MOORE

BUSINESS CONTINUITY

Assist your business for seamless disaster recovery and uninterrupted business operations

Business continuity plan (BCP)

Resilience in business and IT is crucial for ensuring operational continuity. Comprehensive business continuity strategies help secure essential processes, minimise disruptions, and enable swift recovery from unexpected events.

Creating a tailored business continuity plan (BCP) is challenging in today's complex business landscape. Organisations face a multitude of risks, including infectious diseases, ransomware attacks, and natural disasters.

The cost of unpreparedness is significant. An unplanned application outage can lead to substantial financial loss, damage to customer trust, and regulatory penalties. With a robust and adaptable BCP, organisations can mitigate these risks and protect themselves from financial consequences, operational disruptions, and brand damage.

To help you develop and achieve a robust BCP, our IT & Cybersecurity experts offer the following end-to-end process services:

Project planning: We collaborate with you to define the specific goals and boundaries of the BCP, ensuring alignment with your organisation's business objectives and risk management framework.

Risk assessment & analysis: We assess your most critical assets, identify potential threats to those assets, discover weaknesses in your existing controls, and evaluate the potential impacts of those risks.

Business impact analysis (BIA): We review your approach to conducting BIA, evaluating the impact assessment criteria used, such as time frames, priorities, resources and interdependencies of critical processes.

Business continuity strategy development: We examine your business continuity strategies in alignment with your overall business goals.

Business continuity plan development: We evaluate the robustness of your BCP, ensuring it covers all critical business functions, processes, and resources, as well as its ability to address various disruption scenarios, including natural disasters, cyber-attacks, and human-induced incidents.

Business continuity plan testing & awareness training: We assess your BCP test, including test scenarios, roles and responsibilities, and coordination among responsible teams. We also observe the execution of BCP tests and evaluate your ability to meet the objectives and metrics defined.

Business continuity plan monitoring, maintenance and update: To ensure a current and effective BCP that aligns with the evolving organisational and operational landscape, we help you verify that your BCP maintenance activities are performed at regular intervals and in response to internal and external changes.

Disaster recovery strategy

A robust disaster recovery (DR) plan, developed from business impact analysis (BIA) conducted during business continuity planning (BCP), ensures the recovery of critical IT infrastructure and systems during disruptive incidents. DR facilitates a smooth transition from crisis management to business recovery. Without a comprehensive backup and recovery plan, organisations risk severe financial and operational consequences.

IBM reports the global average cost of a data breach at nearly $4.5 million, highlighting the importance of a comprehensive DR strategy. Lack of such a strategy can lead to system downtime, data loss, reputational damage, and loss of customer trust.

Our IT & Cybersecurity experts offer an end-to-end process to help orchestrate a coordinated response to disruptive events, providing benefits including cost optimisation, data protection, minimised downtime, and business continuity.

Business impact analysis: We collaborate with your business units to assess the impact of disasters, evaluate potential consequences, and provide guidance on recovery objectives such as recovery point objective and recovery time objective for the organisation's critical assets.

Risk evaluation: We conduct comprehensive risk assessments, leveraging our expertise in threat intelligence and security analysis to identify and prioritise risks while evaluating the effectiveness of existing security controls in mitigating them.

Asset cataloguing: We assist you in maintaining a comprehensive inventory of your organisation's critical assets, including detailed information about their dependencies, recovery requirements, the associated security controls, and disaster recovery capabilities.

Responsibility alignment: We collaborate with your disaster recovery planning team to define and align their roles and responsibilities, including threat detection, incident containment, data protection, and secure recovery, as part of the organisation's incident response and disaster recovery procedures.

Testing & refinement: We participate in the regular testing and simulation of your disaster recovery plan, providing expertise to identify areas for improvement and assist in refining the security-related procedures, controls, and recovery capabilities.

Enterprise risk management

Strategic risk management, central to the enterprise risk management (ERM) process, shapes a flexible and robust Business Continuity Plan (BCP). It equips organisations to identify, assess, and mitigate threats that could disrupt operations, ensuring business continuity and resilience.

Lacking a strong ERM framework exposes organisations to various risks, including data breaches, supply chain issues, and IT system failures. Without proactive risk management, companies may be unprepared for disruptive events, leading to financial losses, operational disruptions, reputational damage, and loss of customer trust. These consequences can undermine long-term viability and competitive advantage.

Our IT & Cybersecurity team enhances your organisation's versatility and technological resilience. We help you achieve objectives while navigating various disruptive scenarios through our ERM process.

