EBA consult on guidelines on ICT and security risk management

Comments from ISACA European Chapters Workgroup

Overview

Following the "European Banking Authority (EBA)" Consultation on ICT and security risk management (EBA / CP / 2018/15), a group of professionals members of ISACA European chapters met to analyze and document. The main objective of this initiative was to ensure a coordinated response from a group of professionals who over the years have collaborated with ISACA and to promote their good professional practices in the areas of ICT audit, risk and control.
With this initiative, participants intend to demonstrate to EBA their willingness to ensure an adequate alignment of EBA's normative requirements with the ISACA good practices used by professionals and their organizations, promoting a set of synergies that allow the adoption of a common language, especially at the level of security, risk, control and functions, ie second and third line of defense.
As in past initiatives such as the Sarbanes-Oxley Act.[1], the NIST's cybersecurity framework[2]; or the requirements of the European Network and Information Security Agency (ENISA)[3], the alignment of requirements with management and control practices of ISACA, in particular its COBIT framework, has enabled professionals to better understand the requirements, but above all, to better guide the practices to be adopted in order to respond effectively and efficiently.
In this context, and taking into account the recent launch of the COBIT 2019 framework[4] we are confident that future initiatives to align EBA requirements with ISACA good practices could be of added value to European professionals and organizations, and we hope that our contribute can contribute to bring the two organizations more close.

Reviewers

- Bruno Horta Soares, ISACA Lisbon Chapter (coordinator)
- Francisco Guimarães, ISACA Lisbon Chapter
- Francisco Lopes, ISACA Lisbon Chapter
- Feargal O'Neill, ISACA Ireland Chapter
- João Antunes, ISACA Lisbon Chapter
- Joris Vredeling, ISACA Madrid Chapter
- Luca Pertile, ISACA Milan Chapter
- Luka Milinkovic, ISACA Belgrade Chapter
- Peter Marti, ISACA Switzerland Chapter
- Petr Hujnak, ISACA Czech Republic Chapter
- Pierluigi Satori, ISACA Venice Chapter

---

1 http://www.isaca.org/About-ISACA/Press-room/News-Releases/2014/Pages/ISACA-Issues-Updated-IT-Control-Objectives-for-Sarbanes-Oxley.aspx

2 http://www.isaca.org/About-ISACA/Press-room/News-Releases/2014/Pages/New-US-Cybersecurity-Framework-Developed-by-NIST-Features-COBIT-5-in-the-Core.aspx?utm_referrer=

3 http://www.isaca.org/About-ISACA/Press-room/News-Releases/2014/Pages/ISACA-Releases-European--Guidance-on-Cybersecurity.aspx?utm_referrer=

4 http://www.isaca.org/About-ISACA/Press-room/News-Releases/2018/Pages/ISACA-Refreshes-COBIT-Framework-to-Address-Latest-Business-Technology-Trends-and-Standards.aspx

- Radka Vankova, ISACA Czech Republic Chapter
- Sanja Kekic, ISACA Belgrade Chapter
- Stefano Scapecchi, ISACA Milan Chapter
- Vanesa Gil, ISACA Madrid Chapter

About ISACA

Now in its 50th anniversary year, ISACA (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Today's world is powered by information and technology, and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations. ISACA leverages the expertise of its 460,000 engaged professionals—including its 140,000 members—in information and cybersecurity, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI Institute, to help advance innovation through technology. ISACA has a presence in 188 countries, including more than 220 chapters worldwide and offices in both the United States and China.

