The Need for a Digital Security Architecture

IT and security professionals tend to have a high degree of focus on tools and technology. While some place additional focus on processes, organizational structures and tasks, still others focus on policies. There are even those who are singularly focused on fulfilling a particular requirement, often driven by compliance concerns. However, there are many different aspects to be considered when managing security; they all need to work together and fit into the enterprise's needs. But there is no general model to allow steering of all capabilities required for security.

Digital security[1]—all information and technology-related activities—is highly driven by technology vendors and their market amplifiers (i.e., Gartner or Forrester), the vital market of consultants, and value-adding resellers. On the other hand, there are the malicious individuals (including state-driven activists and other actors) who have a vital interest in insecure systems and technology environments.

The key questions for security professionals and their stakeholders to ask are:

- Is what is being done enough to meet current and future needs?
- Should more be done or is the organization just following market-driven hype?
- Can resources available for security be used more effectively by shifting priorities?
- Should these resources be bundled or restructured to achieve higher value?

There will never be enough capabilities to address all the expectations of a security professional, especially if the chief information security officer (CISO) is wooed by offers from vendors, consultants and others in the vital market, or if the security professional is moving beyond professional skepticism to paranoia. It is common sense that there will never be 100 percent security. The likelihood of a breach will always be higher than 0.0 percent and the impact higher than 0. Consequently, security professionals need to aim for a certain level of business resilience toward security issues and attacks.

As part of their responsibilities, security practitioners are accountable for managing the required capabilities to protect an organization from bad things, to detect issues if something goes wrong, to respond quickly and professionally, and to recover systems and services.

But what are those required capabilities, and at what point are there enough of them? It is worthwhile to look at the digital security architecture that supports security professionals in overseeing these capabilities. The architecture does not reflect aspects of a single system or a particular service's technical architecture, but aims to achieve a comprehensive view of all capabilities and components required to keep the security ship on course without overspending or taking on undue risk (or even being unaware of the icebergs).

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2LOqaWI

Jimmy Heschl, CISA, CISM, CGEIT
Is a board member of the ISACA® Austria Chapter and head of digital security at Red Bull. He has supported ISACA on COBIT® and other topics since 2003 and is an accredited COBIT trainer.

What Is Driving Security Management?

Different drivers for digital security stem from different design factors: good practice, standards or compliance requirements; vendors and their offerings; information from industry peers; risk catalogs and identified issues; and more. All these include diamonds and rust; some drivers are more beneficial than others. However, there are limiting factors such as budget or resource constraints or dependencies on legacy environments. For security professionals, the need is to find the right priorities and feed those into a security management system.[2] A security architecture helps to identify blind spots (or areas for improvement) as it provides a comprehensive and digestible overview of the components required to manage security.

> “THERE ARE SEVERAL COMPONENTS IN THE SECURITY MANAGEMENT SYSTEM THAT NEED TO BE IDENTIFIED, PRIORITIZED, REALIZED, OPERATED AND OVERSEEN IN SMART WAYS.”

There are several components in the security management system that need to be identified, prioritized, realized, operated and overseen in smart ways. These components can be policies, tools, skills and other types of capabilities. These components of the security management systems are not silos. Systems analyzing incoming emails to identify spam and malicious emails, those working on endpoints to identify suspicious behavior, and the network controls used to identify communication with sinkholes, can be seen as different tools, but they should work together, not only in prevention and detection, but also in response and in the ongoing improvement of control. The same goes for components such as the business entities and functions accountable for these issues. It is not just an isolated security operations center (SOC) issue; there are also service owners, a service desk and end users involved in preventing (or acting on) security issues. And there is a dependency and relationship between principles, policies, guidelines, and the processes and procedures. All these components have an interdependency that can be taken as a given or that can be addressed and improved as components of a professional management system. They need to work closely to properly address security risk factors, threats and vulnerabilities that the organization faces. But it is not the objective of security management to address risk, threats and vulnerabilities; the underlying goal is to foster resilience against these to allow the business to focus on relevant business goals, such as satisfied customers, profitability, growth, innovation and a solid ecosystem.

