Topic 4
Topic 2
Topic 3
Topic 1
Topic 5

Topic1
p8

Topic2
p37-38, p41, p48-49, p63, p70-71, p84-85

Topic3
p35-36, p38-40, p66-67, p76-77, p87

Topic5
p25, p84

MALTA
FINANCIAL
SERVICES
AUTHORITY

GUIDANCE ON TECHNOLOGY ARRANGEMENTS, ICT AND SECURITY RISK MANAGEMENT, AND OUTSOURCING ARRANGEMENTS

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

FOREWORD

Technology is at the core of the financial services industry, acting as an enabler for innovation, shorter time-to-market, improved customer experience, operational efficiencies and regulatory compliance.

Business models, as well as the products and services offered by the financial services sector, are shaped by several factors including greater significance of data, analytics, risk management, compliance, security, digitisation, enterprise mobility, payments and enhanced customer experience. This digital transformation is contributing towards more innovative products and services to the benefit of consumers and the market at large.

Compute, storage and network virtualisation technology, and the proliferation of Cloud Services have rapidly transformed the manner by which infrastructure, software platforms, information systems and services, and indeed entire business and/or operational functions, are implemented for consumption along process chains in the financial services sector.

Application Programming Interfaces (APIs), particularly those exposed through Web Services, provide the programmatic interconnectedness between systems from service providers and their internal or external downstream customers, regardless of geography, for the consumption of services through data interchange over private networks or the Internet. Therefore, APIs play a crucial role across the financial services sector's technology landscape.

Business process automation, whether through traditional rule-based logic or supplemented with state-of-the-art techniques, such as Machine Learning, is reducing the need for manual intervention and expediting decision-making in process chains.

The net result of this rapidly evolving technology landscape is the increasing reliance on ICT-enabled critical or important business and/or operational functions that are provided through, or dependent upon, infrastructure, software and services implemented and managed remotely by third parties. In many instances Technology Arrangements involve a mix of on-premises and remote technologies and data sources, in a geographically dispersed data processing and storage architecture that is seamless to other parts of the business or to downstream customers.

Cloud services bring a multitude of benefits to firms, including agility, flexibility and cost savings. The adoption of Cloud, and other technologies in general, for driving product innovation and for increasing operational performance, is therefore encouraged. However, while on the one hand technological sophistication delivers clear benefits to authorised financial services firms and their customers, it also changes the nature of operational risks that need to be managed and mitigated.

The increasing breadth of scope of outsourced services and functions, as well as the very low technical barriers for the provision of such services through technology from practically any geographical region implies that certain outsourced services and functions, or elements thereof, may be unregulated and/or may introduce compliance risks. Outsourcing of important or critical services and functions, especially when the service provider is located outside the EU/EEA, must not impair the Licence Holder's, and any competent authority's, oversight capabilities with respect to regulatory compliance, or alter the conditions subject to which authorisation was granted. Financial stability and consumer protection need to be safeguarded.

Hybrid or entirely Cloud-based enterprise architectures and services can significantly alter the risk profile of licensed entities. Risks emanating from increased reliance on such Technology Arrangements need to be effectively managed and mitigated. Effective and clear ICT governance frameworks must be in place. Moreover, it calls for the Management Body of a Licence Holder, as well as any entity seeking authorisation, to ensure that there is clear awareness and understanding of the extent of reliance on outsourcing service providers. Business continuity and contingency planning also need to encompass all aspects of outsourcing arrangements.

The MFSA recognises the increasing reliance by authorised firms on Technology Arrangements that drive critical or important functions, and that may involve multiple remote third-party service providers which are contracted directly and/or sub-contracted. It also recognises the blurring of traditional enterprise perimeters - not just physically but also logically. This is not only brought about by Cloud-based workloads and geographically dispersed data storage or services but is also due to the need for firms to accommodate multifaceted operating requirements for accessing computing and data assets. The latter includes wireless and off-site employees, including those of outsourcing providers and business partners, access to services and resources from mobile phones, and multiple upstream and downstream integration points. This presents a challenging elastic attack surface in terms of cybersecurity exposure, which therefore requires utmost attention at strategic and operational planning levels, combined with an effective governance framework, as part of the authorised firms' holistic risk management framework.

