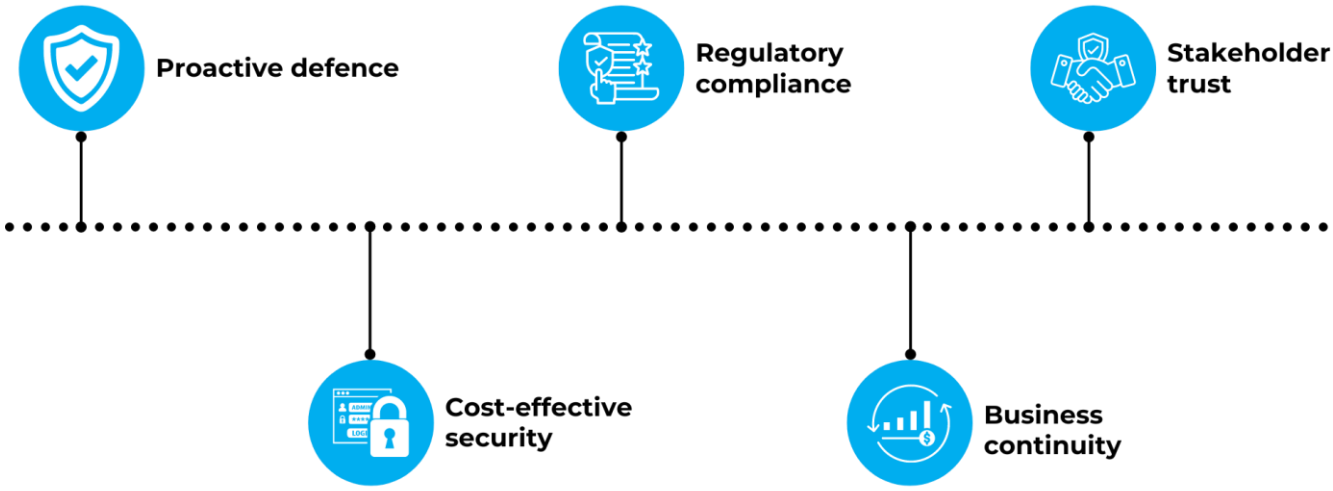
Understanding cyber risk assessments

Cyber risk assessment is a systematic process of identifying, analysing, and evaluating potential cybersecurity threats and vulnerabilities within an organisation's IT infrastructure.

This comprehensive approach enables businesses to:

- identify and prioritise critical assets and data;
- recognise potential threats and vulnerabilities;
- assess the potential impact of cyber incidents; and
- develop targeted strategies for risk mitigation.

Why cyber risk assessment matters



1. **Proactive defence:** In 2024, the average time to detect and contain a data breach is 204 days. Regular risk assessments help identify vulnerabilities before they can be exploited, significantly reducing this timeframe.
2. **Cost-effective security:** The average cost of a data breach reached $4.45 million in 2023. Investing in risk assessments and targeted mitigation strategies is far more cost-effective than dealing with the aftermath of a cyber incident.
3. **Regulatory compliance:** With the increasing focus on data protection regulations like GDPR and CCPA, regular risk assessments are crucial for maintaining compliance and avoiding hefty fines.
4. **Business continuity:** By identifying and addressing potential cyber risks, organisations can ensure operational resilience and minimise downtime in the event of an incident.
5. **Stakeholder trust:** Demonstrating a commitment to robust cybersecurity through regular risk assessments helps maintain the trust of customers, partners, and investors.

In a digital landscape where, cyber threats are constantly evolving, a comprehensive cyber risk assessment is the foundation of a resilient cybersecurity strategy. By leveraging our expertise in cyber risk assessment, your organisation can navigate the complex threat landscape with confidence, safeguarding your digital assets and maintaining a competitive edge in the digital age.

The evolving cyber threat landscape

Recent trends and statistics underscore the urgent need for robust cyber risk assessments:

- According to CrowdStrike's 2024 Global Threat Report, there was a 95% increase in cloud exploitation cases in 2023, highlighting the growing risks associated with cloud infrastructure.
- The first half of 2024 saw a 37% increase in weekly cyberattacks per organisation compared to the same period in 2023, as reported by Check Point Research.
- Qualys' 2024 Midyear Threat Landscape Review revealed a 76% surge in critical vulnerabilities during the first half of 2024, emphasising the importance of continuous vulnerability assessment.