The Architecture Model

The aim of a digital security architecture is to combine good practice from the key guiding standard shaping cybersecurity: the US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)[3] and the management and governance framework COBIT®.[4]

Other standards of good practice such as the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standard ISO/IEC 27000,[5] The Open Group Architecture Framework (TOGAF)[6] or ITIL[7] can be seen as additional points of reference to ensure the completeness of components when seeing its content as process, tool, guidance or other component type. There is no contradiction in the standards, and different mapping exercises can prove that there is no substantial difference in the standards other than issuing sources and evangelists’ personal views.

The Approach for a Digital Security Architecture

There is a long list of core drivers for a sound approach toward security, but what can be done to achieve all the required components?

The approach for the security architecture proposed herein is a combination of:

- A security process
- Layers of technology (that are relevant for security)
- Components for a management system

Security Process

The NIST CSF outlines five key security functions (identify, protect, detect, respond and recover) that are the cornerstones of a security process.[8] This groundbreaking work from NIST[9] is used as a basis for the security process:

- **Manage**—Organizational understanding to manage security risk to systems, assets, data and capabilities. The activities are foundational for the other functions and help explain the business context and the resources that support critical functions by anticipating threats and vulnerabilities. Examples include asset management, planning guidance and resilience.
- **Prevent**—Safeguards to ensure the security (availability, integrity, confidentiality) of services. The activities limit or contain the impact of a potential security event. Examples include access control, awareness and training; data security; information protection processes; and procedures, maintenance and protective technology.
- **Detect**—Activities to identify the occurrence of a security event. This function enables timely discovery of security events. Examples include anomalies and events, security continuous monitoring and detection processes.
- **Respond**—Activities to take place after a detected security event and efforts to contain the impact. Examples include response planning, communications, analysis, mitigation and improvements such as enhanced protection on other components to deter further incidents.
- **Recover**—Activities to restore any capabilities or services that are impaired due to a security event. These activities support timely recovery to normal operations to reduce the impact of a security event. Examples include recovery planning, recovery testing and communications.

When applying the structure, it turns out that the last two functions—respond and recover—have considerable overlap. Hence, these have been combined to be "respond and recover."

Layers of Technology

Information technology can—as shown successfully in the Zachman architecture framework[10] or the ISO/IEC Open Systems Interconnection (OSI) model[11]—be shown as different layers. For the purposes of this discussion, the layers to be looked at include:

- **User**—Internal or external users, business processes, roles, accounts and rights, administrators, service accounts, physical access, etc.
- **Client**—Standard or individual client PC/Mac, mobile device or removable media
- **Application**—Business and web applications and the like
- **Information**—Digital information in any form (e.g., files, email, collaboration posts and messages)
- **Infrastructure**—Technical infrastructure (e.g., servers, networks, databases)
- **Service provider**—Vendors providing services such as cloud and data center

Governance and Management System Components

The leading source for governance and management of IT is COBIT. COBIT® 2019[12] matured the concept of enablers introduced in COBIT® 5,[13] and these components can be seen as different types of levers to address a focus area, such as cybersecurity. From an architectural perspective, it makes sense to look at the world through these different lenses and differentiate the following components:

- **Guidance**—Policies, standards, frameworks and other instructions
- **Tools**—Systems, services and other IT infrastructure in place
- **Organization**—Internal and external units or individuals
- **Information**—Repositories, reports, templates and the like
- **Process**—Defined and implemented workflows and procedures
- **Skills**—Available know-how
- **Culture**—Approaches and ethics in place

The process, the layers and the components are the three core dimensions of the security architecture. The first two can be shown as a matrix where the process steps form the columns and the layers build the rows. The matrices' fields—or boxes—can be filled with the components (e.g., which

component should be used to prevent security issues for clients) (**figure 3**). In practice, it makes sense to differentiate between the different types of components and have a separate matrix—or architecture view—of tools, one for organization and so on.

> “THE PROCESS, THE LAYERS AND THE COMPONENTS ARE THE THREE CORE DIMENSIONS OF THE SECURITY ARCHITECTURE.”

