
Can cybersecurity framework implementation transform from standard to innovative?
ey.com/better working world
#BetterQuestions
The better the question. The better the answer.
The better the world works.
EY
Building a better working world

Overview

The paper talks about how ICT organizations are leading digital advancements in the world, but how this advancement is actually exposing many areas of risk. The paper starts by suggesting a few steps before starting to develop the framework. It challenges a one-size-fits-all framework so it is essential to profile companies (see section 6) to determine size and maturity. The next thing discussed is the need to focus on the people, process and technology in order to analyze the domain and supporting domains such as vulnerability, threat, incident and crisis management. Then focuses on developing the framework (part 8) while emphasizing three important steps: current state analysis, benchmarking and gap analysis. The paper concludes with discussions that talk about the framework and guidelines.

Contents

01	Foreword	04
02	Executive summary	06
03	Introduction	07
04	Framework development	08
05	ICT sector landscape	13
06	VTI and CM framework essentials	14
07	Lessons learnt	22
08	Conclusion	24
09	Contributors	27
10	Contacts	28
11	Glossary of terms	29

01 Foreword

Empowering and enabling leading digital nations across the world requires an approach based on security by design where security is factored from the onset of all technology projects. The authors of this whitepaper are seasoned professionals who were extensively involved in the creation of a standardized framework that considered the core domains essential for implementing security by design concepts within Information, Communication, and Technology (ICT) organizations. The defined framework serves as thought leadership that will assist ICT organizations across the world to enhance their security posture, allow executive management of these ICT organizations to understand the current landscape and identify improvement areas within their organization or sector.

This whitepaper deep dives into the approach undertaken for developing the framework and provides insights into the leading practices that could be considered by similar entities developing sectoral cybersecurity frameworks globally.

The focus was on enhancing the cybersecurity posture of the ICT sector at a rate that is commensurate with the rapid advancements in technology and innovation across the global ICT sector. In order to guide ICT organizations regarding methods to upscale cybersecurity maturity, a series of activities have culminated in this whitepaper on how ICT organizations and sectors globally can prepare a framework and guidelines that cover the essential topics of vulnerability management, threat management, incident management and crisis management.

02

Executive summary

ICT organizations are the catalyst for enabling digital transformation and large-scale changes across all industries and sectors around the globe. Ground-breaking innovations within the technology world, quite often led by ICT organizations, are altering businesses and business models, connecting people with services that offer comfort and flexibility, and requiring entire industries to reimagine their futures.

However, they must continue to tap into new markets while improving operational efficiencies and managing risks while meeting customer expectations. They must continually foster creativity, as well as quickly and efficiently adapt to changing markets and economic environments in today's rapid and unpredictable landscape.

The rapid digital advancements that the ICT organizations are making and the disruption it brings increase the risk of a cyberattack. Digitalization allows ICT organizations to deliver unique and connected data-driven and in-demand client experiences at a rapid pace, which leads to greater inherent cyber risks. Innovative developments and new business models provide additional entry points for cyber attacks, while emerging technologies, such as IoT and increasing consumer end-points must be made secure.

The challenges ICT organizations across the world are facing have been considered and bottlenecks as well as inherent risks within business models have been addressed through the issuance of a cybersecurity framework. The framework encompasses four key domains which are essential for cyber defense and resilience. The framework is supported by a number of guidelines that cover each identified domain in depth and provides a consistent methodology for attaining a target level of cybersecurity maturity that is commensurate with the organization's risk levels.

The adoption and implementation of the framework is a vital step in ensuring that the ICT sector is resilient and capable of detecting and containing cybersecurity threats and attacks before they have a large-scale impact on the operations of the sector and the other related entities. The framework also aims to ensure cyber threats and risks are appropriately monitored and managed throughout the sector, paving the way for a secure digital ecosystem.

Representatives of the ICT sector and wider cybersecurity communities, subject matter resources (SMRs), and consultants with national and international exposure have been engaged to build a framework that not only meets the needs of the sector but also acts as a trendsetter in terms of enhancing sectoral cybersecurity practices and encouraging their adoption in other sectors and other regions.

03 Introduction

The factors that make cybersecurity such a core component of any ICT organization were identified, in coordination with SMRs and consultants across the globe. It is a well-known fact that digital transformation is the catalyst for the proliferation of more services, experiences and benefits to customers – bringing increased revenue opportunities as well as risks. Cybersecurity is especially critical for ICT organizations across the globe due to the following inherent business issues and risks:

Digital

The intrinsic nature of many ICT products and services – software, games, films, and other products delivered to a growing list of platforms – makes cybersecurity particularly challenging for ICT organizations.

New business models

The growing adoption of direct-to-consumer (D2C) models means ICT organizations will shoulder unprecedented end-to-end cybersecurity risks.

A connected world

More devices are connecting to the internet and each other through the IoT (sensors, actuators, etc.), exponentially increasing the number of potential entry points for cybercriminals.

Data-driven customer experiences

ICT organizations are collecting more data than ever to enhance the customer experience and deliver targeted services. This provides a real competitive advantage for organizations and forces a balancing act to ensure customer trust and loyalty while protecting their customer base and their business.

Lower customer switching costs

Many ICT segments have lower customer switching costs than traditional industries. Customers can quickly and inexpensively move to alternative providers if ICT organizations have real or perceived cybersecurity vulnerabilities.

Taking note on the aforementioned factors, it was essential to focus on domains that ensure that cybersecurity and resiliency are embedded as an intrinsic part of the overall digital transformation programs. Hence, it was decided to pursue a customized framework that takes into account the following four domains which would allow ICT organizations around the world to mitigate the inherent business issues, manage cyber risks, and most importantly, implement a program that enhances cyber defense and resilience capabilities.

04 Framework development

As part of the framework development, a series of activities are conducted, including but not limited to performing a current state assessment, gap analysis and benchmarking exercise. The conduct of such activities ensures that the final outcome considers the nuances of the sector, current challenges of the ICT organizations, missing control gaps and best practices observed in all regions across the globe.