Many challenges and risk mitigation factors are common across the whole financial services industry. ICT and Security Risk Management, including cybersecurity, and Outsourcing Arrangements are already subject to provisions in relevant sectoral legislation, rulebooks, and guidance to varying degrees. The principle of proportionality applies across the different sectors. Clarity and detail with respect to specific requirements and/or guidance provided, however, these vary across the different sectors, but convergence and harmonisation across sectors, particularly with respect to guidance related to outsourcing of cloud services at European level is ongoing.

It is therefore the MFSA's view that there is a clear opportunity to harmonise the approach on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements, by providing a single guidance document for all sectors authorised by the MFSA, without prejudice to all applicable Acts, Regulations, rules or sector specific guidelines.

The purpose of this Guidance document is therefore to provide general guidance to authorised firms with respect to the implementation of Technology Arrangements, ICT and Security Risk Management, and relevant Outsourcing Arrangements. It lays out the supervisor's expectations for ongoing compliance by authorised firms in the aforementioned areas, and for the Authority to ensure that it can continue to exercise its oversight across the relevant sectors.

This Guidance document should be considered as a live document due to the dynamic nature of regulatory developments, technology evolution, and related opportunities and risks. It will be updated from time to time to reflect any relevant developments.

In the event of any inconsistency or conflict between this Guidance document and any applicable Acts, Regulations, rules or sector-specific guidelines, the provisions of the said Acts, Regulations, rules or sector-specific guidelines shall always prevail.

CONTENTS

REVISIONS LOG

VERSION	DATE ISSUED	DETAILS
1.00	30 JUNE 2020	GUIDANCE ISSUED FOR CONSULTATION
1.01	11 DECEMBER 2020	GUIDANCE ISSUED

Title 1 Scope and Application

Section 1 Scope and Application

1.1.1 Licence Holders are expected to establish and maintain an operational governance framework according to applicable Acts, Regulations, rules and sector-specific guidelines. ICT governance and risk-mitigation are an intrinsic part of such governance frameworks.

1.1.2 This Guidance document addresses internal governance arrangements on ICT and Security Risk Management, including cybersecurity and outsourcing, that Licence Holders or prospective applicants should implement for Technology Arrangements. Given the need, on the other hand, to provide clarity and more specific guidance to Licence Holders and prospective applicants regarding Technology Arrangements, particularly those involving relevant outsourcing arrangements, and furthermore, the need for unhindered supervisory oversight in the context of ever growing reliance on cloud services and geographically dispersed hosting arrangements, the Authority is providing harmonised baseline guidance on Technology Arrangements to authorised entities listed in 1.1.9, without prejudice to sector-specific legislation, including delegated measures, sector-specific guidance, and all other EU and national legislation.

1.1.3 Guidance on ICT and Security Risk Management, particularly information security, is largely based on the requirements emanating from the EBA Guidelines on ICT and Security Risk Management (EBA/GL/2019/04), relevant European Supervisory Authority (ESA) Guidelines that may be issued from time to time[1], generally accepted standards and cybersecurity frameworks, and takes into consideration existing Maltese and EU regulatory frameworks.

1.1.4 Technology Arrangements frequently involve outsourcing of services or functions to third parties, while critical or important functions are increasingly becoming dependent on such Technology Arrangements.