Objects and Their Attributes

The objects (e.g., tools or organizational units) can be assigned to one or more boxes in the matrix. In many cases, it makes sense to assign more than one field. It is not mandatory to aim for a 1:1 relationship. The objects can be equipped with different attributes that help further identification or filtering. Attributes can include owners (e.g., service owners for tools or responsible roles for maintenance of policies), costs, maturity and various other attributes that can help to differentiate different types of objects. An easy way to differentiate the objects is by adding colors or symbols. There is, however, a trade-off between the number of attributes, the effort to maintain the matrix and the value add of insight. Options to differentiate should be selected carefully and can be expanded over time.

Risk, Threats and Vulnerabilities

Most organizations have a specific risk model or list of risk factors. A valuable resource for risk can be found in *COBIT® 5 for Risk*,[14] in which approximately 100 different risk scenarios (and references to management and governance practices) are elaborated on in detail. A selection of relevant risk scenarios, threats or vulnerabilities (RTV)[15] is useful. There are RTVs with a direct impact to security management or information and those with an impact on security of services. All of them add up to issues outside a typical security area (e.g., risk as impact on safety, impact on product quality, business process efficiency, reputation or compliance risk beyond information-related topics). An overview of prioritized risk scenarios for security management can be found in **figure 1**.

Further risk scenarios (or merely threats and vulnerabilities that might end up as risk) stemming from information and technology areas are shown in **figure 2**.

Applying the Model

The model described previously was not created for an academic purpose. It has a clear objective in mind: having a model that helps answer the key questions of security.

Architecture Views

Understanding issues and weaknesses is often achieved by a simplified view of a complex environment. The architectural views show a simplified illustration of process and layers and put focus on a single component. This is shown in **figure 3**, and this view will be used to further populate the process and the layers with the objects supporting them.

This architecture view can be used to:

- Summarize common or good practice to provide a uniform understanding of applicable capabilities
- Consolidate the current state of coverage
- Identify areas for improvement

By only showing one component type, the view is kept as digestible as possible. **Figure 4** is an example of a view showing only the tools component type populated with the common practice tool sets as objects. Note that these objects show generic types of tools but, for a specific organization, it should make a reference to the specific solutions, applications and products.

Other architecture views (matrices) can contain objects for the processes, information, guidance, etc.

Figure 1—List of Risk Scenarios, Threats and Vulnerabilities

Security Management	Lack of awareness	Risk of little or no awareness on security-related risk and threats to the enterprise operations
	Lack of transparency	Risk of little or no transparency around the organization's exposure to security threats and risk
	Lack of priority	Risk of having little focus on security in system/service development and operation
	Lack of resources	Risk of lack of resources to address security and implement adequate capabilities to manage, identify, respond to and recover from security issues
	Lack of control	Risk of lack of oversight and steering on capability's adequacy and effectiveness
	Lack of flexibility	Risk of lack of flexibility in applying or adapting security controls (e.g., legacy technology, vendor buy-in)
Information Security	Impact on confidentiality	Risk that information is made available or disclosed to unauthorized individuals, entities or processes
	Impact on integrity	Risk to accuracy and completeness of data over its entire life cycle (i.e., no unauthorized modification)
	Impact on availability	Risk that information (or underlying services or systems) is not available when needed

Figure 2—Risk, Threats and Vulnerabilities Stemming From Information and Technology Areas

RTV AREA	Examples
Applications	Insufficient logging, input validation, application/application programming interface (API) abuse, insecure development, lack of authorization, inadequate availability, access to configuration, logic error, session management, lack of access control, weak encryption, exception handling, memory/garbage collection, technical vulnerability (e.g., operating systems, databases), zero-day exploits, buffer overflow
Websites	Defacement, cross-site scripting, injection, denial of service (DoS), domain grabbing/spoofing
Compliance	Regulatory or contractual risk of processing; data leakage; inability to inform, correct, delete or transfer
Malware and devices	Malware, unwanted applications, key logging, screen capturing, device theft/loss/destruction
Communications	Spam, blacklisting, malicious web links, surf-by, mail bombs, instant messages
Credentials	Brute-force attacks, account spoofing, hijacking, certificate issue, privileged account misuse, horizontal or vertical escalation
Social engineering	Reconnaissance, scouting/water holing, personnel (human resources [HR] infiltration), shoulder surfing, piggybacking
Operations	Human error, malicious intent, equipment theft/misuse, unhardened service, system/database failure, inadequate backup, loss of backup data/media, lack of capacity, lack of logging information
Network	Sniffing/wiretapping, man-in-the-middle (MITM), distributed denial of service (DDoS)
Facilities	Physical access, fire, water, acts of nature, data center equipment/network connection, sabotage
Partners and service providers	Disgruntled partner, bad cloud service, unaccepted network access
Advanced persistent threats (APTs)	Targeted attacks, blackmail, espionage