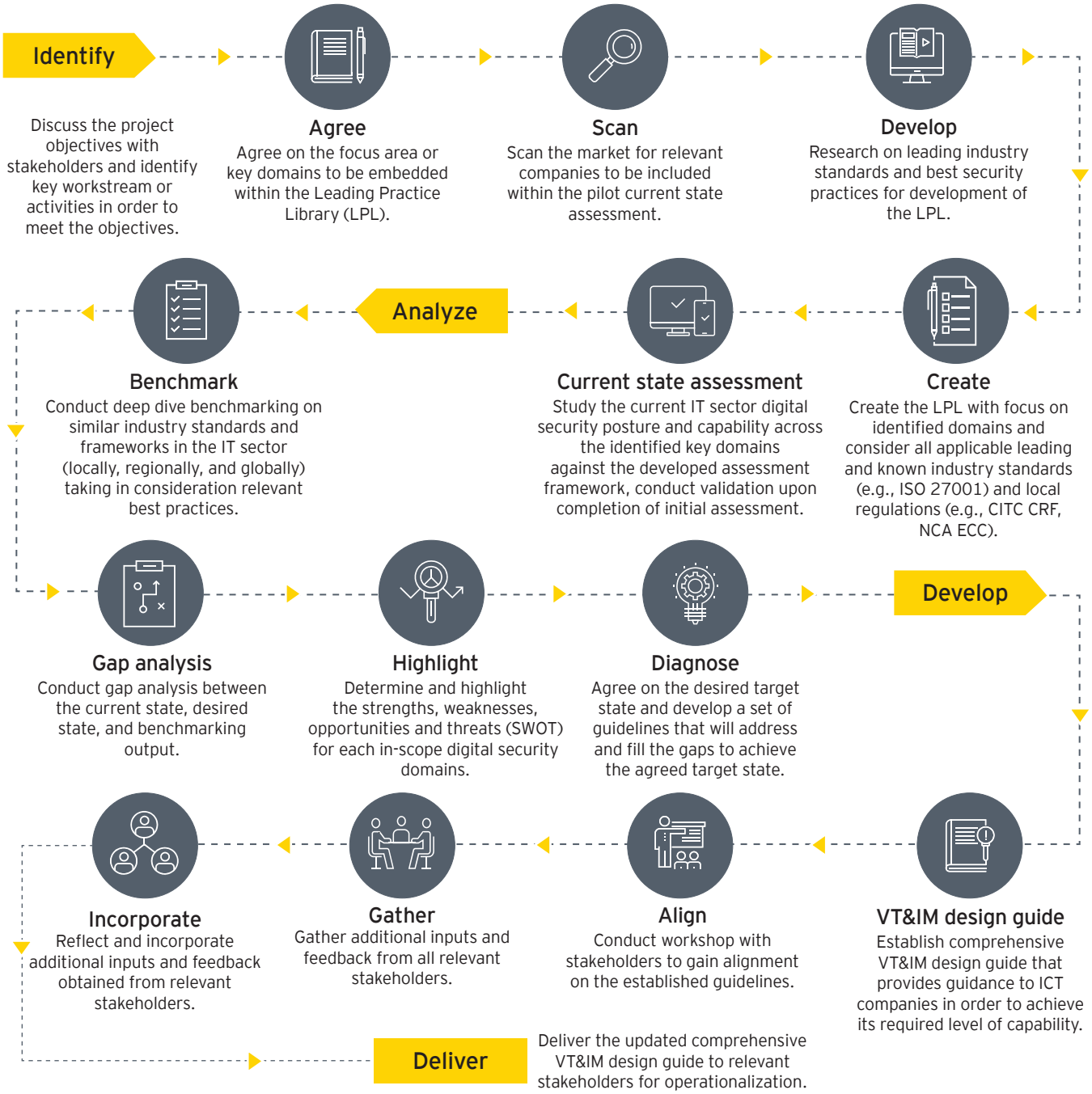


Figure 1: Approach used for defining the framework

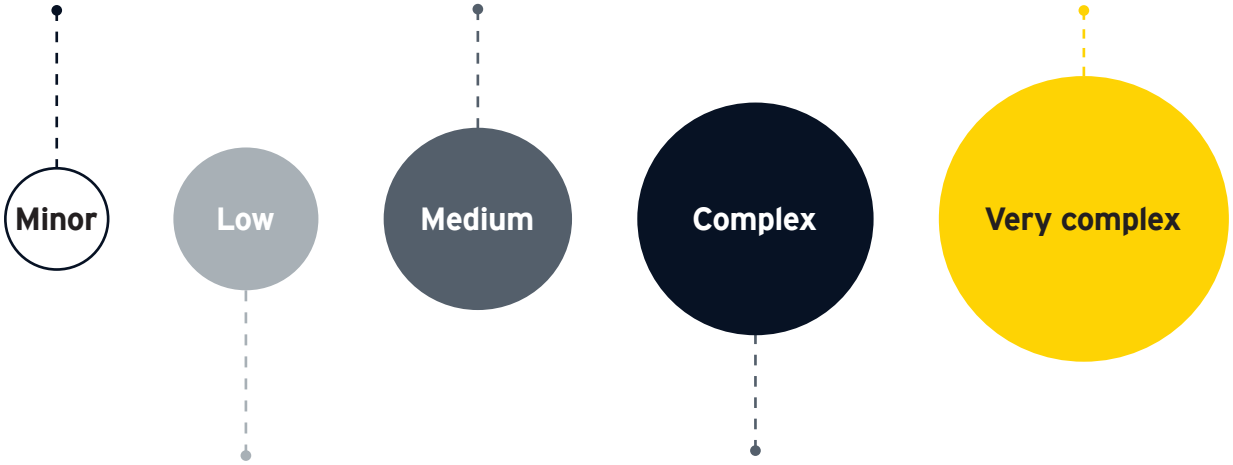
The starting point of the framework development is to understand that a one-size-fits-all approach is not ideal for a complex and evolving ICT sector. The ICT sector is undergoing rapid changes and technological advancements as part of the dynamic vision of organizations across the world and due to the innovation landscape and trends that can be observed globally.

Therefore, ICT organizations should be encouraged to adopt a level of cybersecurity maturity that is commensurate with the complexity level of the organization being assessed. Based on this understanding and consensus across all parties involved, it should be determined whether a company profiling exercise would be a prerequisite for the implementation of the framework. This profiling exercise will enable ICT organizations globally to identify their respective complexity levels and thereby identifying a target maturity level that will secure their business in line with their risk level. The company profiling exercise should consider several factors, such as the nature of operations, the complexity of IT infrastructure, and organizational characteristics to profile the organizations. The suggested company profile ratings are provided below:

Company with "Minor" complexity level generally has very limited use of digital platforms for service delivery. It has few or limited applications, systems, endpoints, servers and external connections. Company uses limited third-party services and emerging technologies. The company has faced limited or very few cyber attacks.

Company with "Medium" complexity level generally uses several digital platforms for service delivery. It has several applications, systems, endpoints, servers and external connections. The company uses several third-party services and emerging technologies. The company has faced several cyber attacks.

The company allows substantial number of personal devices and uses substantial number of servers, applications and endpoints.



Company with "Low" complexity level generally uses a few digital platforms for service delivery. It has few applications, systems, endpoints, servers and external connections. The company uses few third-party services and emerging technologies. The company has faced a few cyber attacks.

The company offers high-risk products and services that may include emerging and disruptive technologies. The company allows either a large number of personal devices and substantial number of servers, applications and endpoints.

Figure 2: Company profile ratings

The structure of the framework, essentially the building block or foundation, should be brainstormed extensively, given its significance, and should ultimately result in a six-layered model (as shown below).

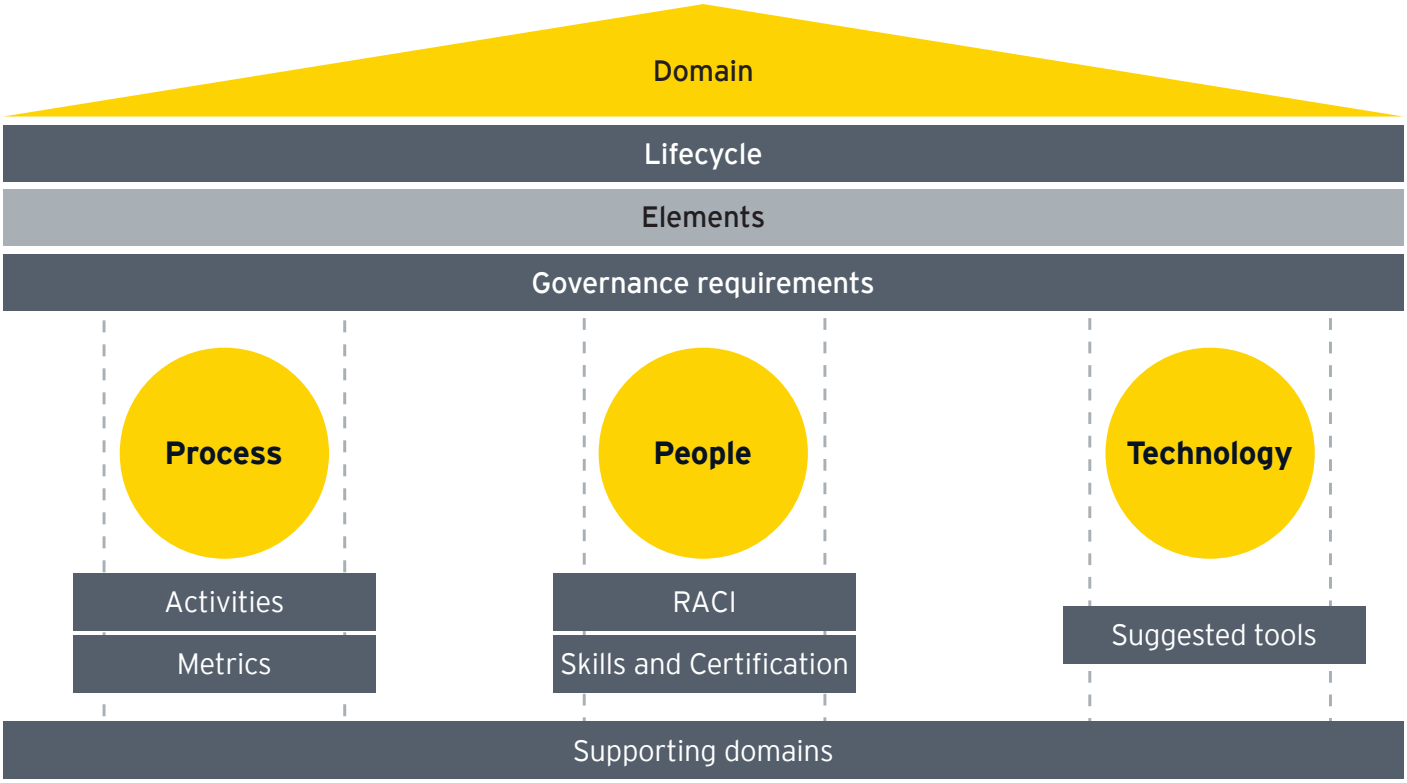


Figure 3: Framework components

Each layer should be thoroughly considered in terms of significance or value it will deliver for the overall implementation of the framework. The consensus is that the resulting framework structure will ensure that the methodology of people, process and technology (in which the balance of people, process, and technology drive action) is woven into the fabric of each domain and covers a broader lens of processes across an ICT organization.