1.Risk Identification
- Understand emerging digital threats, vulnerabilities, and technological risks
- Provide valuable insights on potential cyber attacks, system failures and other IT-related disruptions

2.Risk assessment and analysis
- Conduct thorough risk assessment and analyses of the firm's technology ecosystem
- Assess the probability and consequences of diverse technology-based risks

3.Risk response & mitigation
- Develop tailored risk mitigation strategies for technology-risks, including ensuring redundancy measures for critical assets

4.Risk monitoring & mitigation
- Continuously examine the organisation's technology environment, scanning for new vulnerabilities, emerging threats and shifts in threat landscape

5.Risk reporting & communication
- Communicate technical risks and mitigation strategies to the broader risk management and business continuity teams

6.Risk integration & alignment
- Integrate technology-related risk management into the firm's overall strategic planning and decision-making

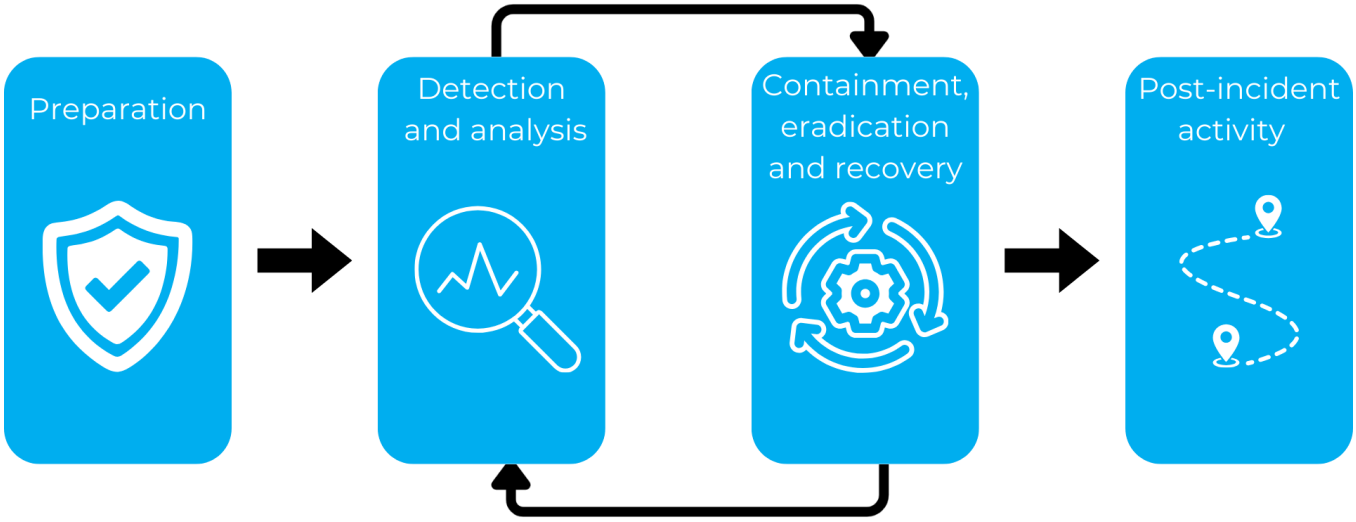
IT incident management and response

In today's technology-driven business world, IT incidents like data breaches and cyber-attacks are unavoidable. These events can severely impact an organisation's operations, finances, and reputation. Effective IT incident management and response strategies are crucial for protecting against unexpected events.

A comprehensive approach to IT incident management is essential for maintaining business operations and mitigating potentially catastrophic consequences of unresolved incidents.

Even minor issues, if undetected due to inadequate incident management, can trigger a chain reaction across interconnected systems. This can lead to operational paralysis, financial losses, customer churn, and difficulty in restoring normal operations.

Our IT & Cybersecurity professionals can help businesses build a robust and adaptable incident management framework to mitigate the impact of disruptive events and maintain operational resilience through four key incident management steps.



Preparation: We help you establish the foundation for effective incident management by defining roles and responsibilities and ensuring the availability of technology, resources and software related to incident management.

Detection & analysis: We identify and conduct an initial assessment of the incident that happened in your business, involving the implementation of robust security monitoring and anomaly detection mechanisms, clear channels and procedures for receiving incident reports from stakeholders and thorough analysis to understand the scope, impact, and potential causes of the identified incidents.

Containment, eradication & recovery: We evaluate the effectiveness of your incident containment measures, conduct an in-depth analysis to identify the root cause, and make recommendations for further improvements to the incident response process.

Post-incident activity: We thoroughly review your entire incident response process and analyse the effectiveness of your organisation’s response and lessons learned meetings held to identify areas for improvement in your existing processes.

Moore Hong Kong

WHY MOORE?

At Moore, it's not about us. It's all about you. When it comes to providing personalised and commercially astute audit, accounting, tax and business advisory services, it simply can't be anything else.

With over 30 directors and a team of over 300 staff, we offer a wide range of audit, assurance tax, and advisory services to our clients. Our global family of 30,000 professionals in more than 110 countries allows us to share expertise, knowledge, and best practices to ensure our clients receive the highest quality of service, no matter where their work takes them.

As your genuine professional partner, we will not only advise you but also challenge you to meet your goals and objectives for the future. With our team's personal qualities, skills, and experience, we are confident in our ability to support your group's development.

CONTACT US

Our IT and Cybersecurity practice offers a spectrum of services that help businesses achieve a robust IT architecture and security framework through identifying vulnerabilities, threats and areas for improvement.

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