



Think, Start and Connect

Managing IT and Cyber risk
to create value

The Deloitte Platform of IT and Cyber Services can help you to...

- identify insider threats
- develop actionable and measurable plans to enhance IT Security
- implement data-related best practices
- identify and prevent reoccurrence of breach
- protect your corporate and sensitive customer data
- build the necessary trust, reputation and confidence
- design your system to be protected from attacks, damage or unauthorised access

Understanding your requirements

Assessing security maturities against capabilities

Deloitte's framework is the result of a comprehensive research and amalgamation of NSIT, SANS and ISO 27001, making it the best security assessment against capabilities.

Our approach is to design a target state by assessing the vulnerability of business towards a catalogue of IT threats. Using this framework, a maturity dashboard will be created to portray the organisation's maturity scores, by threat, including:

Governance

Ensuring that the necessary structures and rules are in place to maintain and enhance prevention and detection.

Secure

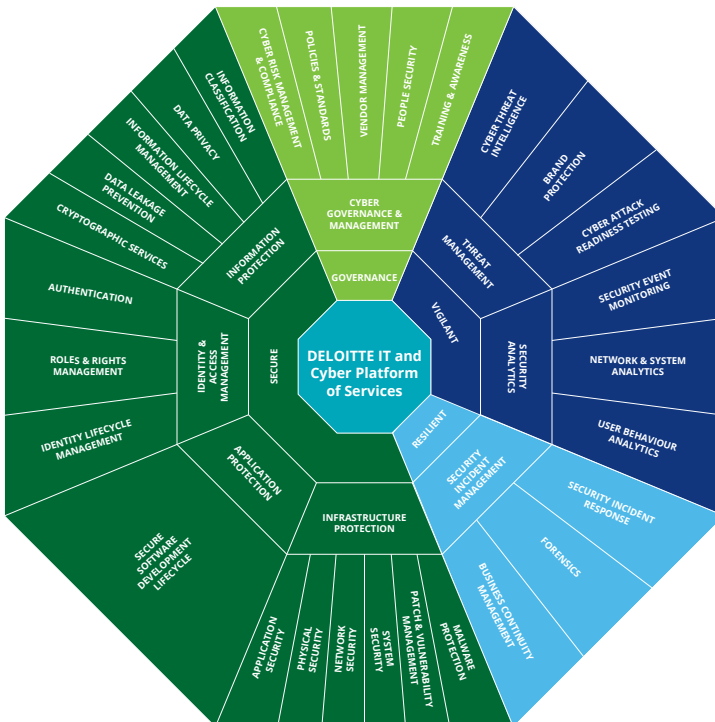
Proactive protection against successful cyber attacks before they occur by developing, implementing and enhancing security systems.

Vigilant

Ability to discover internal and external threats by leveraging threat intelligence, and proactively mitigating threats, or minimising any adverse impacts to the organisation.

Resilient

It is not a question of whether your organisation will be attacked or not; it is a question of when: the key is to be prepared.



The Deloitte Platform of IT and Cyber Services

	Services	Details
Governance	Strategy & Operating Model	Implement and maintain a security strategy and supporting roadmap with the necessary security governance structure, working groups, resources and roles and responsibilities to achieve this.
	Policies, Standards & Architecture	Define, implement and update policies and standards related to the intended audience, as well as reference architectures, network diagrams, procedures and guidelines to support where necessary.
	Risk Culture & Behaviour	Educate, coach and mentor employees, customers and third parties on their security responsibilities and IT risks to drive an IT-aware culture, from Senior Management to employees.
	IT Risk Management, Metrics & Reporting	Manage and report to Senior Management on the organisation's key IT risks and compliance, in order to provide an appropriate comprehension and a timely and effective mitigation.
Secure	Cloud Security	Plan and monitor Cloud activities for adherence with internal, contractual, legal and regulatory security requirements – embedding security into the organisation's Cloud strategy.
	Third Party Risk Management	Implement, assess and mitigate security standards with IT due diligence assessment and risk rating of suppliers.
	HR Security	Manage and assess risks related to people, including IT security training, employee security screening, timely communication with IT, movers and leavers, and secure management of personal information.
	Physical Security	Assess, implement and monitor physical security processes and controls to restrict physical access to authorised individuals only, as well as protect sensitive physical information and access to these.
	Identity Lifecycle Management	Implement, maintain and assess identities, manage the joiner, mover and leaver process, and manage generic accounts, identity repositories and passwords.
	User Access Control	Define and implement adequate authentication methods (based on risk), as well as manage incorrect access attempts or forgotten credential requests.
	Role-Based Access Control	Limit the risk of unwanted or accidental changes, align rights with the business needs and support the principles of least privilege and separation of duties.
	Secure SDLC	Integrate security into the software development process, including the design, implementation, testing and ongoing development changes.
	Post-Development Application Protection	Implement in-depth defence security controls to protect applications (excluding the Secure Software Development Life Cycle (SDLC) process). Includes defining and maintaining application inventories that define criticality, a risk assessment process to capture application security requirements, web application firewalls and other layer seven controls to protect applications.
	System Security	Establish and maintain a standardised, predetermined image to help ensure that servers, network devices and endpoints are built to a consistent and secure standard. The standard image includes enabling secure functions and services and disabling insecure or unnecessary TCP and UDP services, changing default passwords and locking down user access to the minimum needed for their role.
	Malware Protection	Assess the signature and behavior-based malware protection software being installed, and configure and protect the network and systems vulnerable to malware infection.