ISACA have 36.038[5] members in Europe distributed by the following chapters:

• Israel • Milano, Italy • London, UK • Oslo, Norway • Paris, France • Stockholm, Sweden • Denmark • Netherlands • Germany • Northern England • Finland • Switzerland • Budapest, Hungary • Central UK • Athens, Greece	• Slovenia • Latvia • Belgium • Czech Republic • Irish • Austria • Slovensko • Estonia • Moscow, Russia • Croatia • Barcelona, Spain • Romania • Scottish • Rome, Italy • Lithuania	• Valencia, Spain • Madrid, Spain • Malta • Sofia, Bulgaria • Luxembourg • Istanbul, Turkey • Kyiv, Ukraine • Lisbon, Portugal • Cyprus • Winchester, UK • Venice, Italy • Ankara, Turkey • Warsaw, Poland • Katowice, Poland • Belgrade, Serbia

Disclaimer

The comments made in this document are of responsibility of the group of professionals referred above, not constituting at any moment an official position of ISACA.

I. ABOUT THE METHODOLOGY USED

The above-mentioned participants organized a workgroup to align their individual contributions and to share with EBA a common response that represents their vision about how ISACA related knowledge, tools (e.g. COBIT 2019 Framework) and professional certifications (e.g. CISA, CRISC, CISM, CGEIT, CSX-P) could support European Organizations to address EBA requirements.

[5] ISACA Membership Statistics: December 2018

II. OUR COMMENTS

Section	Topic	Sub topic	Ref	General Comment	ISACA Related Comment
2. Executive Summary					
3.Background and rationale					
Compliance and reporting obligations	Status of these guidelines		1;2		
	Reporting requirements		3;4		
Subject matter, scope and definitions	Subject matter		5;6		
	Scope of application		7;8		
	Addressees		9		
	Definitions		10		
Implementation	Data of application		11		
	Repeal		12		
Guidelines on ICT and security risk management	4.1. Proportionality		1	Term "proportionality" (explained in chapter 4.1. Proportionality) is better expressed as "a graded approach" according to the specific context, objectives, conditions and needs of financial institutions. We know from practice that the ability to apply a graded approach is crucial to the successful implementation of the Guidelines, and it is therefore appropriate to set minimum criteria (factors) to be taken into account. In order to verify compliance, design factors and their impact on implementation need to be properly documented. We propose to amend	*Related COBIT 2019 Governance and Management Objectives* ***COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*** *COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution is a breakthrough publication for the COBIT framework. Since there is no such thing as a one-size-fits-all governance system for enterprise I&T, every organization must uniquely tailor its governance system in order to maximize value out of its uses of I&T. The COBIT 2019 Design*

				the text of paragraph 4.1. to the new one: The management body should apply the graded approach to comply with the provisions set out in these Guidelines in such a way that is proportionate to, and takes into account of, at least the following factors: a) security significance of the financial institution and its parts, b) the financial institutions' size and complexity, c) internal organisation, d) the nature, scope, complexity and riskiness of the services and products that the financial institutions provide or intend to provide, e) the strategy and the goals. The factors used to grade the development and application of the Guidelines shall be documented.	*Guide provides a blueprint for enterprises through the use of "design factors." This publication:* ● *Explores the implications of various design factors and their impacts on the design of a governance solution* ● *Presents a four-step workflow for designing an enterprise governance solution, which takes into account all potential design factors.* ● *Helps enterprises create a customized governance system that fits their unique needs* ● *Provides guidance for also using the COBIT 2019 Implementation Guide in tandem with this Design Guide.* *The guide* *uses the following set of design factors:* *1. Enterprise strategy* *2. Enterprise goals* *3. Risk profile of the enterprise* *4. I&T-related issues* *5. Threat landscape under which the enterprise operates* *6. Compliance requirements* *7. Role of IT for the enterprise* *8. Sourcing model for IT* *9. IT implementation methods.*