During the process, where EY teams implement ideas, several local regulations, industry standards, and good cybersecurity practices were considered, in addition to the requirements identified within the preceding phases of current state assessment, gap analysis, and benchmarking. Some of the common industry standards and good cybersecurity practices we considered are the Saudi CITC CRF (Communications and Information Technology Commission Cybersecurity Regulatory Framework), Saudi NCA ECC (National Cybersecurity Authority Essential Cybersecurity Controls), ISO (International Organization for Standardization) 27001, NIST CSF (National Institute of Standards and Technology Cybersecurity Framework), NIST (National Institute of Standards) 800-53, BS (British Standards) 11200.

The design structure of each of the four domains should include a lifecycle (outlined in Figure 4), that must be broken down into elements that encompass a set of required activities to support the capability building, based on three pillars (i.e., people, process, technology). The detailed guidelines for each domain will provide details on these elements and relevant pillars (i.e., suggested activities, metrics, RACI, skills and certifications, and suggested tools).

The framework should also comprise of four suggested domains that are essential for an effective cybersecurity defense program: vulnerability, threat, incident and crisis management.

Moreover, each domain should be associated with supporting domains that could be considered by companies for wider coverage of the main domain. The following supporting domains are essential to mitigate cybersecurity flaws, gaps or vulnerabilities within the IT environment and its effective management allows a company to ensure a high degree of cybersecurity:

Vulnerability management	Threat management	Incident management	Crisis management
▸ Secure configuration management and hardening ▸ Penetration testing ▸ Secure application development ▸ Patch management	▸ Emerging threat management ▸ Logging and monitoring	▸ Emergency management and staff safety ▸ Business continuity management	▸ Risk management ▸ Emergency management and staff safety ▸ Business continuity management

The following graph illustrates the lifecycle of each domain:

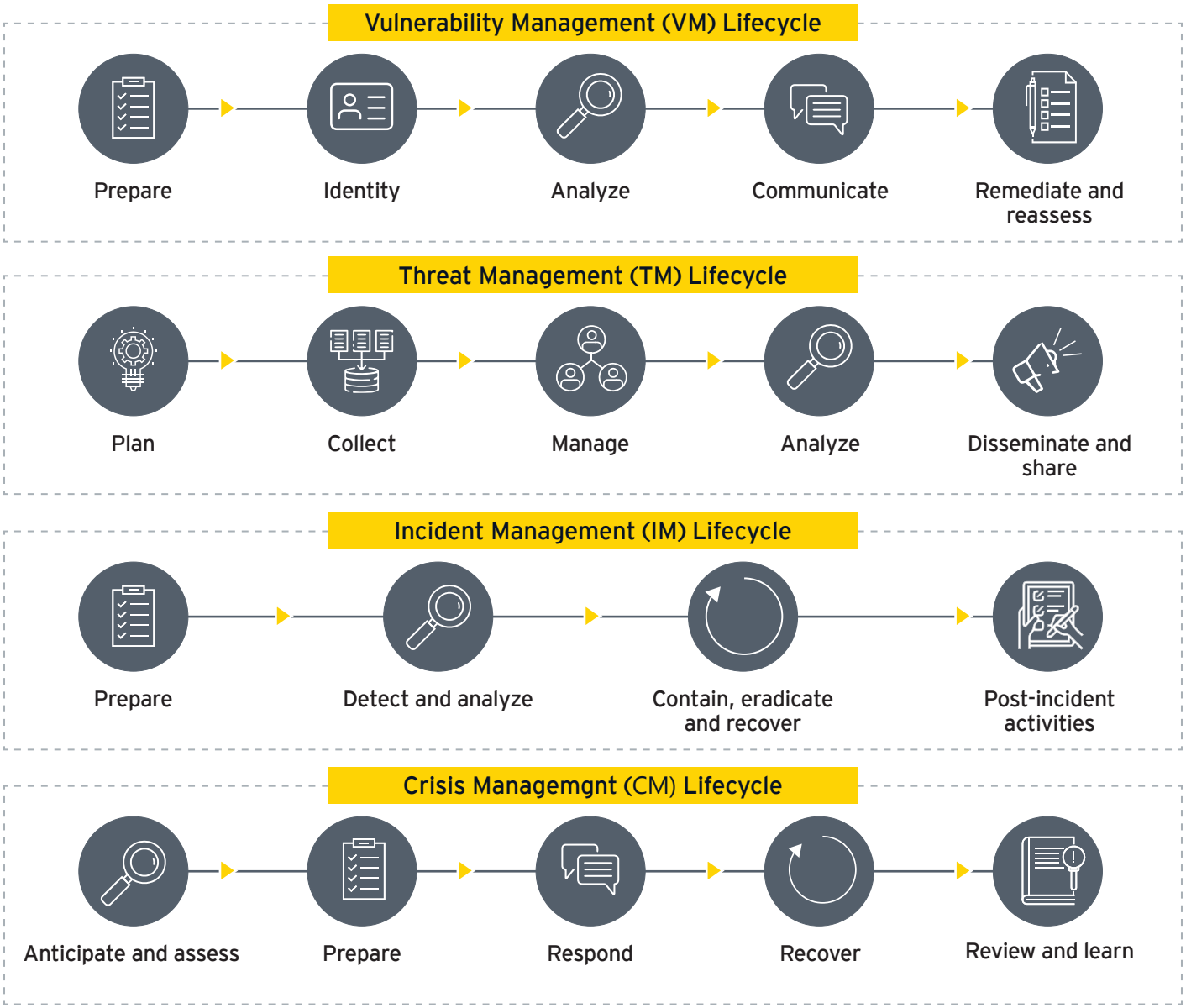


Figure 4: Domain lifecycle

The primary focus of the framework development phase should involve directions to be provided to ICT organizations to:

- Better understand, manage and diminish the potential cybersecurity risks
- Act as a core enabler for resiliency across critical operations and service delivery
- Empower the ICT organization to identify, prioritize and manage the projects within the cybersecurity program, which allows for optimal level of cybersecurity investment and budget spending
- Provide every member of the ICT organization with a common language to understand the required level of cybersecurity practices and a consistent methodology for assessing maturity
- Improve communication within the ICT organization, based on the adoption of the framework and requirements stated within the guidelines, to facilitate a better understanding of the cybersecurity requirements by key stakeholders and the board
- Act as an enabler – in ICT organizations with mature cybersecurity programs – for understanding additional programs which might need to be considered for enhancing the cybersecurity posture or to assess maturity levels commensurate with the identified complexity levels
- Act as a catalyst – in ICT organizations that have underdeveloped or developing cybersecurity programs – for understanding cybersecurity requirements, communicating control gaps to the board, and identifying the required level of cybersecurity investment

In summary, the framework is applicable to all ICT organizations, though the applicability may vary based on the organization's present status, objectives, goals and most importantly its risk appetite.

The primary goal of the framework and guidelines developed by other nations or sectors should be to serve as a directional tool that will allow a consistent approach for assessing current cybersecurity practices and management techniques in line with the framework's principles, industry standards, and good cybersecurity practices.

05

ICT sector landscape

As more and more nations launch a new generation of giga-projects and accelerate their modernization effort to create a sustainable, investor-friendly business environment, an onslaught of digital technology is unavoidable. The push to establish the foundations of a digital nation is stronger than ever, and it will necessitate high levels of collaboration among ICT businesses, which are the essential facilitators of a digital nation-state. Shifting industry dynamics and evolving digital transformation plans across the world are continually prompting organizations internationally to innovate and explore new technologies and delivery models.

As a result, a complex ecosystem with new cybersecurity challenges is emerging. Cybersecurity must now do more than just safeguard technical assets; it must also assure business resilience. A greater emphasis on digital enablement via advanced digital technologies is critical for increasing industrial activity, attracting investment, and diversifying the economy via the growth of public service sectors such as health, education, infrastructure, recreation and tourism. Amid the global acceleration of the digital transformation agenda, the need to secure critical cyber assets has gained strategic significance for various business sectors and industries, particularly since the nation's critical infrastructure has been threatened several times in recent years. While the cybersecurity market is quite large in itself , key services will drive the majority of this growth. Global ICT spending has traditionally been product and infrastructure oriented, although growth in those sub-segments is expected to decline. International Data Corporation (IDC) predicts that cybersecurity market growth over the forecast period (and beyond) will be driven by spending on professional services, which mainly consist of cybersecurity advisory and consulting, cybersecurity integration and implementation, and managed cybersecurity services.