Our cyber risk assessment approach

Our IT & Cybersecurity team offers a comprehensive cyber risk assessment service designed to fortify your organisation's digital defences:

Asset identification and valuation

- Catalogue critical IT assets, systems, and data
- Assess the value and sensitivity of each asset

Threat analysis

- Identify potential internal and external threats
- Evaluate the likelihood of various attack scenarios

Vulnerability assessment

- Conduct thorough scans of network infrastructure and applications
- Identify and categorise existing vulnerabilities

Impact analysis

- Assess the potential financial, operational, and reputational impact of cyber incidents
- Evaluate regulatory and compliance implications

Risk evaluation and prioritisation

- Quantify and prioritise identified risks based on likelihood and potential impact
- Develop a risk heat map for clear visualisation of the threat landscape

Mitigation strategy development

- Recommend tailored risk mitigation strategies
- Propose cost-effective security controls and measures

Continuous monitoring and reassessment

- Implement ongoing risk monitoring processes
- Conduct periodic reassessments to address emerging threats

Benefits of our cyber risk assessment services

By partnering with our team, your organisation can:

- Gain a comprehensive understanding of your current cybersecurity posture
- Make informed decisions about resource allocation for cybersecurity initiatives
- Enhance compliance with industry regulations and standards
- Demonstrate due diligence to stakeholders and regulators
- Develop a proactive approach to cybersecurity, staying ahead of emerging threats

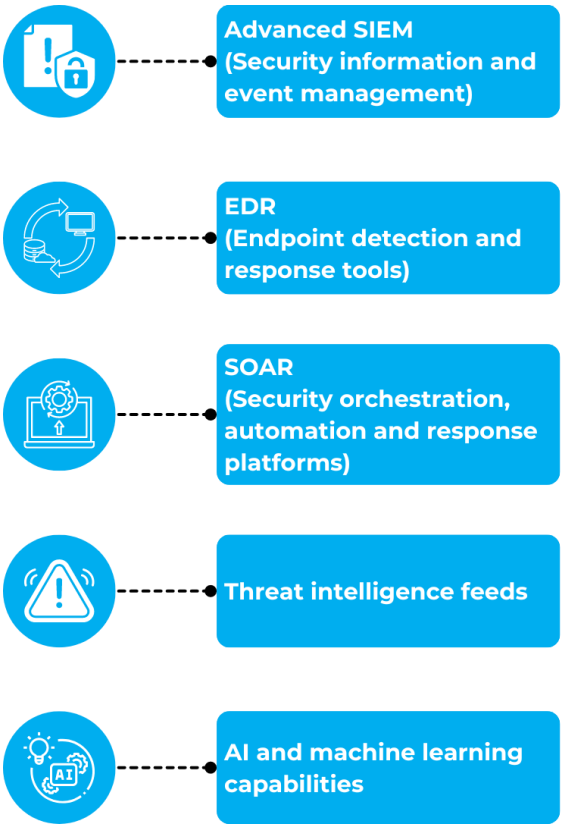
Security operation centre (SOC)

In today's hyperconnected digital ecosystem, cyber threats are constant and evolving. A security operation centre (SOC) stands as the nerve centre of an organisation's cybersecurity strategy, providing round-the-clock monitoring, detection, and response to security incidents. As we navigate the complex cybersecurity landscape of 2024 and beyond, a robust SOC is no longer optional—it's a critical necessity for maintaining digital resilience.

Understanding the modern SOC

A security operation centre is a centralised unit that employs people, processes, and technology to continuously monitor and improve an organisation's security posture while preventing, detecting, analysing, and responding to cybersecurity incidents.

Key components of a modern SOC



The evolving SOC landscape

As cyber threats become more sophisticated, SOCs are adapting to meet new challenges:

- **AI-driven threat detection:** Leveraging artificial intelligence to identify complex attack patterns and reduce false positives.
- **Cloud-native SOC:** Embracing cloud technologies for improved scalability and flexibility.
- **Extended detection and response (XDR):** Providing holistic threat detection and response across multiple security layers.
- **Proactive threat hunting:** Actively searching for hidden threats that have evaded initial detection mechanisms.