	4.2. ICT governance and strategy	4.2.1. Governance	2;3;4	Point 4. After "management of ICT risks"We would add as the integral part of overall business risk management process. Replace management body with senior management body every time we are talking about Governance and mentioning the activity of Ensure. We should promote a view of corporate governance of ICT and by definition the governance Responsibility is from the Board with the management is from the management Body.	*Related ISACA Professional Certifications* ***Certified in the Governance of Enterprise IT (CGEIT)*** ***Certified Information Systems Auditor (CISA)*** ***Certified in Risk and Information Systems Control (CRISC)*** Related COBIT 2019 Governance and Management Objectives **EDM01—Ensured Governance Framework Setting and Maintenance**: *Analyze and articulate the requirements for the governance of enterprise I&T. Put in place and maintain governance components with clarity of authority and responsibilities to achieve the enterprise's mission, goals and objectives.* **APO01—Managed I&T Management Framework:** *Design the management system for enterprise I&T based on enterprise goals and other design factors. Based on this design, implement all required components of the management system* **MEA02 Managed System of Internal Control:** *Continuously monitor and evaluate the control environment, including self-assessments and self-awareness. Enable management to identify control deficiencies and inefficiencies and to initiate improvement actions. Plan, organize and maintain standards for internal control assessment and process control effectiveness*
		4.2.2. Strategy	5;6	5 Section a) we would add in first line "to effectively support and participate in". This reflects role of ICT as integral part of	*Related ISACA Professional Certifications* ***Certified in the Governance of Enterprise IT (CGEIT)*** Related COBIT 2019

				processes, not only as support function that is involved in late stages of already established processes and procedures. Section c) we would add at the end of sentence "in line with general security and governance policies established in organization". The ICT strategy should be fully integrated into, and aligned with, Should include also the alignment of ICT Strategy with Innovation to avoid disruption and to support LEAN digital transformation based on ICT Architecture Should include also the proper portfolio of changes to align ICT transformation according to business transformation	Governance and Management Objectives **APO02—Managed Strategy:** *Provide a holistic view of the current business and I&T environment, the future direction, and the initiatives required to migrate to the desired future environment. Ensure that the desired level of digitization is integral to the future direction and the I&T strategy. Assess the organization's current digital maturity and develop a roadmap to close the gaps. With the business, rethink internal operations as well as customer-facing activities. Ensure focus on the transformation journey across the organization. Leverage enterprise architecture building blocks, governance components and the organization's ecosystem, including externally provided services and related capabilities, to enable reliable but agile and efficient response to strategic objectives.* **APO04 - Managed Innovation:** *Maintain an awareness of I&T and related service trends and monitor emerging technology trends. Proactively identify innovation opportunities and plan how to benefit from innovation in relation to business needs and the defined I&T strategy. Analyze what opportunities for business innovation or improvement can be created by emerging technologies, services or I&T-enabled business innovation; through existing established technologies; and by business and IT process innovation. Influence strategic planning and enterprise architecture decisions.* **APO05 - Managed Portfolio:** *Execute the strategic direction set for investments in line with the enterprise architecture vision and I&T road map. Consider*

					the different categories of investments and the resources and funding constraints. Evaluate, prioritize and balance programs and services, managing demand within resource and funding constraints, based on their alignment with strategic objectives, enterprise worth and risk. Move selected programs into the active products or services portfolio for execution. Monitor the performance of the overall portfolio of products and services and programs, proposing adjustments as necessary in response to program, product or service performance or changing enterprise priorities.
		4.2.3. Use of third party providers	7;8;9	At 8 add: Financial institutions should ensure that contracts and service level agreements with the provider (outsourcing provider, group entity, or third party provider) include the following: a) appropriate and proportionate information security objectives, ICT risks and measures ... added words "ICT risks"; d) The right to audit the provider to validate compliance of the requirements established in the contract. 9 At the end we would add "on regular basis with remediation plans created and implemented based on findings obtained by	Financial institutions should identify the ICT risks, that impact the business functions, supporting processes, and information assets that are outsourced to third parties. The security objectives, ICT risks and measures should be documented in the contract to the third party and periodically reviewed. Without knowledge and understanding of the risks, including their context and impact, the measures are carried out only formally and can be missed. Related COBIT 2019 Governance and Management Objectives **APO10—Managed Vendors:** *Manage I&T-related products and services provided by all types of vendors to meet enterprise requirements. This includes the search for and selection of vendors, management of relationships, management of contracts, and reviewing and monitoring of vendor performance and vendor ecosystem (including upstream supply chain) for effectiveness and compliance.*