With many digital transformation initiatives in the ICT sector globally, the significance of cybersecurity for the nation's economy and outcomes for citizens and enterprises is humongous.

Multiple initiatives should be undertaken to enhance the overall digital cybersecurity posture of the nations and the ICT sector, such as the establishment of a national cybersecurity authority, an ICT sector-specific cybersecurity framework and a national cybersecurity strategy.

06 VTI and CM framework essentials

How to develop the framework and guidelines?

1. Develop LPL

Although the ICT organizations at the global level are rapidly growing, they might remain mostly underdeveloped in terms of cybersecurity procedures. As per interviews with key stakeholders of organizations, it was observed that many organizations and their employees have yet to completely comprehend their cybersecurity duties and obligations. In such a case, prior to developing the framework and related recommendations, it is required to assess the present environment across the four domains and identify critical areas for development inside the organizations, and therefore the ICT sector. While the need to perform a current state assessment should be evident based on internal discussions, the challenges might remain in terms of identifying the best possible way to go about it. By performing multiple brainstorming sessions it can be agreed that an LPL should be defined and consist of good cybersecurity practices and also leveraging industry standards such as ISO (International Organization for Standardization) 27001, NIST CSF (National Institute of Standards and Technology Cybersecurity Framework), BS (British Standards) 11200, etc. For example, during the development phase of the framework, to ensure that the local landscape was embedded within the LPL, applicable regulatory frameworks such as Saudi CITC CRF (Communications and Information Technology Commission Cybersecurity Regulatory Framework) and Saudi NCA ECC (National Cybersecurity Authority Essential Cybersecurity Controls) were given a high degree of importance. The resulting outcome is the LPL which essentially consists of the following components:

Company profiling

The company profile questionnaire is a five-category model to be used to categorize entities into five-tiers based on the size, type, and complexity of operations for the organization being evaluated. The organization profile exercise includes a variety of parameters that impact an organization's operations, including but not limited to the number of workers, the number of offices, recent changes in the IT infrastructure and the number of cyber attacks faced.

Domain assessment

Following the identification and definition of techniques for classifying organizations, the next stage is to design a strategy for analyzing the present condition of the organizations in relation to the four domains such as vulnerability, threat, incident and crisis management. To do this, a five-step maturity model that categorizes organizations based on the cybersecurity posture seen thus far within the organizations is developed. The maturity model is designed in such a way that it can be utilized by organizations to undertake self-assessment and identify the necessary sequence of steps required for an organization to attain maturity level. Initial, Managed, Defined, Quantitatively Managed, and Optimizing are the recommended maturity stages. Each maturity level builds onto the capabilities established in the preceding level. The higher degrees of maturity are based on industry standards, best practices in cybersecurity, and appropriate regulatory requirements.

Significance

Defining the LPL is an essential step, given its significance in identifying strengths and weaknesses across the organizations within the ICT sector. The alignment of the LPL with good cybersecurity practices, industry standards and applicable regulatory frameworks ensures that the organizations are assessed according to practices and capabilities that the industry requires to keep cyber attacks at bay. Going by EY experience, we believe that the LPL serves as a precursor to the ultimate framework and guideline and paves the way for nations and organizations to understand focus areas that demand greater attention across the ICT sector. Additionally, a leading-in-class five-step maturity model for the four domains ensures that the organizations are not only identifying their cybersecurity weaknesses but also are being made aware of essential cybersecurity practices that would be needed to upscale their cybersecurity posture. In turn, the LPL leads to further conversations across organizations, regarding investments in upgrading cybersecurity capabilities and practices.

2. Current state analysis

Having designed the methodology and approach to conduct a current state analysis, the next step involves identifying a set of organizations that will form part of a pilot assessment. From a broad list of organizations, the most prominent and applicable ones are selected. To get at this point, it is recommended that organizations are classified as small, medium, or big, based on pre-defined criteria that consider organizational features and IT services supplied. To categorize the organizations and guarantee a broad variety of IT organizations are included in the pilot project, subjective elements such as the types of services provided by the organization are paired with objective factors, such as the number of workers and approximate yearly turnover.

To ensure smooth conduct of the pilot exercise, it is recommended to use a digital tool to capture the responses of the organizational representatives and assist in consolidating responses across the pilot organizations. The responses are collated to prepare dashboards that provide a sector-wide view as well as a company-level view, to assist the nation and the organizations to understand the existing cybersecurity posture. The methodology is illustrated as follows:

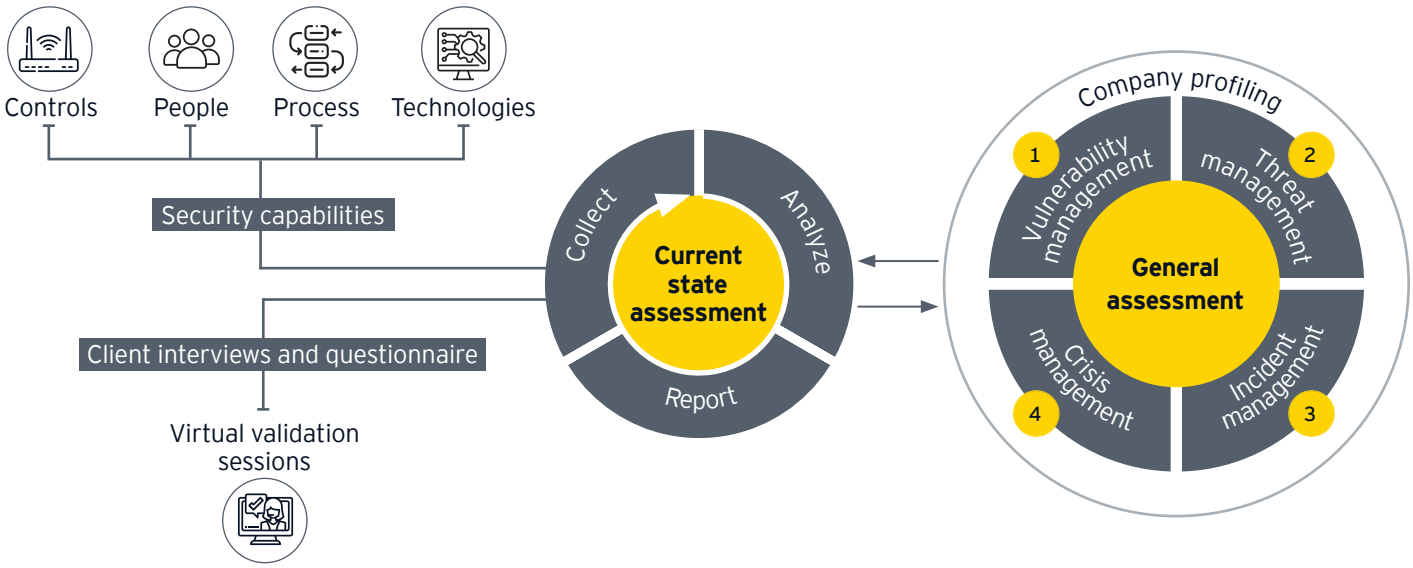


Figure 5: Current state analysis methodology

The comprehensive exercise provides insights into the current state of practices and capabilities across the four domains.

Significance

The current state analysis provides a view of the existing cybersecurity landscape to the nations as well as the organizations being assessed. The results will show whether the maturity appears to be evolving across all four domains, with the need to invest in people, process and technology to upscale cybersecurity maturity. The results of the current state analysis are used as input into the framework to determine the guidelines to be developed and prioritize specific areas. The pilot exercises also ensure that key companies within the ICT sector are made aware of persistent weaknesses within their IT environment. It is also believed that the current state analysis exercise results in the identification of common themes underpinning low levels of maturity across organizations. These key areas and themes are considered during the framework development process and have a higher degree of focus in the domain-associated guideline documents.

3. Benchmarking

The necessity for a benchmarking effort is motivated by nations' desire to comprehend effective cybersecurity procedures developed by other nation-states (and possibly their critical sectors) and global practices. While the necessity is obvious, the procedure for conducting the benchmarking exercise needs to be addressed and finalized. It is recommended to define a multi-criteria selection process that considers global cybersecurity indices and other qualitative criteria, such as availability of documentation and levels of digital development in the countries, to ensure smooth delivery and selection of the countries to be included in the benchmarking exercise. Applying these concepts, EY teams benchmarked against the global services of six countries that were chosen.