1.1.5 EBA Guidelines EBA/GL/2019/02, effective as of 30th September 2019, repeal the Committee of European Banking Supervisors (CEBS) guidelines on outsourcing of 14th December 2006 and the EBA recommendations EBA/REC/2017/03 on outsourcing to cloud service providers. These new guidelines take into consideration Directive 2013/36/EU (Capital Requirements Directive; CRD), Directive 2014/65/EU (Markets in Financial Instruments Directive; MiFID II) and Directive 2015/2366/EU (Revised Payment Services Directive; PSD2) which have specific outsourcing provisions and governance

[1] For example, the EIOPA Guidelines on Information and Communication Technology (ICT) security and governance

arrangements. The EBA's recommendations apply to credit institutions and investment firms as defined under article 4(1) of the Regulation (EU) No 575/2013 (Capital Requirements Regulation – CRR). The EBA Guidelines on ICT and Security Risk Management (EBA/GL/2019/04) repeal EBA Guidelines EBA/GL/2017/17 'Guidelines on the security measures for operational and security risks of payment services'.

1.1.6 ESMA issued[2] draft guidelines on outsourcing to cloud service providers to help clarify supervisory expectations in outsourcing arrangements.

1.1.7 EIOPA provides general guidelines on outsourcing within the Solvency II framework as part of the EIOPA Guidelines on System of Governance (EIOPA-BoS-14/253). While the Solvency II framework (Directive, Delegate Regulations and Guidelines) covers most of the content of the EBA recommendations EBA/GL/2019/02, EIOPA has stated that the EBA guidelines are more specific about the execution of the materiality assessment of outsourced services, the registration of outsourcing arrangements and the duty to inform supervisory authorities, access and audit rights for the undertaking, and dealing with specific cloud outsourcing risks[3]. Recognising the potential risks of regulatory fragmentation, EIOPA has therefore developed guidelines[4] on how outsourcing provisions set forth in Solvency II and Commission Delegated Regulation (EU) No 2015/35 need to be applied in case of outsourcing to cloud service providers while also largely aligning with EBA recommendations EBA/GL/2019/02. EIOPA's research suggests that the usage by (re)insurance undertakings of cloud computing services (which fall under existing regulatory measures on outsourcing and current guidance), and the risks arising from such usage, is aligned to that of the banking sector, with few minor (re)insurance specificities[5]. On 12/10/2020 EIOPA finalised and published their Guidelines on information and communication technology (ICT) security and governance.[6]

1.1.8 It is the authorised entities' responsibility to ensure compliance with all relevant Acts, Regulations, rules or sector-specific guidelines.

1.1.9 This Guidance document is addressed to the following entities licensed by the Authority:

- Credit Institutions
- Financial Institutions
- Insurance Undertakings and Reinsurance Undertakings

[2] https://www.esma.europa.eu/press-news/consultations/draft-guidelines-outsourcing-cloud-service-providers

[3] https://eiopa.europa.eu/Publications/EIOPA%20Outsourcing%20to%20the%20cloud_Contribution%20to%20Fintech%20action%20plan%20%283%29.pdf

[4] https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/final_report_on_public_consultation_19-270-on-guidelines_on_outsourcing_to_cloud_service_providers.pdf

[5] https://eiopa.europa.eu/Pages/News/EIOPA-calls-for-principle-based-regulation-of-could-computing-.aspx

[6] https://www.eiopa.europa.eu/content/eiopa-finalises-guidelines-information-and-communication-technology-security-and-governance_en

- Insurance and Reinsurance Undertakings which are part of a group in line with Article 212 of Directive 2009/138/EC
- Captive Insurance Undertakings and Captive Reinsurance Undertakings
- Insurance Intermediaries
- Ancillary Insurance Intermediaries
- Retirement Pension Schemes (Occupational Retirement Schemes and Personal Retirement Schemes)
- Pension Service Providers (Retirement Scheme Administrator, Investment Manager and Custodian)
- Investment Services Licence Holders
    - Investment Firms Categories 1 to 3
    - Custodians of Collective Investment Schemes – Categories 4a and 4b
    - Fund Managers: De minimis AIFMs, full scope AIFMs and UCITS Management Companies
    - Self-managed Collective Investment Schemes (including Professional Investment Funds, UCITS and Alternative Investor Funds)
    - Recognised Fund Administrators
- Trading Venues
- Central Securities Depositories
- Trustees and other Fiduciaries
- Company Service Providers
- Virtual Financial Assets

This Guidance document is cross-referenced by the respective prudential rules of these listed sectors.