				monitoring and testing".	
	4.3. ICT risk management framework	4.3.1. Organisation and objectives	10;11;12; 13;14;15	Suggest the adoption of a well recognized security management framework. 13. I would switch points a) and b).We would first identify and assess and then determine risk tolerance 15a. The ICT risk management framework should be reviewed, at least once a year, by an external and independent or Is once a year enough for approval and review process? I suggest twice a year.	Related COBIT 2019 Governance and Management Objectives **APO01—Managed I&T Management Framework:** *Design the management system for enterprise I&T based on enterprise goals and other design factors. Based on this design, implement all required components of the management system.* **APO12 - Managed Risk:** *Continually identify, assess and reduce I&T-related risk within tolerance levels set by enterprise executive management.*
		4.3.2. Identification of functions, processes and assets	16;17	Should mention the holistic view of organization detailed on a appropriated enterprise architecture to control changes and impacts Should mention Data Governance to capture and control metadata information in corporate view that explain and describe organization data and related risk	Related COBIT 2019 Governance and Management Objectives **APO01—Managed I&T Management Framework:** *Design the management system for enterprise I&T based on enterprise goals and other design factors. Based on this design, implement all required components of the management system* **APO03 - Managed Enterprise Architeture:** *Establish a common architecture consisting of business process, information, data, application and technology architecture layers. Create key models and practices that describe the baseline and target architectures, in line with the enterprise and I&T strategy. Define requirements for taxonomy, standards, guidelines, procedures,*

					templates and tools, and provide a linkage for these components. Improve alignment, increase agility, improve quality of information and generate potential cost savings through initiatives such as re-use of building block components. **APO08—Managed Relationships:** *Manage relationships with business stakeholders in a formalized and transparent way that ensures mutual trust and a combined focus on achieving the strategic goals within the constraints of budgets and risk tolerance. Base relationships on open and transparent communication, a common language, and the willingness to take ownership and accountability for key decisions on both sides. Business and IT must work together to create successful enterprise outcomes in support of the enterprise objectives* **APO14 - Managed Data:** *Achieve and sustain effective management of the enterprise data assets across the data life cycle, from creation through delivery, maintenance and archiving.* **BAI09—Managed Assets:** *Manage I&T assets through their lifecycle to make sure that their use delivers value at optimal cost, they remain operational (fit for purpose), and they are accounted for and physically protected. Ensure that those assets that are critical to support service capability are reliable and available. Manage software licenses to ensure that the optimal number are acquired, retained and deployed in relation to required business usage, and the software installed is in compliance with license agreements.*
		4.3.3. Classification and risk	18;19;20; 21;22	22 We would add at the	*Related ISACA Professional Certifications*

		assessment		end "and establish actions and activities in relation with newly discovered risk vectors".	***Certified in Risk and Information Systems Control (CRISC)*** Related COBIT 2019 Governance and Management Objectives **APO01—Managed I&T Management Framework:** *Design the management system for enterprise I&T based on enterprise goals and other design factors. Based on this design, implement all required components of the management system.* **APO12 - Managed Risk:** *Continually identify, assess and reduce I&T-related risk within tolerance levels set by enterprise executive management.* **APO14 - Managed Data:** *Achieve and sustain effective management of the enterprise data assets across the data life cycle, from creation through delivery, maintenance and archiving.*
		4.3.4. Risk mitigation	23;24	Should mention the role of business process controls to risk mitigation	*Related ISACA Professional Certifications* ***Certified in Risk and Information Systems Control (CRISC)*** Related COBIT 2019 Governance and Management Objectives **APO12 - Managed Risk:** *Continually identify, assess and reduce I&T-related risk within tolerance levels set by enterprise executive management.* DSS06 - Managed Business Process Controls
		4.3.5. Reporting	25	25 We would add "documented" before "reported".	*Related ISACA Professional Certifications* ***Certified in Risk and Information Systems Control (CRISC)*** Related COBIT 2019 Governance and Management Objectives

