1600 CYBER

CYBER RESILIENCE GUIDE

LONDON FRANKFURT SILICON VALLEY LOS ANGELES AMSTERDAM

www.1600cyber.com

HOW TO BE CYBER RESILIENT!

Nowadays organisations are constantly facing two challenges – first, what risk do we run for cyber-attacks? And second, if cyber-attacks occur, has the Board of Directors positioned the organisation to see minimal interruptions to business operations?. This is what categorises organisations as weak or non-resilient versus being resilient.

Whenever a cyber-attack happens, the non-resilient organisation struggles to survive and resumes critical business capabilities and functions.

The cyber resilient organisation plans and forecasts against the most relevant threats, understands its risk appetite, and has procedures in place to smoothly handle cyber-attacks. Being cyber resilient blends the right mix of defensive and offensive techniques.

So – What type of organisation is yours?

If you are first category kind organisation then these ideas are for you. Here, we try to highlight key considerations regarding the current status of your organisation.

Are you Cyber RESILIENT?

If your organisation would like more details, it will be our pleasure to organise a workshop or follow-on call free of charge. We are an authorised ISACA training organisation with decades of relevant experience to help your Board reach its goals.

WHAT IS **CYBER RESILIENCE** AND HOW DIFFERENT IT IS FROM CYBER SECURITY?

Cyber criminals are often just as skilled if not more skilled than the cyber professionals you have hired to protect you. So it is inevitable that your IT Security team will not be able to prevent every cyber-attack. Cyber resilience is a direct measure of an organisation's ability to respond once a successful cyber-attack has happened.

STEP 1

You should prioritise protecting the most valued assets

Organisations must fully understand their vulnerable attack surfaces (both internet facing and within the company). With this knowledge, as part of their Risk Management Process they should characterise their risk using a mixture of qualitative and quantitative measures.

Adopting standards like ISO 31000 can help organisations better identify opportunities for improvement and threats. Most importantly engaging Cyber Consultants that follow this and similar standards ensures the Board is aligning their management of risk and corporate governance with an internationally recognised benchmark.

One of the products of proper Risk Management is the identification of the organisation's critical processes and its Crown Jewels, the assets valued most.

Take Away: To increase Cyber resilience an organisation must harden their footprint surrounding their Crown Jewels.

TIPS: IDENTIFYING CRITICAL SERVICES AND THEIR ASSETS

Goal: Identify the services required for an organisation to bounce back after a successful attack. Using the outputs from your Risk Management Process, make a complete catalogue of all IT services and attach a “Value” to each of the services. Use this Value in order to prioritize which services need to be restored first. Highest priority should be given to the services supporting each of the Crown Jewels. Lastly, after identifying assets and their relationships in the CMDB, keep the CMBD clean.

STEP 2

Identify risk based on your attack surface

Again using the outputs from your Risk Management Process, complete a risk assessment similar to the following example:

Asset	Asset Value	Which IT service asset belongs to	Threat	Vulnerability	Likelihood	Impact	Risk	Risk Rank	Treatment

A sample of the Frameworks and Risk Management standards that a Cyber Consultant will reference with your team during this process include:

- COBIT Risk Guide
- COBIT Cyber Security Guide to identify organisational most attacked risks
- ISO 31000 for organisational methodology to adopt
- ISO 27005 for Cyber security Risk Management – identifying information security risks
- NIST 800-53 for identifying necessary security and privacy controls
- COSO frameworks for internal controls

Tech Tip! Instead of documenting and managing the results of your Risk Assessment in a spreadsheet, work with a Cyber Consultant to identify the right Risk Tool.
This tool will provide the Board a much needed, enterprise level, bird's eye view of its risk. This visibility will make the Board Member much more capable of carrying out their duties.

STEP 3

Threat Identification and Prioritisation

Never will there be a single organization that has the resources to completely defend against every possible type of cyber-attack!

So Boards need to make sure that whenever an investment decision regarding Cyber security needs to be made, business and security leaders do so based on risk.

CISOs are brilliant at determining which threats pose the greatest risk and guide the C-Level investments accordingly. The CISO will factor in both past attack history and threat intelligence source. Threat Intelligence helps a CISO forecast risk based on trends, indicators of attack in Threat Intelligence communities, as well as popular and evolving Tactics, Techniques, and Procedures (TTPs).

Threat Intelligence is a valuable tool and will help the CISO identify the specific threats facing an organisation, so Boards can prioritise time and resources accordingly. The CISO should engage the IT Security team to support threat modeling, identify threat actors, and utilise threat modeling (i.e. STRIDE, DREAD. OWASP, etc.)