Rationale for selection

Recommended countries at regional, national and international levels with available English documentation:

- Geographical proximity, cultural similarity to KSA, presence of AE-CERT, established information assurance regulations.
- Self-developed cybersecurity implementation framework, G20 Country.
- Established implementation plan to the national-level cybersecurity strategy, presence of a formal Cybersecurity and Infrastructure Security Agency, G20 Country.
- Cultural diversity, technology innovative country, Smart Cities initiative.
- Defined cybersecurity legislation, established digital service providers standard.
- Established implementation plan to the national-level cybersecurity strategy, contribution to the international cybersecurity standards, G20 Country.

Figure 6: Countries selected for benchmarking exercise and associated rationale for selection

The benchmarking technique should make use of an IT – Capability Maturity Framework that is tailored to match the demands of the ICT industry and analyze cybersecurity practices across nations and industries. The framework should then be subdivided into Capability Building Blocks (CBBs), which serve as domains for the benchmarking experiment. Furthermore, each CBB should be separated into a five-step maturity model that would be used to measure each country state's level of maturity. To ensure the data being captured is accurate and comprehensive, it is recommended to engage an expert panel of researchers and they are responsible for evaluating sources of evidence to seek convergence and corroboration about the current topic (cybersecurity at the national level). The panel should rely on publicly available information and expertize garnered in previous similar exercises to rate the maturity for each nation-state. The countries should be scored according to the observed maturity across the multiple capability building blocks and their cybersecurity practices or capabilities should be ascertained. The benchmarking exercise should reveal if there are certain areas of improvement in terms of vulnerability, threats, incident and crisis management, indicating the need for the nation to further expand on capabilities in these domains.

Significance

The benchmarking exercise is an essential step in developing the framework and associated guidelines as they provide insights into good cybersecurity practices adopted by other countries. The exercise also assists in performing a gap analysis that differentiates between current cybersecurity practices established by the nation across the four domains to that of the other countries . The benchmarking exercise also provides a series of qualitative findings (i.e., documentation which does not necessarily increase or decrease the maturity of a particular country but provides relevant details for enhancing the guidelines being developed). Such qualitative findings, in addition to the main documents selected that cover the themes in the assessment matrix (IT-CMF) will aid in performing a gap analysis.

4. Gap analysis

The gap analysis is based on outcomes obtained through company profiling, domain assessment performed for a sample set of IT companies and results obtained by comparing the nation's current capabilities to leading global cybersecurity practices observed within the benchmarked countries.

A gap analysis report should be generated based on the gap analysis and should highlight the key areas of improvement observed with regards to the four cybersecurity domains. The cybersecurity domains are vulnerability management, threat management, incident management and crisis management (VTI&CM) within the ICT sector of the nation. The gap analysis is a critical step in the end goal of the engagement, which aims at delivering a fit-for-purpose and contextualized framework and guidelines that will assist the nation in addressing the key gaps identified and enhancing the level of cybersecurity maturity within the ICT sector.

The gap analysis should be divided into two sections: gap analysis at the national or sectoral level and gap analysis at organizational level. The gap analysis at the national or sectoral level assists in identifying the missing cybersecurity practices across the four domains to achieve the target state determined in coordination with key stakeholders. In contrast, the gap analysis at organizational level identifies the cybersecurity gaps across the four domains for each type of organization (i.e., low, medium and high). Figure 5 depicts the suggested methodology to be employed for this exercise.

Significance

The gap analysis exercise is the most critical step in defining the framework and guidelines as it assists in contextualizing the content of the documents to the needs and demands of the ICT sector. The gap analysis also provides a pathway to understand the missing pieces in order to get to the desired target state and achieve a level of cybersecurity maturity observed in higher-ranked countries included within the benchmarking exercise. The results and outcomes of the gap analysis serve as a significant input in the framework and are to be referred to at several instances during discussions and brainstorming sessions. The outcomes of the benchmarking exercise should also enable further enhancement and upgrade of the guidelines on a recurring basis.

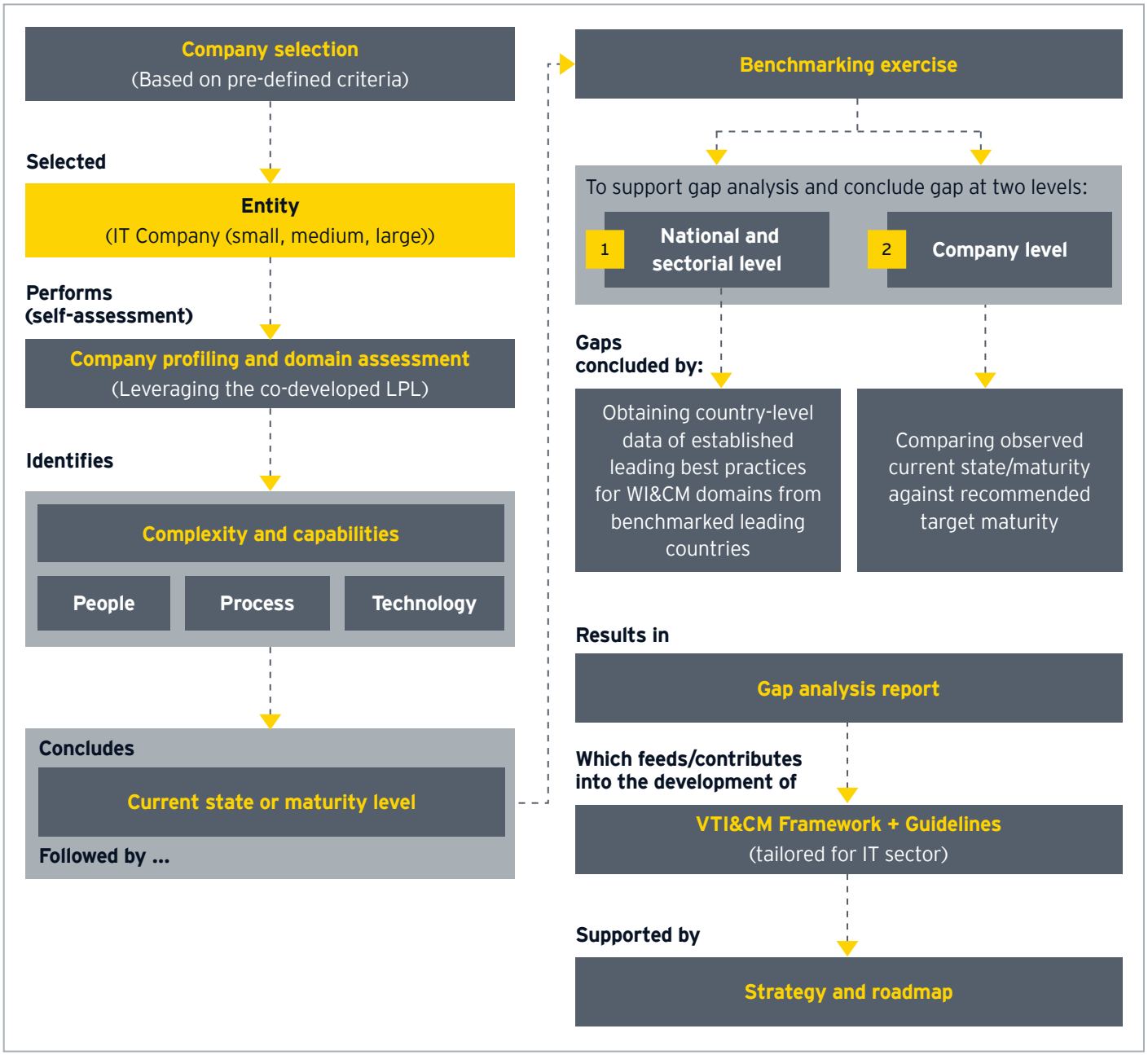


Figure 7: Gap analysis methodology

5. Framework and guidelines

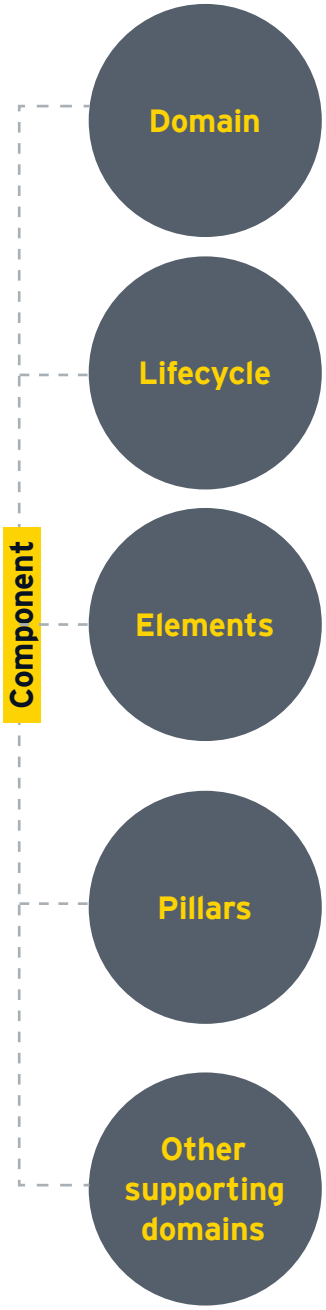
In order to enhance the digital cybersecurity posture of the ICT sector, the nations should embark on a path that ultimately contributes to the development of a framework and guidelines that comprises four domains that are essential for an effective cybersecurity defense program: vulnerability, threat, incident and crisis management.