The Deloitte Platform of IT and Cyber Services

	Services	Details
Secure	Asset Management	Identify, classify and maintain details relating to assets (includes information, software and IT infrastructure assets), as well as assess ownership of assets. All assets are classified according to their use, sensitivity of their data and importance.
	Network Security	Identify malicious attacks and control remote access into the network with a strong protection of the physical environment and a segregation of the internal network into security zones to prevent and identify attacks.
	End-User Device Security	Secure end-user devices to prevent unauthorised access, installation of malicious software and removal of sensitive information.
	Data Loss Prevention	Monitor and protect data whilst in-use, in-motion and at-rest. Includes, but is not limited to, data from systems, applications, personal workstations, mobile devices and removable media.
	Encryption	Define when and how information should be encrypted, and implement and maintain effective encryption solutions that protect the data based on its level of confidentiality.
	Information Lifecycle Management	Assess information quality and integrity, manage data back-up and recovery, define retention periods and securely de-identify or destroy data once no longer required.
	Data Privacy	Implement applicable country privacy requirements and practices around the collection, storage, use, sharing, and transfer of personal information. Personally identifiable information (PII) must be handled securely and de-identified or disposed of once it is no longer required for legitimate business use.
	Information Classification	Establish information classification levels and associated security controls as well as protect the confidentiality, integrity, availability and regulatory needs of the structured and unstructured information assets based on their business impact.
Resilient	Incident Readiness	Test the response to a possible cyber-attack in order to assess the adequacy of the preparedness and the responsive capabilities.
	Incident Response	Prepare for and respond to IT incidents in order to recover the environment impacted, including the collection and tracking of cyber-security incident response KPIs across the organisation.
	Business Continuity Planning & Recovery	Establish processes and procedures needed to restore critical operations following a disruption caused by an IT incident and to take reasonable and appropriate steps to protect its people and its business.
Vigilant	Penetration Testing & Vulnerability Scanning	Implement a risk-based approach to test for application, system and network security vulnerabilities and weaknesses. Testing should include dealing with new projects and significant architecture changes.
	Threat Intelligence	Collect information on the context, mechanisms, indicators and implications of threats and actionable advice, as well as existing or emerging threats to key business operations and information assets.
	Brand Protection	Monitor internet references to the organisation and its brands in order to gather relevant information that might compromise the organisation's image, reputation, individuals or security of its information systems, including the detection of fraudulent websites associated with phishing or malware.
	Security Event Monitoring	Analyse security events and applicable threat data, in order to detect and ensure visibility into policy violations and unusual IT and network activity.
	Patch & Vulnerability Management	Identify, assess, mitigate and track technical vulnerabilities to systems and applications.
	IT Analytics	Analyse user, system and network behaviour by assessing data for variations that differ from normal activity and that can indicate suspicious behaviour or anomalies that could lead to a potential cyber-attack.
	Security Platform Administration and Operations	Access and manage solutions used to secure and monitor the organisation's network.

Contacts

Rui Figueiredo

Senior Manager
Risk Advisory
rfigrdo@deloitte.com
+95 99 6014 0501

Soe Win

Country Managing
Partner,
Myanmar
soewin@deloitte.com

Victor Keong

Partner,
Risk Advisory
vkeong@deloitte.com

Cheryl Khor

Partner,
Risk Advisory
ckhor@deloitte.com

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/mm/about to learn more about our global network of member firms.

Deloitte provides audit, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 245,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

About Deloitte Southeast Asia

Deloitte Southeast Asia Ltd – a member firm of Deloitte Touche Tohmatsu Limited comprising Deloitte practices operating in Brunei, Cambodia, Guam, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam – was established to deliver measurable value to the particular demands of increasingly intra-regional and fast growing companies and enterprises.

Comprising 290 partners and over 7,400 professionals in 25 office locations, the subsidiaries and affiliates of Deloitte Southeast Asia Ltd combine their technical expertise and deep industry knowledge to deliver consistent high quality services to companies in the region.

All services are provided through the individual country practices, their subsidiaries and affiliates which are separate and independent legal entities.