These guidelines are not intended to cover Technology Arrangements, or parts thereof, which are authorised and supervised by the Malta Digital Innovation Authority.

1.1.10 In the event of any inconsistency or conflict between this Guidance document and any applicable Acts, Regulations, rules, or sector-specific guidelines, the provisions of the said Acts, Regulations, rules or sector-specific guidelines shall always prevail.

Section 2 Definitions

1.2.1 'Agile Project Management (APM)' is an iterative approach to project execution by way of breaking down a project into small deliverables that typically take two to four weeks, and where quality assurance is inbuilt in each iteration;

'Algorithmic Bias' describes systematic and repeatable errors in a computer system that create unfair outcomes, such as privileging one arbitrary group of users over others[7];

'Asset owner', person or entity with the accountability and authority for an information and ICT asset;

'Artificial Intelligence (AI)' refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals[8];

'Authority' refers to the Malta Financial Service Authority, the single regulator of financial services in Malta;

'Black Box Testing', also known as closed-box testing, is a software testing technique that focuses on the analysis of software functionality, by providing inputs and validating expected outputs or outcomes. Black box testing does not involve, or rely upon, access to source code;

'Business Process as a Service (BPaaS)' includes application functionality coupled with physical and human resources required to perform a broader set of business activities – typically a major module of activity in a broader business process (e.g., a call centre module, as part of the customer service process), or in some cases the complete business process itself (e.g., fully cloud-based supply chain management);

'Cloud Broker' means an entity that manages the use, performance and delivery of cloud services, and negotiates relationships between cloud providers and cloud customers. A cloud customer may request cloud services from a cloud broker, instead of contacting a cloud service provider directly;

'Cloud Computing', as defined by the National Institute of Standards and Technology (NIST)[9] at the U.S. Department of Commerce, is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or Cloud Service Provider (CSP) interaction;

'Cloud Forensics' is the application of digital forensics science in cloud computing environments. Technically, it consists of a hybrid forensic approach towards the generation of digital evidence. Organisationally, it involves interactions among cloud actors (i.e., cloud provider, cloud consumer, cloud broker, cloud carrier, cloud auditor) for the purpose

[7] https://en.wikipedia.org/wiki/Algorithmic_bias
[8] https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF
[9] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

of facilitating both internal and external investigations. Legally it often implies multi-jurisdictional and multi-tenant situations[10];

'Cloud Service' means services provided using cloud computing;

'Cloud Service Provider (CSP)' is a service provider responsible for delivering cloud services under an outsourcing arrangement. Arrangements with third parties which are not cloud service providers but rely significantly on cloud infrastructure to deliver their services e.g. where the cloud service provider is part of a sub-outsourcing chain, fall within the scope of this Guidance document. The same principle applies to cloud brokers;

'Community Cloud' is cloud infrastructure that is available for the exclusive use of a specific community of entities, institutions or entities/institutions with a single group;

'Containers' / 'Application Containers' are a form of operating system virtualisation combined with application software packaging including all library dependencies, binaries and configuration files, which together provide an entire runtime environment that is portable, reusable, and automatable in terms of deployment. Containers can live on-premises or in the cloud;

'Containerisation' is a virtualisation strategy that makes use of containers;

'Continuous Integration (CI)' is a software development practice in which each member of a development team integrates her work with that produced by others on a continuous basis[11]. CI systems provide automation of the software build and validation process driven in a continuous way by running a configured sequence of operations every time a software change is checked into the source code management repository[12]. CI is closely associated with agile development practices;

'Continuous Delivery (CD') is a set of processes, tools and techniques for the rapid, reliable and continuous development and delivery of software[13]. A CD process deploys all code changes to a testing and/or a production environment after the build stage, readily prepared for a release to production upon manual approval;