Why a modern SOC matters

1. **Evolving threat landscape:** With cyber threats becoming increasingly sophisticated, a modern SOC is essential for staying ahead of attackers.
2. **Rapid incident response:** The average time to identify and contain a data breach is 277 days. A well-equipped SOC can significantly reduce this timeframe, minimising potential damages.
3. **Skill gap mitigation:** Address the cybersecurity skills shortage by leveraging our team of expert analysts and advanced technologies.
4. **Regulatory compliance:** Meet stringent compliance requirements with comprehensive monitoring and documentation capabilities.
5. **Business continuity:** Ensure uninterrupted operations by proactively identifying and mitigating potential security risks.

The future of SOC: trends shaping 2024 and beyond

- **AI and machine learning integration:** Enhancing threat detection and automated response capabilities.
- **Cloud-based and virtual SOCs:** Offering greater flexibility and scalability for organisations of all sizes.
- **Focus on user behaviour analytics:** Identifying insider threats and compromised accounts through advanced behavioural analysis.
- **Integration with DevSecOps:** embedding security throughout the development lifecycle for more resilient applications.
- **Emphasis on purple teaming:** Combining red (offensive) and blue (defensive) team exercises to continuously improve SOC effectiveness.

In an era where cyber threats are a constant reality, a robust security operation centre is your organisation's first line of defence. By leveraging our state-of-the-art SOC services, you can navigate the complex cybersecurity landscape with confidence, ensuring the protection of your digital assets and maintaining stakeholder trust in an increasingly interconnected world.

Third-party risk management (TPRM)

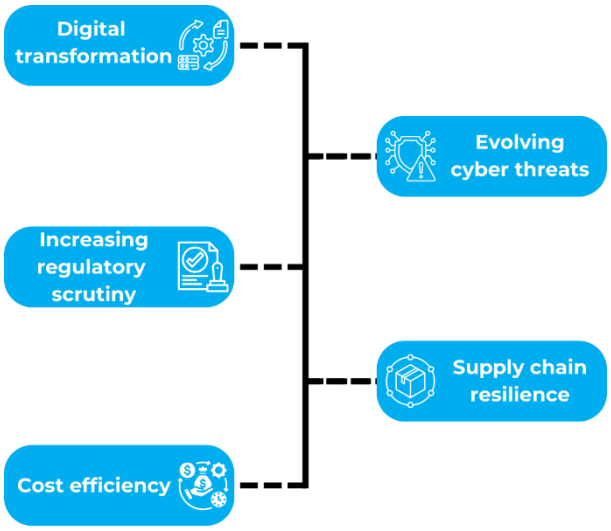
In today's interconnected business landscape, organisations increasingly rely on a network of third-party vendors, suppliers, and partners to drive innovation, efficiency, and growth. However, this extended enterprise also introduces a myriad of potential risks that can compromise your organisation's security, compliance, and reputation. Third-party risk management (TPRM) has become a critical component of a comprehensive risk management strategy, ensuring that your organisation's ecosystem remains resilient and secure.

Understanding third-party risk management

TPRM is a comprehensive approach to identifying, assessing, and mitigating risks associated with your organisation's reliance on third parties. It encompasses a wide range of potential risks, including:

- Cybersecurity vulnerabilities
- Data privacy breaches
- Operational disruptions
- Regulatory non-compliance
- Reputational damage

Why TPRM matters now more than ever



1. **Digital transformation:** As businesses rapidly adopt new technologies, often through third-party services, managing the associated risks becomes crucial.
2. **Evolving cyber threats:** As cyber-attacks become more sophisticated, organisations must ensure their third parties don't become weak links in their security chain.
3. **Increasing regulatory scrutiny:** With regulations like GDPR and CCPA holding organisations accountable for their third parties' actions, robust TPRM is essential for compliance.
4. **Supply chain resilience:** Recent global disruptions have highlighted the need for robust risk management across the entire supply chain.
5. **Cost efficiency:** Effective TPRM can prevent costly incidents and disruptions, ultimately saving your organisation money and resources.