Figure 3—Architecture View Structure

	Manage	Prevent	Detect	Respond
User				
Client				
Application				
Information				
Infrastructure				
Service Provider				

Assessing the completeness and adequacy of the current capabilities in place can be done easily, and it is primarily driven by the security professional's own demand and environment to address certain aspects rather than being driven by products and the vital security market.

A recommendation to assess the adequacy of components in place is to use the general good practices for a certain component in a single box (e.g., prevent and client) and check if the tools in place address the generic practices listed in the model and capture options for improvement. Discussion with peers and stakeholders helps, but the most important driver is the professional judgement of the CISO. Seeing a gap can aid professionals in identifying, addressing and closing the issue. So the CISO, rather than being constantly frustrated, can have oversight and gain control to complete his or her duties in a responsible and diligent manner.

Another View on Components—The RTVs

All components address one or more risk scenarios, threats or vulnerabilities, and one example is provided in **figure 5**. The chart can, of course, include other components such as guidance, processes, etc., but was limited to a selected view herein.

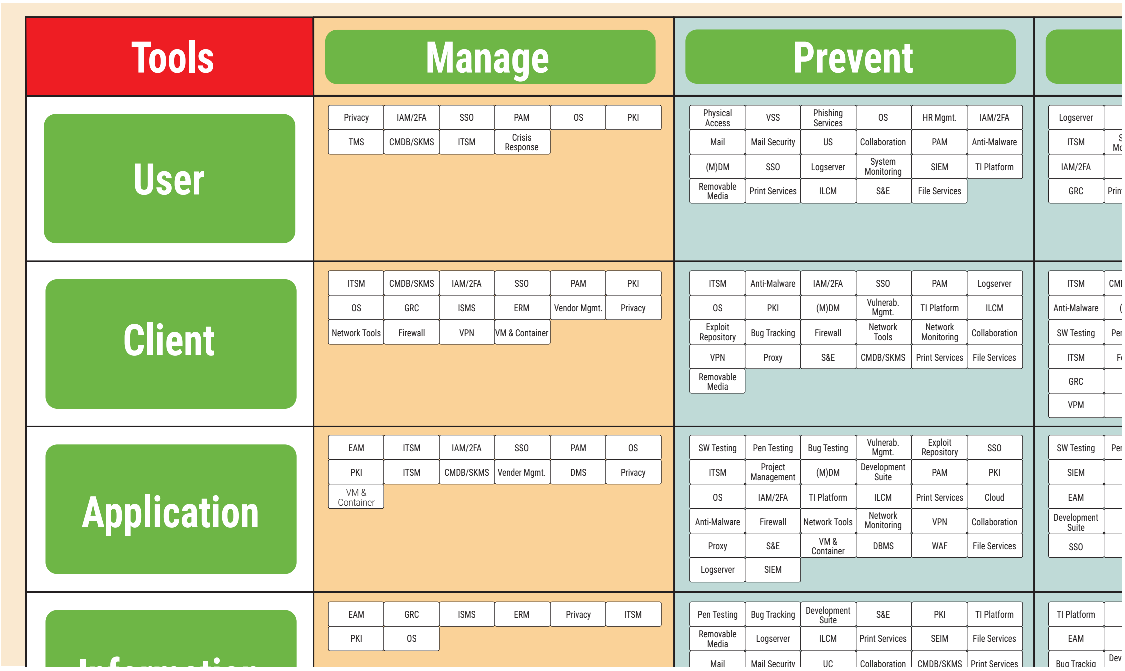
As all generic objects are linked with RTVs and they appear on certain boxes in the architecture view, it is fairly simple to take the perspective from a single RTV and assess its coverage. The views allow a straightforward overview on which components (here, tools) are in place to mitigate the risk. Hence, it is rather easy to assess the capabilities in place across all layers and the process stages. Consequently, an assessment can be done easily to clarify which components are addressing the RTV on which layer(s) and at which process stage(s). **Figure 6** shows the example of credentials for the corresponding architecture view on the tools.