					APO12 - Managed Risk: *Continually identify, assess and reduce I&T-related risk within tolerance levels set by enterprise executive management.*
		4.3.6.	26;27;28	26 We consider that the methodology should be periodically updated, to guarantee it covers requirements related to new trends and changes in the payment ecosystem (Cloud platforms, Big Data, new technologies, new actors in the payment ecosystem,…). Therefore, we propose to add the following sentence: "The methodology should be periodically updated, to guarantee it considers requirements related to new trends and changes in the payment ecosystem".	*Related ISACA Professional Certifications* ***Certified Information Systems Auditor (CISA)*** ***Certified in Risk and Information Systems Control (CRISC)*** Related COBIT 2019 Governance and Management Objectives **MEA04—Managed Assurance**: *Plan, scope and execute assurance initiatives to comply with internal requirements, laws, regulations and strategic objectives. Enable management to deliver adequate and sustainable assurance in the enterprise by performing independent assurance reviews and activities.*
	4.4. Information security	4.4.1. Information security policy	29;30;31	29 In our opinion Risk Assessment is based on Information Security Policy and not vice versa The Information Security Policy establishes the information security objectives and security framework of the financial institution. These objectives will determine the risk tolerance and how to manage the results of the Risk Assessment. Therefore, we consider that the wording in Point 29 should be changed. At the end we would add "It shall take into	*Related ISACA Professional Certifications* ***Certified Information Security Manager (CISM)*** ***CSX Cybersecurity Practitioner (CSX-P)*** Related COBIT 2019 Governance and Management Objectives **APO13—Managed Security:** *Define, operate and monitor an information security management system.* **DSS05 - Managed Security Services:** *Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy. Establish and maintain information security roles and access*

				account regulatory and legal requirements for financial institutions and other legal provisions that affect ICT in general". 31 Add an incident response/management process (see 4.5.1) 33 I would add f) "Be involved in all ICT initiatives and projects from their early stages". Should mention also software security controls and data masking in non-production environment	*privileges. Perform security monitoring.*
		4.4.2. Information security function	32:33		*Related ISACA Professional Certifications* ***Certified Information Security Manager (CISM)*** ***CSX Cybersecurity Practitioner (CSX-P)*** Related COBIT 2019 Governance and Management Objectives **APO01—Managed I&T Management Framework:** *Design the management system for enterprise I&T based on enterprise goals and other design factors. Based on this design, implement all required components of the management system*
		4.4.3. Logical security	34;35		*Related ISACA Professional Certifications* ***Certified Information Security Manager (CISM)*** ***CSX Cybersecurity Practitioner (CSX-P)*** Related COBIT 2019 Governance and Management Objectives **DSS05.04 Manage user**

					identity and logical access: *Ensure that all users have information access rights in accordance with business requirements. Coordinate with business units that manage their own access rights within business processes.*
		4.4.4. Physical security	36;37;38		*Related ISACA Professional Certifications* ***Certified Information Security Manager (CISM)*** ***CSX Cybersecurity Practitioner (CSX-P)*** Related COBIT 2019 Governance and Management Objectives **DSS05.05 Manage physical access to I&T assets**: *Define and implement procedures (including emergency procedures) to grant, limit and revoke access to premises, buildings and areas, according to business need. Access to premises, buildings and areas should be justified, authorized, logged and monitored. This requirement applies to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party*
		4.4.5. ICT operations security	39;40	39 We consider that secure configuration baselines should be established not only for critical network components, but also for system components (servers, databases,…) Therefore, we would add the following reference "Secure configuration baselines of critical network components…. **and system components, such as servers and databases".** The Guidelines refer to "encryption of data at	*Related ISACA Professional Certifications* ***Certified Information Security Manager (CISM)*** Related COBIT 2019 Governance and Management Objectives **DSS01—Managed Operations:** *Coordinate and execute the activities and operational procedures required to deliver internal and outsourced I&T services. Include the execution of predefined standard operating procedures and the required monitoring activities.* **DSS02 - Managed Service**