'Continuous Deployment' takes Continuous Delivery one step further by fully automating code deployment into a production environment with no human intervention for approval;

[10] K. Ruan, J. Carthy, T. Kechadi, and I. Baggili, "Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results," *Digital Investigation*, vol. 10, no. 1, pp. 34-43, 2013. https://www.researchgate.net/publication/271603639_Cloud_forensics_definitions_and_critical_criteria_for_cloud_forensic_capability_An_overview_of_survey_results

[11] https://www.techopedia.com/definition/24368/continuous-integration-ci

[12] https://www.gartner.com/en/information-technology/glossary/continuous-integration-ci

[13] https://www.techopedia.com/definition/28958/continuous-delivery-cd

‘Critical or Important function’ (material activity) means any function that is considered critical or important as set out in 5.3.5 and 5.3.6 of this Guidance document;

‘Cyber’, relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems;

‘Cyber-attack’, any type of hacking leading to an offensive / malicious attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorised use of an information asset that targets ICT systems;

‘Cyber Threat’, a circumstance with the potential to exploit one or more vulnerabilities that adversely affects cybersecurity;

‘Cybersecurity’, preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved;

‘Data Governance’ refers to the strategy, policies, processes and controls for the effective use of an organisation’s data assets;

‘Data Loss Prevention (DLP)’ is a suite of technologies aimed at stemming the loss of sensitive information from within an organisation, by focusing on the location, classification and monitoring of information at rest, in use and in motion[14]. Data Loss Prevention may also be referred to as Data Leak or Leakage Prevention;

‘Defence-In-Depth (DiD)’ is an information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organisation[15], such that if an attack causes one security mechanism to fail, other mechanisms may still provide the necessary security to protect an information system against other attack vectors;

‘Electronic Discovery’ (also called e-discovery or ediscovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case[16];

‘Explainability’ refers to the capability of Artificial Intelligence (AI) to describe its purpose, rationale and decision-making process in a way that can be understood by the average person;

[14] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Data-Leak-Prevention.aspx
[15] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[16] https://searchsecurity.techtarget.com/definition/electronic-discovery-e-discovery-or-ediscovery

'Explainable AI (XAI)' means Artificial Intelligence that is programmed to describe its purpose, rationale and decision-making process in a way that can be understood by the average person[17];

'Exploit' is the specially crafted code adversaries use to take advantage of a certain vulnerability and compromise a resource[18];

'Greenfield deployment' refers to the installation of an IT system where previously there was none[19];

'Hybrid Cloud' refers to cloud infrastructure that is composed of two or more distinct cloud infrastructures, and which usually refers to a cloud infrastructure composed of on-premises and off-premises (remotely hosted) infrastructures;

'ICT and security risk', risk of loss due to breach of confidentiality, failure of integrity of systems and data, inappropriateness or unavailability of systems and data or inability to change information technology (IT) within a reasonable time and with reasonable costs when the environment or business requirements change (i.e. agility). This includes security risks resulting from inadequate or failed internal processes or external events including cyber-attacks or inadequate physical security;

'ICT Asset', an asset of either software or hardware that is found in the business environment;

'ICT Project', any project, or part thereof, where ICT systems and services are changed, replaced, dismissed or implemented;

'ICT-related incident' means an unforeseen identified occurrence in the network and information systems, whether resulting from malicious activity or not, which compromises the security of network and information systems, of the information that such systems process, store or transmit, or has adverse effects on the availability, confidentiality, continuity or authenticity of financial services provided by the financial entity;

'ICT services', preservation of confidentiality, integrity and availability of information and/or information systems. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved;

'ICT systems', set of applications, services, information technology assets, ICT assets or other information-handling components, which includes the operating environment;

[17] https://whatis.techtarget.com/definition/explainable-AI-XAI
[18] https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/vulnerabilities-and-exploits
[19] https://www.techopedia.com/definition/5063/greenfield-deployment