This overview provides a straightforward assessment of adequate coverage of RTVs and oversight on the capabilities in place. Of course, a closer look is beneficial to finalize the assessment. A fool with a tool is still a fool, after all, but an expert supported by a tool can be smarter in identifying areas that need further improvement and also areas where adequate capabilities are in place.

The Times They Are A-Changing

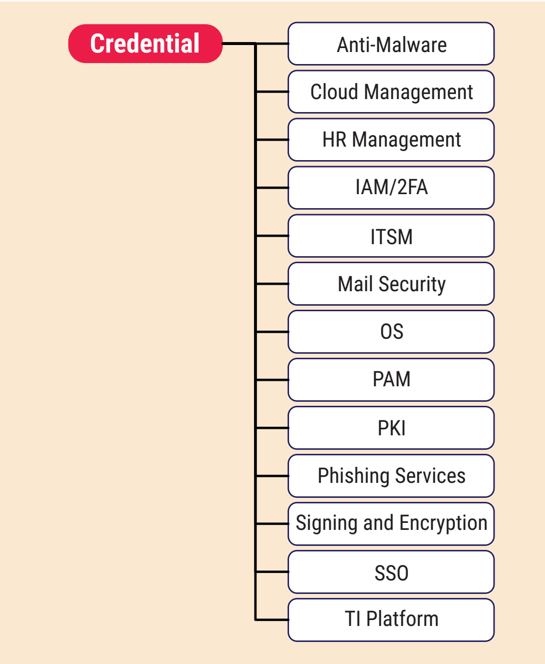
As the architecture evolves over time, it is imperative to keep the model current and forever young, and use it as a methodology to keep track of progress, manage the pace of addressing

Figure 4—Excerpt of Architecture View of the Component Tools



Tools	Manage	Prevent		
User	Privacy IAM/2FA SSO PAM OS PKI TMS CMDB/SKMS ITSM Crisis Response	Physical Access VSS Phishing Services OS HR Mgmt. IAM/2FA Mail Mail Security US Collaboration PAM Anti-Malware (M)DM SSO Logserver System Monitoring SIEM TI Platform Removable Media Print Services ILCM S&E File Services	Logserver ITSM IAM/2FA GRC	S Mo Prin
Client	ITSM CMDB/SKMS IAM/2FA SSO PAM PKI OS GRC ISMS ERM Vendor Mgmt. Privacy Network Tools Firewall VPN VM & Container	ITSM Anti-Malware IAM/2FA SSO PAM Logserver OS PKI (M)DM Vulnerab. Mgmt. TI Platform ILCM Exploit Repository Bug Tracking Firewall Network Tools Network Monitoring Collaboration VPN Proxy S&E CMDB/SKMS Print Services File Services Removable Media	ITSM Anti-Malware SW Testing ITSM GRC VPM	CMI (Per F
Application	EAM ITSM IAM/2FA SSO PAM OS PKI ITSM CMDB/SKMS Vender Mgmt. DMS Privacy VM & Container	SW Testing Pen Testing Bug Testing Vulnerab. Mgmt. Exploit Repository SSO ITSM Project Management (M)DM Development Suite PAM PKI OS IAM/2FA TI Platform ILCM Print Services Cloud Anti-Malware Firewall Network Tools Network Monitoring VPN Collaboration Proxy S&E VM & Container DBMS WAF File Services Logserver SIEM	SW Testing SIEM EAM Development Suite SSO	Per
Information	EAM GRC ISMS ERM Privacy ITSM PKI OS	Pen Testing Bug Tracking Development Suite S&E PKI TI Platform Removable Media Logserver ILCM Print Services SEIM File Services Mail Mail Security UC Collaboration CMDB/SKMS Print Services	TI Platform EAM Bug Trackig	Dev

Figure 5—Objects Related to a Single RTV



improvements, and also communicate the status of current and future coverage and plans to stakeholders.