				rest and in transit". We agree that sensitive data must be encrypted (as defined by the legal requirements applicable and the data classification criteria of the financial institution). However, we consider that not all the data needs to be encrypted. Therefore, we propose the following alternative wording: **"Encryption of sensitive data at rest and in transit".**	**Request and Incidents:** *Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents.* **DSS05 - Managed Security Services:** *Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy. Establish and maintain information security roles and access privileges. Perform security monitoring.*
		4.4.6. Security monitoring	41;42;43		*Related ISACA Professional Certifications* ***Certified Information Security Manager (CISM)*** ***CSX Cybersecurity Practitioner (CSX-P)*** Related COBIT 2019 Governance and Management Objectives **APO13—Managed Security:** *Define, operate and monitor an information security management system.*
		4.4.7. Information security reviews, assessment and testing	44;54;46; 47;48;49; 50;51	49 We consider that Point 49 should be included before Point 47, as Point 49 establishes that *"financial institutions should perform on-going and repeated tests of the security measures"*, while Point 47 refers to "*tests of security measures conducted in the event of changes to infrastructure, processes or procedures".* We consider that tests conducted on an ongoing basis should be mentioned before tests conducted in the event of changes to infrastructure, processes	*Related ISACA Professional Certifications* ***Certified Information Security Manager (CISM)*** Related COBIT 2019 Governance and Management Objectives **APO13—Managed Security:** *Define, operate and monitor an information security management system.* **DSS05 - Managed Security Services:** *Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy. Establish and*

				or procedures.	*maintain information security roles and access privileges. Perform security monitoring.*
		4.4.8. Information security training and awareness	52;53;54		*Related ISACA Professional Certifications* ***Certified Information Security Manager (CISM)*** ***CSX Cybersecurity Practitioner (CSX-P)*** Related COBIT 2019 Governance and Management Objectives **APO13—Managed Security:** *Define, operate and monitor an information security management system.* **DSS05 - Managed Security Services:** *Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy. Establish and maintain information security roles and access privileges. Perform security monitoring.*
	4.5. ICT Operations management		55;56;57; 58;59;60; 61;62;63	58 Identify assets that **are critical** in providing service capability. 59 Identify **legal, regulatory or contractual requirements** that need to be addressed when managing the asset.	55,56,57 Related COBIT 2019 Governance and Management Objectives **DSS01—Managed Operations:** *Coordinate and execute the activities and operational procedures required to deliver internal and outsourced I&T services. Include the execution of predefined standard operating procedures and the required monitoring activities.* 58, 59 Related COBIT 2019 Governance and Management Objectives **BAI09—Managed Assets:** *Manage I&T assets through their lifecycle to make sure that their use delivers value at optimal cost, they remain operational (fit for purpose),*

					and they are accounted for and physically protected. Ensure that those assets that are critical to support service capability are reliable and available. Manage software licenses to ensure that the optimal number are acquired, retained and deployed in relation to required business usage, and the software installed is in compliance with license agreements. **BAI10—Managed Configuration:** *Define and maintain descriptions and relationships among key resources and capabilities required to deliver I&T-enabled services. Include collecting configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository* 60 Related COBIT 2019 Governance and Management Objectives **BAI06—Managed IT Changes:** *Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritization and authorization, emergency changes, tracking, reporting, closure, and documentation* **BAI07—Managed IT Change Acceptance and Transitioning:** *Formally accept and make operational new solutions. Include implementation planning, system and data conversion, acceptance testing, communication, release preparation, promotion to production of new or changed business processes and I&T services, early production support, and a post-implementation review.*