'Information Assurance', in the field of communication and information systems is the confidence that such systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. Effective IA shall ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authenticity[20]. This five-pillar model was introduced by the U.S. Department of Defence (DoD) in 2002[21], which has now transitioned the term Information Assurance (IA) to cybersecurity[22];

'Information Asset', a collection of information, either tangible or intangible, that is worth protecting;

'Infrastructure as a Service (IaaS)' provides raw utilities such as computer power and electronic storage resources, as services over the network;

'Information Security', preservation of confidentiality, integrity and availability of information and/or information systems. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved. It deals with data protection in any form, and is therefore not limited to protection of data in the cyber domain;

'Licence Holder' means an entity or person authorised/licensed/registered by the MFSA to provide specific regulated financial services;

'Machine Learning' is the term coined by Arthur Samuel in 1959 for the field of study that gives computers the ability to learn without being explicitly programmed. Algorithms use large and dynamic data sets such that this form of AI learns and evolves with experience from the data that is analysed;

'Major ICT-related incident' means an ICT-related incident with a potentially high adverse impact on the network and information systems that support critical functions of the financial entity;

'Management Body' means a Licence Holder's body or bodies, which are appointed in accordance with national law, which are empowered to set the authorised firm's strategy, objectives and overall direction, and which oversee and monitor management decision-making. The Management Body includes the board of directors and any other persons who effectively direct the business of the authorised firm;

[20] Council Decision 2013/488/EU Article 10
[21] Dardick G. Australian Digital Forensics Conference: Cyber forensics assurance School of Computer and Information Science. [Internet] Perth, Western Australia: Edith Cowan University; 2010. [cited 2015 May 22]; Available from: https://ro.ecu.edu.au/adf/77/
[22] https://csrc.nist.gov/glossary/term/IA

'Non-functional Requirements' define behaviours, attributes and constraints related to factors such as availability, maintainability, performance, reliability, scalability and usability of software;

'Open Source' describes software that comes with permission to use, copy and distribute, either as is or with modifications, and that may be offered either free or with a charge. The source code must be made available[23];

'Operational Incident' an incident stemming from inadequate or failed processes, people and systems or events of force majeure that affect the integrity, availability, confidentiality, authenticity of ICT systems and services [24] ;

'Operational or Security Incident' is a singular unplanned event or a series of linked unplanned events which has or will probably have an adverse impact on the integrity, availability, confidentiality, authenticity of ICT systems and services[25];

'Outsourcing' means an arrangement of any form between a Licence Holder and a service provider by which that service provider performs a process, a service or an activity that would otherwise be undertaken by the Licence Holder;

'Outsourcing Process' means all the activities performed by the Licence Holder to plan, contract, implement, monitor, manage and terminate outsourcing arrangements;

'Platform as a Service (PaaS)' is a cloud services that includes tools and environments to build and operate cloud applications and services;

'Private Cloud' is a cloud infrastructure that is available exclusively to a single entity;

'Public Cloud' is a cloud infrastructure that is available for open use of the general public;

'Red Team', a group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment[26];

[23] https://www.gartner.com/en/information-technology/glossary/open-source
[24] Adapted from EBA/GL/2017/10 Guidelines on major incident reporting under Directive (EU) 2015/2366 (PD2)
[25] Definition from EBA/GL/2019/04 Guidelines on ICT and security risk management
[26] https://csrc.nist.gov/glossary/term/Red_Team

'Risk Appetite' is the aggregate level and types of risk that the PSPs and institutions are willing to assume within their risk capacity, in line with their business model, to achieve their strategic objectives;

'Security Incident' is a violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices leading to unauthorised access, use, disclosure, disruption, modification or destruction of the Licence Holder's assets that affect the integrity, availability, confidentiality, authenticity and/or continuity of ICT systems or services[27];

'Security Information and Event Management (SIEM) tool' is an application that provides the ability to gather security data from information systems components and present that data as actionable information via a single interface[28];

'Senior Management' refers to those natural persons who exercise executive functions within an organisation and who are responsible, and accountable to the Management Body, for the day-to-day management of the organisation. They are the most senior staff of an entity and led by the Chief Executive Officer;