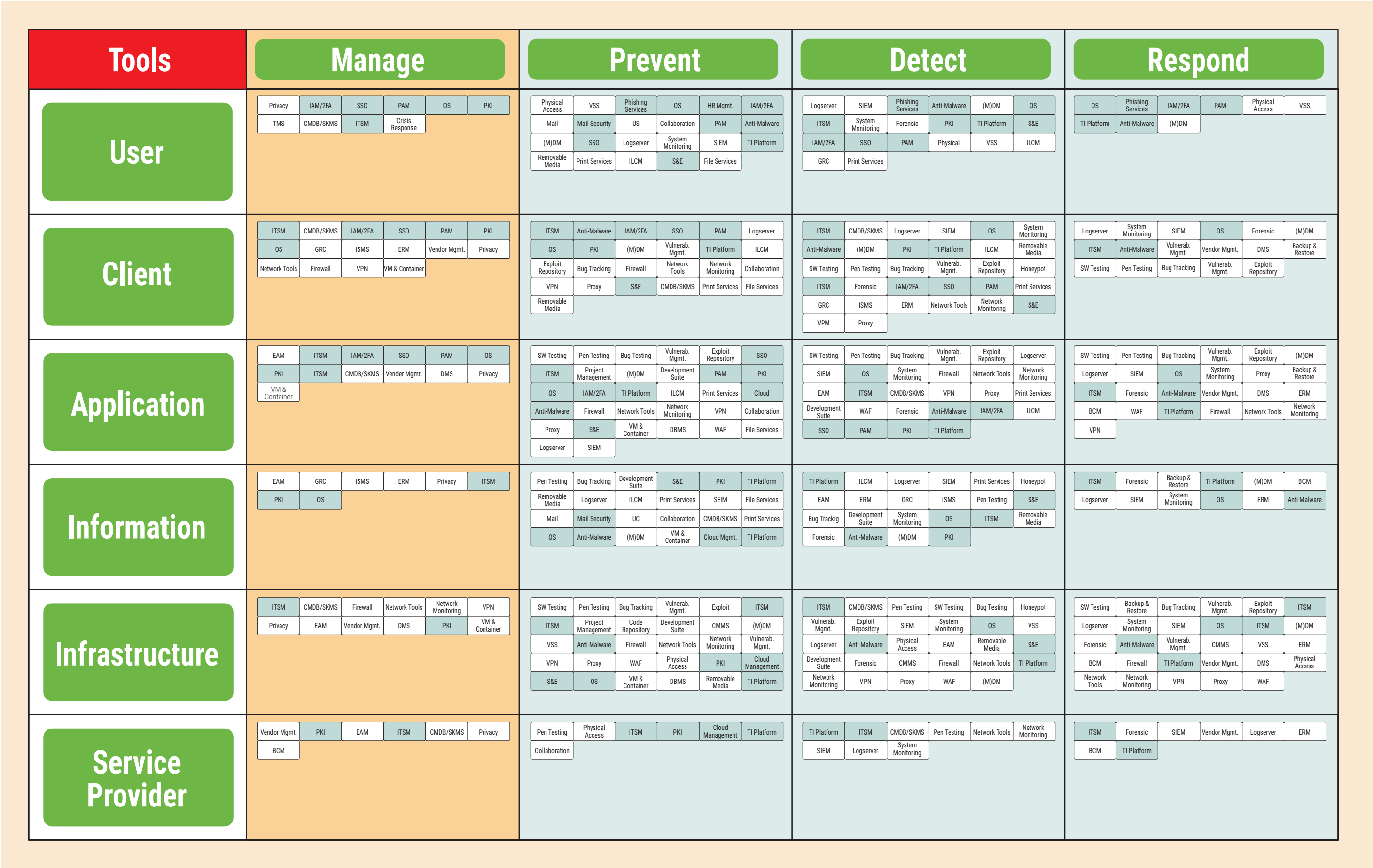
A Note on Tool Support

Software tools to handle the inherent complexity of the security architectures' components and relationship are, of course, beneficial. The process4.biz tool can be used to extend Microsoft Visio's graphical front end with customization of object data and a database link that manages the various relationships between objects when they are assigned to one or more boxes in the architecture view. And it also graphically handles the relationships between RTVs and the objects. A generic reference model that can be adapted and adopted to individual needs will soon be available with the process4.biz tool.