Emerging trends in TPRM

- **AI and machine learning integration:** Leveraging advanced analytics for more accurate risk predictions and anomaly detection.
- **Automation of risk assessments:** Streamlining the assessment process to handle an increasing number of third-party relationships efficiently.
- **Focus on fourth-party risk:** Extending risk management to your third parties' vendors and partners.
- **Emphasis on resilience:** Moving beyond compliance to ensure business continuity in the face of third-party disruptions.
- **Collaborative risk management:** Fostering partnerships with key third parties to jointly address and mitigate shared risks.

The growing importance of TPRM

Recent trends and statistics underscore the critical nature of effective TPRM:

- According to Prevalent's 2024 Third-Party Risk Management Study, 75% of organisations experienced a third-party incident in the past year, up from 58% in 2023.
- The same study revealed that 45% of organisations now conduct third-party risk assessments quarterly or more frequently, indicating a shift towards more proactive risk management.
- ISACA's 2024 report highlights that 68% of organisations believe digital transformation has significantly increased third-party risks.

Our TPRM approach

Our IT & Cybersecurity team offers a comprehensive TPRM service designed to safeguard your extended enterprise:

Risk identification and assessment

- Conduct thorough due diligence on potential and existing third parties
- Assess risks across multiple domains (e.g., cybersecurity, financial, operational)

Risk categorisation and prioritisation

- Classify third parties based on criticality and risk level
- Prioritise risk mitigation efforts for high-risk relationships

Continuous monitoring

- Implement real-time monitoring of third-party risk indicators
- Utilise advanced analytics and threat intelligence feeds

Policy and contract management

- Develop and enforce robust third-party risk policies
- Ensure contracts include appropriate risk mitigation clauses

Compliance management

- Ensure third-party compliance with relevant regulations (e.g., GDPR, CCPA)
- Conduct regular compliance audits and assessments

Incident response planning

- Develop and test incident response plans for third party-related events
- Ensure clear communication channels with critical third parties

Reporting and analytics

- Provide comprehensive dashboards and reports on third-party risk posture
- Offer actionable insights for risk mitigation and relationship optimisation

Benefits of our TPRM services

By partnering with our team, your organisation can:

- **Enhance visibility:** Gain a comprehensive view of your third-party ecosystem and associated risks.
- **Improve decision-making:** Make informed decisions about third-party relationships based on data-driven risk assessments.
- **Ensure compliance:** Meet regulatory requirements and industry standards for third-party risk management.
- **Prevent disruptions:** Identify and mitigate potential risks before they impact your operations.
- **Protect reputation:** Safeguard your brand by ensuring your third parties adhere to your standards and values.

In an era where your organisation's success is increasingly intertwined with that of your third-party ecosystem, a robust TPRM programme is not just a best practice—it's a business imperative. By leveraging our expertise in Third-Party Risk Management, you can confidently navigate the complex web of external relationships, safeguarding your operations, reputation, and bottom line in an increasingly interconnected business world.

OUR PROFESSIONAL TEAM

- Our team includes professionals with practical and solid knowledge and experience.
- The team comprises charter holders or members of professional bodies such as CPA, CISA, CIA, ACCA, CIPP/A and lead auditor for ISO/IEC 27001/27017/27018 & ISO/IEC 20000 (IRCA).
- We have extensive sector knowledge to provide customised advice to suit each client taking into account size, capabilities and goals.

Backed by our international network, we have the scope to provide clients with all solutions and expertise they require, wherever they choose to do business.

For any enquiries, please contact our advisers directly.

Patrick Rozario
Advisory Services Managing Director

T +852 2738 7769
E patrickrozario@moore.hk

Kevin Lau
IT & Cybersecurity Principal

T +852 2738 4631
E kevinlau@moore.hk

At Moore, our purpose is to help people thrive – our clients, our people, and the communities they live and work in. We're a global accounting and advisory family with over 37,000 people in 558 offices across 114 countries, connecting and collaborating to take care of your needs – local, national and international.

MOORE