The issuance of the framework and the associated guidelines is to support the companies achieve the required level of maturity and to build a robust infrastructure along with the necessary cybersecurity controls. The adoption and implementation of the framework is a vital step to ensure that the nation's ICT sector is resilient and capable of detecting and containing cybersecurity threats and attacks before they impact the current status quo. The framework should also aim to build a better working environment in line with the country's vision to ensure cyber threats and risks are appropriately monitored and managed throughout the sector.

Framework

Domains and sub-domains

The following table depicts the design structure of each of the four domains, where each domain includes a lifecycle that is broken down into elements that encompass a set of required activities to support the capability building based on three pillars (i.e., people, process, technology). The detailed guidelines for each domain will provide particulars on these elements and relevant pillars (i.e., suggested activities, metrics, RACI, skills and certifications, and suggested tools). Moreover, each domain will be associated with supporting domains that could be considered by the companies for wider coverage of the main domain.



This section of the design structure covers the four primary domains that are essential for a cybersecurity defense program. The domains should be chosen on the basis of their high significance in the overall management of threats affecting the nation. This section includes the following four domains: vulnerability management, threat management, incident management and crisis management.

The lifecycle provides a guide to ensure that cybersecurity is continually improved, and it helps companies reduce and better manage cybersecurity risks pertaining to the four domains as mentioned above.

Elements encompass specific tasks to be undertaken as part of a particular lifecycle stage of a specific domain. Each element is associated with a set of activities tagged to a defined capability level. The elements with their associated activities provide the basis for enhancing capability across the three key pillars of cybersecurity: people, processes and technology.

The pillars and associated guideline components act as enablers for the successful implementation of the requirements of a particular domain. Each pillar is essential for a company to consider, as the failure to upscale capability in any one particular pillar might result in an inconsistent and inefficient cybersecurity program. Therefore, each pillar must be well understood by the executive management of the company and its staff prior to implementation. The pillars encompass the following:

- People: RACI skills and certifications
- Processes: activities, example metrics
- Technology: tools and technologies

Other supporting domains cover the additional areas of cybersecurity that could be considered by the companies for wider coverage of the main domain.

Implementation lifecycle

The below table and the lifecycle depict a series of steps to be undertaken by companies to enhance their existing level of capability for the four primary domains namely vulnerability management, threat management, incident and crisis management at an implementation phase, at a change phase, and for continual improvement.

Approach

Implement

Upon defining drivers to increase the cybersecurity capability level in the company, the Implement approach defines how a company follows the process of complete profiling to identify the company's complexity level, assess the current capability state of the defined cybersecurity domains, and enables the company to implement improvement to achieve the expected capability levels by following comprehensive guidelines and supportive documents.

Change

Upon deciding the change in the company's environment, structure, or technologies and infrastructure, the Change approach defines how a company follows the process of re-profiling in areas of change to identify the updated company complexity level induced by the change, reassess the current capability state of the defined cybersecurity domains in areas of change, and enables the company to implement improvements to maintain the expected capability levels by following comprehensive guidelines and supportive documents.

Maintain and improve

Upon planning for maintenance and improvement of the cybersecurity capability level in the company, the Maintain and Improve approach defines how a company follows the process of maintaining the company's profile by updating the company's complexity level, reassessing the current capability state of defined cybersecurity domains and identifying gaps of implementation, and enables the company to apply corrective actions to achieve the expected capability levels or enhance them by following comprehensive guidelines and supportive documents.

Guidelines

The purpose of these guidelines is to give guidance and advice to ICT organizations on effective cybersecurity practices across the four aforementioned categories. Although the document is not mandatory, organizations are encouraged to implement the necessary level of controls to improve their cybersecurity posture. The guidelines provide a systematic and comprehensive approach to identify cybersecurity controls required to enhance cybersecurity capability levels.

The guidelines were defined in order to achieve the following set of goals

- Enable the ease of identification of effective cybersecurity and resilience improvement activities
- Enable the setting of meaningful target cybersecurity levels for companies
- Be as straightforward and cost-effective to apply as possible
- Allow companies to enhance their cybersecurity posture

Structure of the guideline

The below diagram presents the three pillars that serve as contributors in the implementation of robust vulnerability, threat, incident and crisis management capabilities in an organization. Each of these pillars is further elaborated into the guidelines. The guidelines outline the recommended lifecycle, that should be adopted to successfully implement a vulnerability, threat, incident and crisis management program that is aligned with relevant regulatory requirements and leading industry standards. Each of the lifecycle phases is supported by elements that provide at the granular guidance and to aid stakeholders responsible for implementation of the cybersecurity program.