Endnotes

1 The term "digital security" was selected to reflect a focus on digital information (or information security) and broaden cybersecurity with the perspective of internal information processing as not only issues from cyberspace should be addressed. The terms can be interchangeable when needed.

Figure 6—Architecture View for a Selected RTV



Tools	Manage	Prevent	Detect	Respond
User	Privacy IAM/2FA SSO PAM OS PKI TMS CMDB/SKMS ITSM Crisis Response	Physical Access VSS Phishing Services OS HR Mgmt. IAM/2FA Mail Mail Security US Collaboration PAM Anti-Malware (M)DM SSO Logserver System Monitoring SIEM TI Platform Removable Media Print Services ILCM S&E File Services	Logserver SIEM Phishing Services Anti-Malware (M)DM OS ITSM System Monitoring Forensic PKI TI Platform S&E IAM/2FA SSO PAM Physical VSS ILCM GRC Print Services	OS Phishing Services IAM/2FA PAM Physical Access VSS TI Platform Anti-Malware (M)DM
Client	ITSM CMDB/SKMS IAM/2FA SSO PAM PKI OS GRC ISMS ERM Vendor Mgmt. Privacy Network Tools Firewall VPN VM & Container	ITSM Anti-Malware IAM/2FA SSO PAM Logserver OS PKI (M)DM Vulnerab. Mgmt. TI Platform ILCM Exploit Repository Bug Tracking Firewall Network Tools Network Monitoring Collaboration VPN Proxy S&E CMDB/SKMS Print Services File Services Removable Media	ITSM CMDB/SKMS Logserver SIEM OS System Monitoring Anti-Malware (M)DM PKI TI Platform ILCM Removable Media SW Testing Pen Testing Bug Tracking Vulnerab. Mgmt. Exploit Repository Honeypot ITSM Forensic IAM/2FA SSO PAM Print Services GRC ISMS ERM Network Tools Network Monitoring S&E VPM Proxy	Logserver System Monitoring SIEM OS Forensic (M)DM ITSM Anti-Malware Vulnerab. Mgmt. Vendor Mgmt. DMS Backup & Restore SW Testing Pen Testing Bug Tracking Vulnerab. Mgmt. Exploit Repository
Application	EAM ITSM IAM/2FA SSO PAM OS PKI ITSM CMDB/SKMS Vender Mgmt. DMS Privacy VM & Container	SW Testing Pen Testing Bug Testing Vulnerab. Mgmt. Exploit Repository SSO ITSM Project Management (M)DM Development Suite PAM PKI OS IAM/2FA TI Platform ILCM Print Services Cloud Anti-Malware Firewall Network Tools Network Monitoring VPN Collaboration Proxy S&E VM & Container DBMS WAF File Services Logserver SIEM	SW Testing Pen Testing Bug Tracking Vulnerab. Mgmt. Exploit Repository Logserver SIEM OS System Monitoring Firewall Network Tools Network Monitoring EAM ITSM CMDB/SKMS VPN Proxy Print Services Development Suite WAF Forensic Anti-Malware IAM/2FA ILCM SSO PAM PKI TI Platform	SW Testing Pen Testing Bug Tracking Vulnerab. Mgmt. Exploit Repository (M)DM Logserver SIEM OS System Monitoring Proxy Backup & Restore ITSM Forensic Anti-Malware Vendor Mgmt. DMS ERM BCM WAF TI Platform Firewall Network Tools Network Monitoring VPN
Information	EAM GRC ISMS ERM Privacy ITSM PKI OS	Pen Testing Bug Tracking Development Suite S&E PKI TI Platform Removable Media Logserver ILCM Print Services SEIM File Services Mail Mail Security UC Collaboration CMDB/SKMS Print Services OS Anti-Malware (M)DM VM & Container Cloud Mgmt. TI Platform	TI Platform ILCM Logserver SIEM Print Services Honeypot EAM ERM GRC ISMS Pen Testing S&E Bug Trackig Development Suite System Monitoring OS ITSM Removable Media Forensic Anti-Malware (M)DM PKI	ITSM Forensic Backup & Restore TI Platform (M)DM BCM Logserver SIEM System Monitoring OS ERM Anti-Malware
Infrastructure	ITSM CMDB/SKMS Firewall Network Tools Network Monitoring VPN Privacy EAM Vendor Mgmt. DMS PKI VM & Container	SW Testing Pen Testing Bug Tracking Vulnerab. Mgmt. Exploit ITSM ITSM Project Management Code Repository Development Suite CMMS (M)DM VSS Anti-Malware Firewall Network Tools Network Monitoring Vulnerab. Mgmt. VPN Proxy WAF Physical Access PKI Cloud Management S&E OS VM & Container DBMS Removable Media TI Platform	ITSM CMDB/SKMS Pen Testing SW Testing Bug Testing Honeypot Vulnerab. Mgmt. Exploit Repository SIEM System Monitoring OS VSS Logserver Anti-Malware Physical Access EAM Removable Media S&E Development Suite Forensic CMMS Firewall Network Tools TI Platform Network Monitoring VPN Proxy WAF (M)DM	SW Testing Backup & Restore Bug Tracking Vulnerab. Mgmt. Exploit Repository ITSM Logserver System Monitoring SIEM OS ITSM (M)DM Forensic Anti-Malware Vulnerab. Mgmt. CMMS VSS ERM BCM Firewall TI Platform Vendor Mgmt. DMS Physical Access Network Tools Network Monitoring VPN Proxy WAF
Service Provider	Vendor Mgmt. PKI EAM ITSM CMDB/SKMS Privacy BCM	Pen Testing Physical Access ITSM PKI Cloud Management TI Platform Collaboration	TI Platform ITSM CMDB/SKMS Pen Testing Network Tools Network Monitoring SIEM Logserver System Monitoring	ITSM Forensic SIEM Vendor Mgmt. Logserver ERM BCM TI Platform