STEP 4

Design and Deploy

USING ISACA'S COBIT AS A FRAMEWORK TO BE CYBER RESILIENT

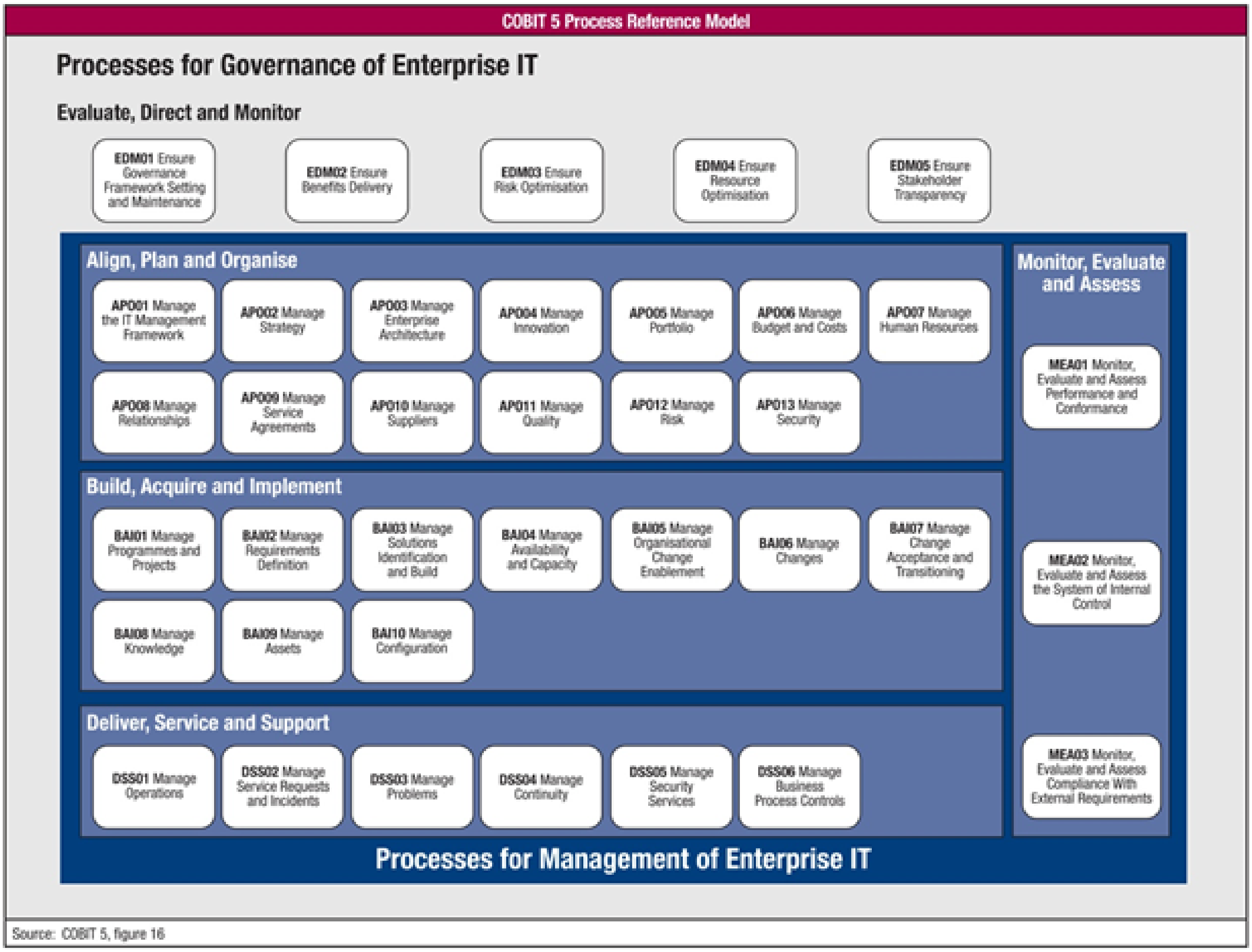
Today the IT department is an enabler for business, and business dependency on IT is very high. Thus the IT department must be governed properly. The COBIT 5 /2019 framework is the globally accepted information and technology management and governance framework. Integrating ISACA's COBIT 5 / 2019 into the design and deployment activities of an organization ultimately helps the Board ensure value results from IT and Cyber security investments. Further COBIT helps ensure that the organisation's performance as a whole is aligned with respect to handling downtimes of services, and Cyber security incidents.

