Deloitte.

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.

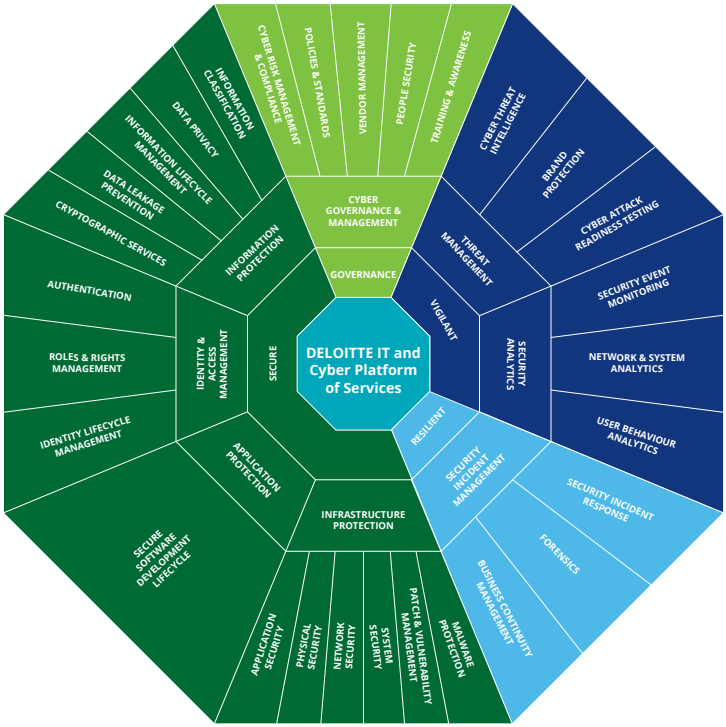
Our approach is to design a target state by assessing the vulnerability of business towards a catalogue of IT threats. Using this framework, a maturity dashboard will be created to portray the organisation's maturity scores, by threat, including:

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 s and roles and responsibilities to achieve this.
	Policies, Standards & Architecture	Define, implement and update policies and stand procedures and guidelines to support where nece
	Risk Culture & Behaviour	Educate, coach and mentor employees, customer Senior Management to employees.
	IT Risk Management, Metrics & Reporting	Manage and report to Senior Management on the a timely and effective mitigation.
Secure	Cloud Security	Plan and monitor Cloud activities for adherence w organisation's Cloud strategy.
	Third Party Risk Management	Implement, assess and mitigate security standard
	HR Security	Manage and assess risks related to people, includ leavers, and secure management of personal info
	Physical Security	Assess, implement and monitor physical security sensitive physical information and access to these
	Identity Lifecycle Management	Implement, maintain and assess identities, manag passwords.
	User Access Control	Define and implement adequate authentication m requests.
	Role-Based Access Control	Limit the risk of unwanted or accidental changes, duties.
	Secure SDLC	Integrate security into the software development
	Post-Development Application Protection	Implement in-depth defence security controls to p Includes defining and maintaining application inv requirements, web application firewalls and other
	System Security	Establish and maintain a standardised, predeterm secure standard. The standard image includes en changing default passwords and locking down us
	Malware Protection	Assess the signature and behavior-based malwar vulnerable to malware infection.

supporting roadmap with the necessary security governance structure, working groups, resources

ards related to the intended audience, as well as reference architectures, network diagrams, essary.

s and third parties on their security responsibilities and IT risks to drive an IT-aware culture, from

e organisation's key IT risks and compliance, in order to provide an appropriate comprehension and

with internal, contractual, legal and regulatory security requirements – embedding security into the

ls with IT due diligence assessment and risk rating of suppliers.

ling IT security training, employee security screening, timely communication with IT, movers and rmation.

processes and controls to restrict physical access to authorised individuals only, as well as protect e.

ge the joiner, mover and leaver process, and manage generic accounts, identity repositories and

methods (based on risk), as well as manage incorrect access attempts or forgotten credential

align rights with the business needs and support the principles of least privilege and separation of

process, including the design, implementation, testing and ongoing development changes.

protect applications (excluding the Secure Software Development Life Cycle (SDLC) process). entories that define criticality, a risk assessment process to capture application security r layer seven controls to protect applications.

hined image to help ensure that servers, network devices and endpoints are built to a consistent and abling secure functions and services and disabling insecure or unnecessary TCP and UDP services, er access to the minimum needed for their role.

e protection software being installed, and configure and protect the network and systems

The Deloitte Platform of IT and Cyber Services

	Services	Details
Secure	Asset Management	Identify, classify and maintain details relating to as assets. All assets are classified according to their u
	Network Security	Identify malicious attacks and control remote acce internal network into security zones to prevent an
	End-User Device Security	Secure end-user devices to prevent unauthorised
	Data Loss Prevention	Monitor and protect data whilst in-use, in-motion mobile devices and removable media.
	Encryption	Define when and how information should be encr level of confidentiality.
	Information Lifecycle Management	Assess information quality and integrity, manage no longer required.
	Data Privacy	Implement applicable country privacy requiremen Personally identifiable information (PII) must be h it is no longer required for legitimate business use
	Information Classification	Establish information classification levels and asso needs of the structured and unstructured informa
Resilient	Incident Readiness	Test the response to a possible cyber-attack in ord
	Incident Response	Prepare for and respond to IT incidents in order to response KPIs across the organisation.
	Business Continuity Planning & Recovery	Establish processes and procedures needed to res appropriate steps to protect its people and its bus
Vigilant	Penetration Testing & Vulnerability Scanning	Implement a risk-based approach to test for appli with new projects and significant architecture cha
	Threat Intelligence	Collect information on the context, mechanisms, i to key business operations and information assets
	Brand Protection	Monitor internet references to the organisation ar image, reputation, individuals or security of its inf malware.
	Security Event Monitoring	Analyse security events and applicable threat data
	Patch & Vulnerability Management	Identify, assess, mitigate and track technical vulne
	IT Analytics	Analyse user, system and network behaviour by a behaviour or anomalies that could lead to a poten
	Security Platform Administration and Operations	Access and manage solutions used to secure and

ssets (includes information, software and IT infrastructure assets), as well as assess ownership of use, sensitivity of their data and importance.

ess into the network with a strong protection of the physical environment and a segregation of the d identify attacks.

access, installation of malicious software and removal of sensitive information.

and at-rest. Includes, but is not limited to, data from systems, applications, personal workstations,

ypted, and implement and maintain effective encryption solutions that protect the data based on its

data back-up and recovery, define retention periods and securely de-identify or destroy data once

ts and practices around the collection, storage, use, sharing, and transfer of personal information. andled securely and de-identified or disposed of once e.

ociated security controls as well as protect the confidentiality, integrity, availability and regulatory ation assets based on their business impact.

der to assess the adequacy of the preparedness and the responsive capabilities.

o recover the environment impacted, including the collection and tracking of cyber-security incident

store critical operations following a disruption caused by an IT incident and to take reasonable and siness.

cation, system and network security vulnerabilities and weaknesses. Testing should include dealing nges.

ndicators and implications of threats and actionable advice, as well as existing or emerging threats s.

nd its brands in order to gather relevant information that might compromise the organisation's ormation systems, including the detection of fraudulent websites associated with phishing or

a, in order to detect and ensure visibility into policy violations and unusual IT and network activity.

rabilities to systems and applications.

ssessing data for variations that differ from normal activity and that can indicate suspicious ntial cyber-attack.

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.