2 Note that the security management system is not to be confused with an application fostering a checklist approach or even a certificate that can be achieved. The management system is considered to be the appropriate combination of capabilities that supports the security governance duties (evaluate, direct and monitor) related to the governance objectives (value realization, risk optimization and resource optimization) for the focus area of cybersecurity.

3 National Institute of Standards and Technology, Cybersecurity Framework, USA, *https://www.nist.gov/cyberframework*

4 ISACA®, *COBIT® 2019 Framework: Introduction and Methodology*, USA, 2018, *www.isaca.org/cobit*

5 International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), ISO/IEC 27000:2018 *Information technology—Security techniques—Information security management systems—Overview and vocabulary,* 2018, *https://www.iso.org/standard/73906.html*

6 The Open Group, The Open Group Architecture Framework, The TOGAF Standard Version 9.2, *https://www.opengroup.org/togaf*

7 Axelos, ITIL-IT Service Management, *https://www.axelos.com/best-practice-solutions/itil*

8 National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, USA, 2018, *https://www.nist.gov/cyberframework/framework*

9 In this definition, the function "identify" is referred to as "manage" as it better summarizes the planning and oversight of implementation and operation of required capabilities. Similarly, the term "prevent" is used in line with the common language of controls in the auditor's universe, and "protect" has a connotation of a military, not a business approach.

10 Zachman International Enterprise Architecture, Zachman Framework, *https://www.zachman.com/*

11 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 7498-1:1994 *Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model*, Switzerland, 1994, *https://www.iso.org/standard/20269.html*

12 *Op cit* ISACA, COBIT 2019

13 ISACA, COBIT® 5, USA, 2012, *www.isaca.org/COBIT/Pages/COBIT-5.aspx*

14 ISACA, *COBIT® 5 for Risk*, USA, 2013, *www.isaca.org/COBIT/Pages/Risk-product-page.aspx*

15 There is not necessarily any differentiation between those types as it is not important if one is a threat or a vulnerability or if it can be shown as a risk (i.e., it is hard to have a valid model for a quantified risk when considering likelihood, ease of exploitation, direct and indirect impact, in assessing inherent or residual risk for a vulnerability). All three types simply mean there is something to do.