					61 Related COBIT 2019 Governance and Management Objectives BAI04—Managed Availability and Capacity: *Balance current and future needs for availability, performance and capacity with cost-effective service provision. Include assessment of current capabilities, forecasting of future needs based on business requirements, analysis of business impacts, and assessment of risk to plan and implement actions to meet the identified requirements.* 62, 63 Related COBIT 2019 Governance and Management Objectives **APO14 - Managed Data:** *Achieve and sustain effective management of the enterprise data assets across the data life cycle, from creation through delivery, maintenance and archiving.*
		4.5.1 ICT Incident and problem management	64;65	64 This description is primarily focused on the aim of **incident** management. Since the chapter 4.5.1 is meant for Incident **and problem management** We would expect to have also an comment such as: *The primary objectives of problem management are **to prevent** Incidents … (proactive problem management).* 64 Expects of financial institutions to have criterias in place for (i) operation or (ii) security incidents as	*Related ISACA Professional Certifications* ***Certified Information Security Manager (CISM)*** Related COBIT 2019 Governance and Management Objectives **DSS02 - Managed Service Request and Incidents:** *Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents.* **DSS03—Managed Problems:** *Identify and classify problems and their root causes. Provide timely resolution to prevent recurring incidents. Provide recommendations for improvements.*

				well as (iii) early warning indicators. 65 Then elaborates further on needed measures for the (i) operational and (ii) security incidents but does not say anything regarding **the (iii) early warning indicators** anymore.	
	4.6. ICT Project and Change management	4.6.1. ICT project management	66;67;&8;69;70;71;72	67 Financial institutions should also monitor and mitigate risks regarding **involvement of external solution provider** during the project (e.g. transfer of confidential data during development or development environments in the cloud). 68 68. Financial institutions should establish and implement an ICT project management policy which defines the phases of each project and includes at a minimum: a) project objectives; **+) project result; (add text)** b) roles and responsibilities; c) project risk assessment; d) project plan, timeframe and steps; e) procurement management; f) key milestones; g) and change management requirements.	The most important part of the project is its focus on the result, not on the way of management. Related COBIT 2019 Governance and Management Objectives **Map BAI11—Managed Projects:** *Manage all projects that are initiated within the enterprise in alignment with enterprise strategy and in a coordinated way based on the standard project management approach. Initiate, plan, control and execute projects, and close with a post-implementation review*

		4.6.2. ICT systems acquisition and development	73;74;75; 76;77;78; 79;80	**77** Use the term 'penetration testing' in this section, e.g. "When applicable, **penetration testing** should be performed to identify system vulnerabilities…. " (analog to number 76 with 'regression testing'). Should mention technical testing and functional testing, instead of testing	Related COBIT 2019 Governance and Management Objectives **BAI03—Managed Solutions Identification and Build:** *Establish and maintain identified products and services (technology, business processes and workflows) in line with enterprise requirements covering design, development, procurement/sourcing and partnering with vendors. Manage configuration, test preparation, testing, requirements management and maintenance of business processes, applications, information/data, infrastructure and services.* **BAI02 - Managed Requirement Definition:** *Identify solutions and analyze requirements before acquisition or creation to ensure that they align with enterprise strategic requirements covering business processes, applications, information/data, infrastructure and services. Coordinate the review of feasible options with affected stakeholders, including relative costs and benefits, risk analysis, and approval of requirements and proposed solutions.* **BAI04—Managed Availability and Capacity**: *Balance current and future needs for availability, performance and capacity with cost-effective service provision. Include assessment of current capabilities, forecasting of future needs based on business requirements, analysis of business impacts, and assessment of risk to plan and implement actions to meet the identified requirements.*
		4.6.3. ICT change management	81;82	**81 and 82**	Related COBIT 2019 Governance and