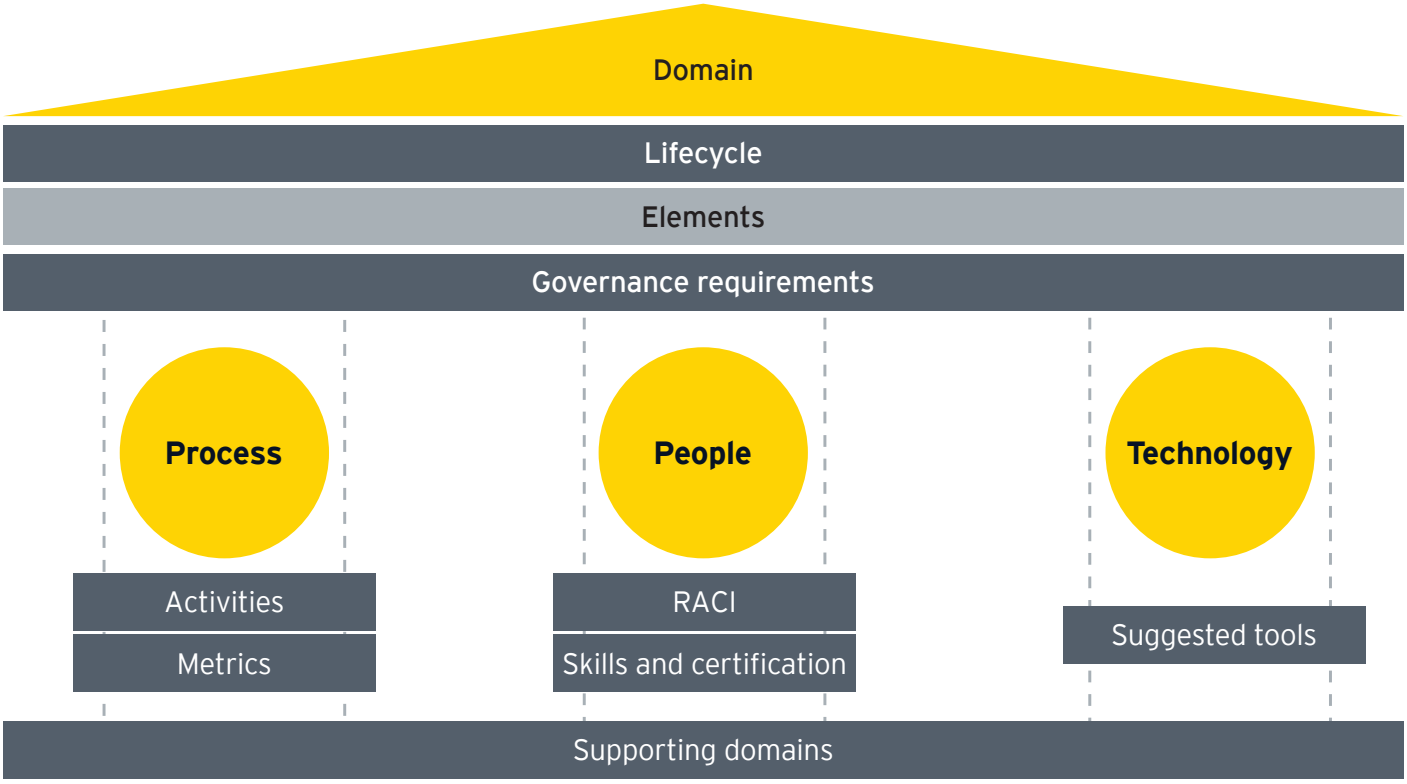
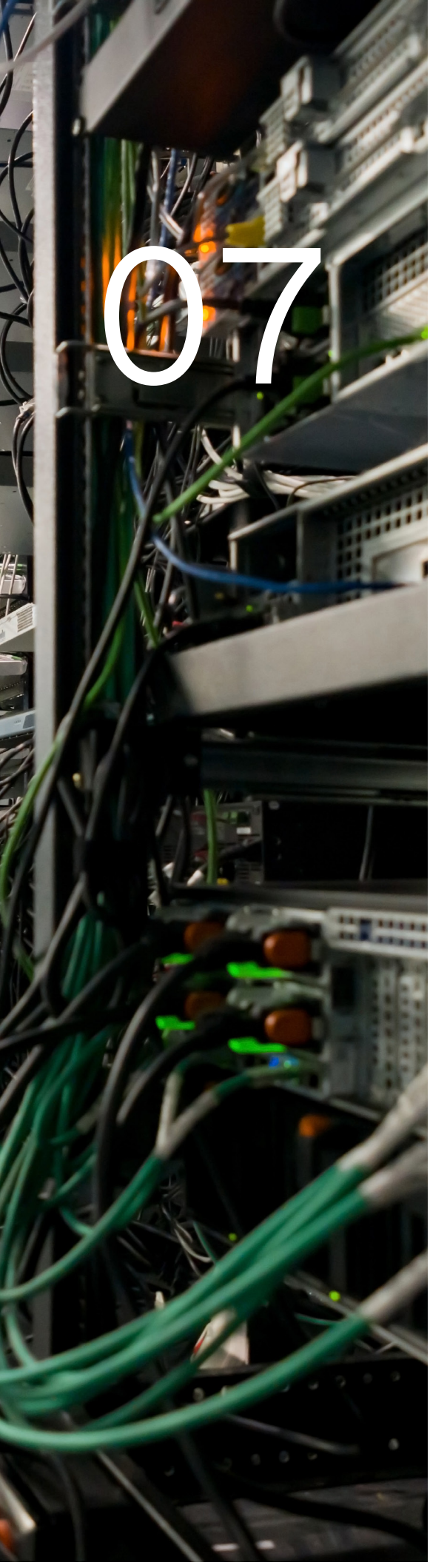


Figure 8: VTI&CM framework implementation

Significance

The framework and its accompanying principles are indicators of good cybersecurity practices that ICT organizations must adopt and execute. They offer a uniform approach for organizations to improve and grow their cybersecurity posture across the four domains as well as to assure the establishment of a robust infrastructure. In the absence of granular and precise processes for improving cybersecurity postures that are linked with size, complexity, and nature, organizations may struggle to grasp the degree of investment and competencies necessary to operate a cybersecurity program. The framework and associated guidelines aim to solve this issue by allowing organizations to identify their respective complexity level (through company profiling) and thereby identifying the level of cybersecurity maturity it needs to achieve which is commensurate with its size and complexity. The framework and guidelines that EY teams have developed and put into practice is truly considered to be one of the best-in-class as it does not consider a one-size-fits-all approach and goes into the granular organizational details prior to defining the required state or target state of cybersecurity maturity.



07

Lessons learned

1. Communication

Throughout the full procedure, from co-developing the LPL to building the structure and principles, clarity and communication will prove to be crucial ingredients for success at each phase. All participants in the exercise should be given explicit instructions on the desired outcome and should work toward a common goal; a contextualized framework that meets the demands of the ICT industry.

EY teams noted three major ingredients for effective communication throughout the procedure:

1

Open-communication channels

These are necessary as the exercise involves several subject matter resources (SMRs) who will contribute a fair deal to the success of this project

2

Executive management buy-in

Realize the importance of this project to the ICT sector, involvement and buy-in of executive management is crucial as any delays or risks encountered during the exercise could be promptly discussed and navigated in a smooth and efficient manner

3

Input from key stakeholders

Ensure that the voices of stakeholders who have had significant number of interactions with ICT companies and understand their pain points or challenges are heard and considered at each step of the project. This ensures that the project and the resulting deliverables are tailored to the needs of the ICT market and customized as required.

2. Project specificities

While each project is unique in its own right, there are some characteristics that need to be addressed across projects of similar nature:

Engagement of SMEs for each domain:

While it is safe to assume that a cybersecurity expert who has spent more than 10 years in the industry is well aware of cybersecurity practices across all domains. Domain-specific knowledge is always considered a boon because the SME can devote all of their attention to one specific focus area and share the technical know-how. Such attention to detail from the start of the project ensured that the initiative would be able to achieve effective results.

Clarity over expected outcome from the benchmarking exercise:

While benchmarking exercises seem to be the trend for most projects, ensuring that the needs of the stakeholders are well understood remains to be the challenge at the onset of a benchmarking exercise. Benchmarking exercises need to be tailored to the needs of the engagement as well as the key stakeholders and teams performing the benchmarking exercise need to be aware of the rationale behind such an exercise.

Countries to include in the benchmarking exercise:

Countries need to be carefully selected and must have a mix of regional, global and low to high cybersecurity maturity. This would ensure that the country being assessed is being benchmarked against a variety of others rather than a biased view of the scheme of things.

08

Conclusion

Sectoral cybersecurity frameworks are a trend which will continue to grow given that they take into consideration sector-specific technical know-how and expand from a national framework that is more tailor-made to meet the needs of the sector. We believe the EY approach in defining the framework along with a set of guidelines that support the implementation of the framework is leading, as it not only considers the size and complexity of the company but also addresses the needs and requirements of industry standards, applicable regulatory frameworks. It is important to note that a one-size-fits-all approach will not necessarily work in a dynamic and volatile sector such as the ICT. Therefore, a tailored approach that considers the size and complexity of the organization in question is assessed prior to identifying the required level of maturity. So, we encourage readers of this paper and sectoral authorities to truly understand the crux of this framework and pay heed to the level of details and granularities the ICT sector framework and guidelines dive into.

The approach adopted comprised of current state analysis, benchmarking and gap analysis prior to defining the framework can be customized as per the needs of other sectors. However, sectors are encouraged to consider similar exercises as it ensures that needs and requirements are well-understood prior to developing policies or guidelines. Essentially such exercises ensure that the final deliverables are a product of a series of steps that help in understanding the needs and requirements of key stakeholders and the organizations who would ultimately be the users of such deliverables.

To be cyber resilient, organizations need to constantly quiz relevant stakeholders with regards to the cyber attacks which might affect the various units and consider cybersecurity risks and threats throughout the lifecycle of technology implementation. The following table provides three core categories of cyber attacks that plague organizations and governments and produce a cybersecurity challenge that seems to keep growing in size and volume on a day-to-day basis.