CISOs would be wise to utilise COBIT 5 / 2019 during the design and deployment of activities initiated to increase Cyber resilience. COBIT 5/ 2019 provides a means to address Cyber security in a systematic way and to integrate it with security governance, risk management and compliance. Also, COBIT 5 / 2019 has taken steps to align several Cyber security Frameworks.

A Cyber security Consultant and/or CISO, using COBIT5 / 2019, can implement 7 enablers to help embed Cyber resilience into day-to-day operations.

1	Policies, Procedures and Framework
2	Organization structure
3	Processes
4	Culture, Behavior and Ethics
5	Information
6	Services and Applications, Tools
7	People, Skill and Talent and competency

For an organisation, it really becomes important to focus on all enablers and in particular the processes. If a process is absent or working at low maturity it poses severe risk. A timebound project to identify gaps and a road map for process maturity must be initiated. The following is a COBIT5 Governance and Management list. The Board is key because for successful implementation there needs to be a top down approach.



COBIT 5 Process Reference Model

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

- EDM01 Ensure Governance Framework Setting and Maintenance
- EDM02 Ensure Benefits Delivery
- EDM03 Ensure Risk Optimisation
- EDM04 Ensure Resource Optimisation
- EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise

- APO01 Manage the IT Management Framework
- APO02 Manage Strategy
- APO03 Manage Enterprise Architecture
- APO04 Manage Innovation
- APO05 Manage Portfolio
- APO06 Manage Budget and Costs
- APO07 Manage Human Resources
- APO08 Manage Relationships
- APO09 Manage Service Agreements
- APO10 Manage Suppliers
- APO11 Manage Quality
- APO12 Manage Risk
- APO13 Manage Security

Build, Acquire and Implement

- BAI01 Manage Programmes and Projects
- BAI02 Manage Requirements Definition
- BAI03 Manage Solutions Identification and Build
- BAI04 Manage Availability and Capacity
- BAI05 Manage Organisational Change Enablement
- BAI06 Manage Changes
- BAI07 Manage Change Acceptance and Transitioning
- BAI08 Manage Knowledge
- BAI09 Manage Assets
- BAI10 Manage Configuration

Deliver, Service and Support

- DSS01 Manage Operations
- DSS02 Manage Service Requests and Incidents
- DSS03 Manage Problems
- DSS04 Manage Continuity
- DSS05 Manage Security Services
- DSS06 Manage Business Process Controls

Monitor, Evaluate and Assess

- MEA01 Monitor, Evaluate and Assess Performance and Conformance
- MEA02 Monitor, Evaluate and Assess the System of Internal Control
- MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT

Source: COBIT 5, figure 16

STEP 5

Respond and Recover

This final step of the Guide recommends that Boards direct the CISO to analyse the organisation's processes, people, and technologies in place and then develop a capability to identify, prioritise, contain and eradicate cyber-attacks. The key questions:

- Do the current processes allow an organisation to respond quickly to attacks and minimise damage?
- Equally important are processes in place to fortify the exploited vulnerability and harvest lessons learned from the attack.

The end goal should be to increase response efficiency to cyber-attacks and where possible prevent future follow-on attacks. The CISO or Cyber security Consultant should implement and manage incidents consistent with the guidelines of an organisation like SANS. SANS is one of the most respected organisations with respect to Incident Handling and Response and has developed a 6-step process. These steps are taken from the SANS Incident Handling Guide:

1. Preparation—risk assessment, identify sensitive assets, define what classifies as a security incident, build a Computer Security Incident Response Team (CSIRT).
If you were following this Cyber Resilience Guide, you would have completed this in Step 1, and 2.
2. Identification—monitor IT systems and detect deviations from normal operations, and see if they represent actual security incidents. When an incident is discovered, collect additional evidence, establish its type and severity, and document everything.

3. Containment—perform short-term containment, for example by isolating the network segment that is under attack. Then focus on long-term containment, which involves temporary fixes to allow systems to be used in production, while rebuilding clean systems.
4. Eradication—remove malware from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.
5. Recovery—bring affected production systems back online carefully, to prevent additional attacks. Test, verify and monitor affected systems to ensure they are back to normal activity.
6. Lessons learned—no later than two weeks from the end of the incident, perform a retrospective of the incident. Prepare complete documentation of the incident, investigate the incident further, understand what was done to contain it and whether anything in the incident response process could be improved.

STEP 6

Conclusion

If you would like to know more about Cyber resilience or have someone from the 1600 Cyber team follow-up with you, feel free to contact us at info@1600cyber.com or visit our website: www.1600cyber.com.

Thank You.