				A comment is missing regarding the 'post implementation review', which should give assurance, that the change implementation has been done successfully without unexpected impacts. Based on a risk assessment, a 'post implementation review' may be required for new implementations as well as changes of a former implementation. Should mention proper change documentation, control and approval	Management Objectives **BAI05—Managed Organizational Change:** *Maximize the likelihood of successfully implementing sustainable enterprise wide organizational change quickly and with reduced risk. Cover the complete life cycle of the change and all affected stakeholders in the business and IT.* **BAI06 - IT Changes:** *Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritization and authorization, emergency changes, tracking, reporting, closure, and documentation.* **BAI07 - Managed IT Changes, Acceptance and Transitioning:** *Formally accept and make operational new solutions. Include implementation planning, system and data conversion, acceptance testing, communication, release preparation, promotion to production of new or changed business processes and I&T services, early production support, and a post-implementation review* **BAI10 - Managed Configuration:** *Define and maintain descriptions and relationships among key resources and capabilities required to deliver I&T-enabled services. Include collecting configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository.*
	4.7. Business continuity management		83		Related COBIT 2019 Governance and Management Objectives **DSS04—Managed Continuity:** *Establish and*

					maintain a plan to enable the business and IT organizations to respond to incidents and quickly adapt to disruptions. This will enable continued operations of critical business processes and required I&T services and maintain availability of resources, assets and information at a level acceptable to the enterprise.
		4.7.1. Business impact analysis	84;85		*Related ISACA Professional Certifications* ***Certified Information Security Manager (CISM)*** Related COBIT 2019 Governance and Management Objectives **DSS04.02 Maintain business resilience:** *Evaluate business resilience options and choose a cost-effective and viable strategy that will ensure enterprise continuity, disaster recovery and incident response in the face of a disaster or other major incident or disruption.*
		4.7.2. Business continuity planning	86;87;88	This part must reflect more BCP process and its connection with third party vendors – BCPs must cover this area – continuity related to services provided by external parties.	*Related ISACA Professional Certifications* ***Certified Information Security Manager (CISM)*** Related COBIT 2019 Governance and Management Objectives **DSS04.03 Develop and implement a business continuity response:** *Develop a business continuity plan (BCP) and disaster recovery plan (DRP) based on the strategy. Document all procedures necessary for the enterprise to continue critical activities in the event of an incident.*
		4.7.3. Response and recovery plans	89;90;91; 92		*Related ISACA Professional Certifications* ***Certified Information Security Manager (CISM)*** ***CSX Cybersecurity***

					Practitioner (CSX-P) Related COBIT 2019 Governance and Management Objectives **DSS04.03 Develop and implement a business continuity response:** *Develop a business continuity plan (BCP) and disaster recovery plan (DRP) based on the strategy. Document all procedures necessary for the enterprise to continue critical activities in the event of an incident.*
		4.7.4. Testing of plans	93;94;95;96		*Related ISACA Professional Certifications* ***Certified Information Security Manager (CISM)*** ***Certified Information Systems Auditor (CISA)*** Related COBIT 2019 Governance and Management Objectives **DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP):** *Test continuity on a regular basis to exercise plans against predetermined outcomes, uphold business resilience and allow innovative solutions to be developed.*
		4.7.5. Crisis communications	97		Related COBIT 2019 Governance and Management Objectives **DSS04.03 Develop and implement a business continuity response:** *Develop a business continuity plan (BCP) and disaster recovery plan (DRP) based on the strategy. Document all procedures necessary for the enterprise to continue critical activities in the event of an incident.*
	4.8. Payment service user relationship management		98;99;100;101;102;103;104		

5. Accompanying documents	5.1. Draft cost-benefit analysis / impact assessment				

III. NEXT STEPS

Taking into account the alignment of EBA's requirements with ISACA good practices, in particular the ISACA 2019 framework, we hope in the future to continue to support ISACA professionals and their organizations through the development of good practices and specific guidelines that can contribute to synergies an efficient and effective alignment between the management and internal control environments and COBIT framework with legal and regulatory requirements.

IV. CONTACT US

If you have any questions regarding this contribution, please contact us by sending an email to bruno.soares@govaas.com.