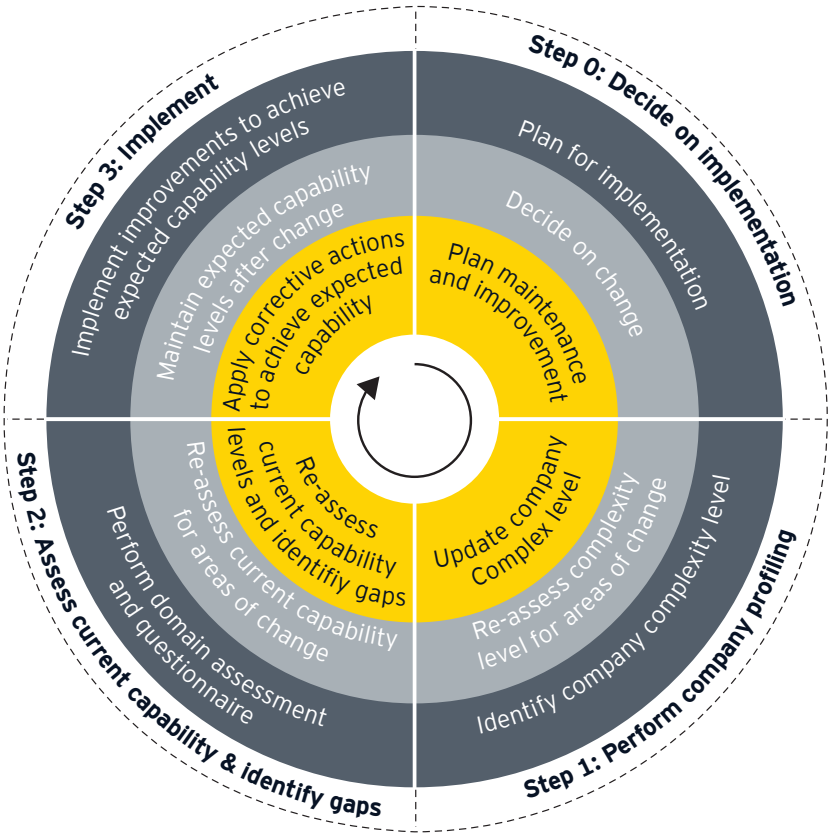
Types of cyber attacks

	Common attacks	Advanced attacks	Emerging attacks
What is it?	These are attacks that exploit known vulnerabilities using freely available hacking tools, with little expertize required to be successful.	Advanced attacks exploit complex and sometimes unknown (zero-day) vulnerabilities using sophisticated tools and methodologies.	These attacks focus on new attack vectors and vulnerabilities enabled by emerging technologies, based on specific research to identify and exploit vulnerabilities.
Typical threat actors	Unsophisticated attackers, such as disgruntled insiders, business competitors, hacktivists and some organized crime groups.	Sophisticated attackers such as organized crime groups, industrial espionage teams, cyber terrorists and nation-states.	Sophisticated attackers such as organized crime groups, industrial espionage teams, cyber terrorists and nation-states.
Examples	Unpatched vulnerability on a website, exploited using a freely available exploit kit. Generic malware is delivered through a phishing campaign, enabling remote access to an endpoint. Distributed Denial of Service (DDoS) attack for hire with a basic random demand.	Spear phishing attacks using custom malware. "Zero-day" vulnerabilities are exploited using custom-built exploit code. Rogue employees "planted" to undertake deep reconnaissance or espionage. Vendors or suppliers are exploited as a way to gain access to the ultimate target smart city.	Exploiting vulnerabilities on "smart" devices to gain access to data and/or control systems. Leveraging cybersecurity gaps created with the convergence of personal and corporate devices into one network. Using advanced techniques to avoid detection and/or bypass defense.

Organizations in the ICT sector are recommended to relook at their strategies and defense mechanisms to better counter cyber threats impacting their environment. It is important to bear in mind that an attack on an ICT organization serving the critical national infrastructure may result in a significant financial, operational and social impact as well. Therefore, in order to better counter cyber threats and attacks, organizations also need to perform proactive risk assessments and identify suitable countermeasures. In order to aid this, sectoral authorities are recommended to implement risk management guidelines that serve as tools for better cyber risk management practices across organizations.

Advantages of the framework

The effective implementation of the VTI&CM framework will allow ICT organizations to upscale their security posture and attain a level of maturity that is commensurate with their risk levels. To guide ICT organizations, the following implementation lifecycle can be considered.



Each step of the implementation lifecycle contributes to the ICT organization identifying and assessing its current capabilities and ultimately would result in well-informed senior management that can provide necessary support for the execution of a cybersecurity program. The competitive advantage lies in the fact that the nation and the ICT sector as a whole would be aware of its current capabilities and implement measures to build on the existing security posture. It would allow sectoral organizations involved in cybersecurity programs to be able to measure compliance based on reporting performed by the ICT organizations, guide the ICT organizations toward better decision-making, and ultimately provide details regarding the security posture of the sector to sectoral organizations — resulting in better coordination and identification of projects to be implemented. It is to be noted that through appropriate governance of the framework and reporting performed by ICT organizations, there is an opportunity to benchmark the ICT organizations against their peers and identify good security practices which may need to be implemented.

09

Contributors

The framework and identified components within this document were developed with the contributions and comments received from representatives of the sector and cybersecurity communities, SMEs and consultants with national and international exposure.

Listed below are the key contributors to this whitepaper:

Eng. Ahmad Alshaba
General Manager of Risk Management
and Business Continuity Center
Email: ashaba@mcit.gov.sa

Eng. Talhah Al Jarad
Advisor, Risk Management and Business Continuity
Email: tjarad@mcit.gov.sa

Majd Almjally
Governance & Compliance Director
Email: mmjally@mcit.gov.sa

10

Contacts

Samer Omar
Senior Principal, Technology Consulting
Ernst & Young for Systems and Programming WLL (Branch)
Email: samer.m.omar1@sa.ey.com

Ritesh Guttoo
Partner, EY Africa Cybersecurity Leader
Ernst & Young Ltd, Mauritius
Email: ritesh.guttoo1@mu.ey.com

Salam Shouman
Director, Technology Consulting
Ernst & Young Jordan
Email: salam.shouman@jo.ey.com

Lavnya Mohonee
Partner, Technology Consulting
Ernst & Young Ltd, Mauritius
Email: lavnya.mohonee@mu.ey.com

Siddhesh Mudbhatkal
Manager, Technology Consulting
Ernst & Young Ltd, Mauritius
Email: siddhesh.mudbhatkal@mu.ey.com

Hemkesh Jhamna
Senior Consultant, Technology Consulting
Ernst & Young Ltd, Mauritius
Email: hemkesh.jhamna@mu.ey.com

Glossary of terms

Term	Definition
Critical infrastructure	The body of systems, networks, and assets that are so critical that their ongoing functioning is necessary to maintain the security of a particular nation, its economy, and the health and/or safety of the population.
Current state analysis	A management method for identifying and evaluating a company's processes and workflows.
Cyber defense	Cyber defense is a computer network defensive technique that comprises action response, critical infrastructure protection, and information assurance for corporations, government bodies, and other potential networks.
Cyber risk	The possibility of harmful consequences resulting from failures in information systems.
Cyber attack	Any offensive move that targets computer information systems, computer networks, infrastructures, or personal computer devices is referred to as a cyberattack.
Cybersecurity framework	A cybersecurity framework is essentially a set of rules, guidelines, and best practices for managing digital risks.
Cybersecurity maturity	Cybersecurity maturity refers to an organization's skill and level of preparedness to combat vulnerabilities and threats posed by hackers.
Data-driven	A data-driven approach enables companies to examine and organize their data with the goal of better serving their customers and consumers.
Digital Nations	The Digital Nations is a network of the world's leading digital governments working together to better citizens' lives via the use of digital technology.
Digital transformation	Digital transformation is the adoption of digital technology by an organization. Common goals for its implementation are to improve efficiency, value or innovation.
Emerging technology	Emerging technologies are those whose development, practical applications, or both are yet substantially unreached, to the point that they are symbolically emerging into prominence from obscurity or nonexistence.
ICT (Information and communications technologies)	ICT is described as a broad range of technical tools and resources used to transmit, store, produce, share or exchange information.
Industry standards	A set of criteria within an industry relating to the standard functioning and carrying out of operations in their respective fields of production.
Innovation landscape	An innovation landscape method aims to foster an atmosphere in which innovation may be encouraged, socialized, created, and tested anyplace and everywhere.
IoT (Internet of Things)	The IoT refers to physical items equipped with sensors, processing power, software, and other technologies that communicate and share data with other devices and systems over the Internet or other communication networks.
RACI	RACI is an acronym that stands for responsible, accountable, consulted and informed. A RACI chart is a matrix of all the activities or decision-making authorities undertaken in an organization set against all the people or roles.
Security-by-design	Security-by-design is a method of developing software and hardware that attempts to make systems as secure and resistant to attacks as feasible using methods such as continuous testing, authentication precautions and adherence to standard programing principles.

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

The MENA practice of EY has been operating in the region since 1923. For over 98 years, we have grown to over 7,500 people united across 26 offices and 15 countries, sharing the same values and an unwavering commitment to quality. As an organization, we continue to develop outstanding leaders who deliver exceptional services to our clients and who contribute to our communities. We are proud of our accomplishments over the years, reaffirming our position as the largest and most established professional services organization in the region.

EYG no. 22-007073Gbl

ED None

ey.com