'Service Provider' is a third-party that performs an outsourced process, service or activity, or parts thereof, under an outsourcing arrangement;

'Software as a Service (SaaS)' enables on-demand use of software over the Internet and private networks;

'Software entropy' is the tendency of software to become more complex and expensive to maintain, the more it changes. Software entropy increases with the accumulation of technical debt;

'Static Application Security Testing (SAST) tool' is a set of technologies designed to analyse application source code, byte code and binaries for coding and design conditions that are indicative of security vulnerabilities. SAST solutions analyse an application from the "inside out" in a nonrunning state[29];

'Sub-outsourcing' means a situation where the service provider under an outsourcing arrangement further transfers an outsourced function to another service provider. Sub-outsourcing may also be referred to as 'chain-outsourcing' or 'chain of outsourcing';

'Technical debt' is a concept in programming that reflects the extra development work that arises when code that is easy to implement in the short run is used instead of applying the best overall solution[30];

[27] Adapted from NIST SP 800-61r2 Computer Security Incident Handling Guide and EBA Consultation Paper on Guidelines on ICT and security risk management.

[28] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf

[29] https://www.gartner.com/en/information-technology/glossary/static-application-security-testing-sast

[30] https://www.techopedia.com/definition/27913/technical-debt

'Technology Arrangement' means the combined use of

a) computer, storage, and network resources that support the flow, storage, processing, analysis and protection of data according to a defined architecture, irrespective of whether the provisioned resources are physical infrastructure or virtualised through software using underlying physical infrastructure, located centrally in one place or spread across regions or countries, and which may be operated or controlled by the Licence Holders and/or one or more third parties;

b) *System Software* – including but not limited to firmware, operating systems and device drivers, network management, IT security management, and cloud management software used to manage, operate and maintain cloud resource pools; *Programming Software* and its management - included but not limited to compilers, interpreters, debuggers and version control systems; and *Application Software* – included but not limited to database systems, sector-specific core software such as banking or insurance software, Customer Relationship Management (CRM), Enterprise Resource Management (ERP), Web portals, and communication suites;

'Thin Client' is used to describe a type of client/server computing in which applications are run, and data is stored, on the server rather than on the client. Because the applications are executed on the server, they do not require client-resident installation, although the graphical user interface and some application logic may be rendered to the client[31];

'Threat', a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm[32];

'Threat Intelligence', Threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes;

'Threat-Led Penetration Testing (TLPT)', a controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors. It is based on targeted threat intelligence and focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations[33];

'Virtual Machine (VM)', a software implementation of a hardware-like architecture, which executes predefined instructions in a fashion similar to a physical central processing unit (CPU). VMs can be used to create a cross-platform computing environment that loads and runs

[31] https://www.gartner.com/en/information-technology/glossary/thin-client
[32] https://www.sans.org/security-resources/glossary-of-terms/
[33] Source: G-7 Fundamental Elements

on computers independently of their underlying CPUs and operating systems[34];

'Vulnerability', a weakness, susceptibility or flaw of an asset or control that can be exploited by one or more threats;

'Waterfall Project Management' is a linear or sequential approach to project management where a project goes through well-defined stages or phases;

'Web Service' is a software service used to communicate between devices on a network. More specifically, a Web service is a software application with a standardised way of providing interoperability between disparate applications. It does so securely over HTTP with encryption, and uses standards, protocols or specifications such as XML, SOAP, WSDL, and UDDI[35];

'White Box Testing', also known as clear-box testing, this is a testing technique which involves examining source code to verify the flow of inputs and outputs through an application, with the aim of improving design, usability, performance, and strengthening security particularly by detecting known exploitable security vulnerabilities;

1.2.2 In the event that definitions contained in this document conflict with those stipulated in primary legislation, regulations or rules issued thereunder, the definitions set out in such legislation, regulations or rules shall prevail.

[34] https://www.gartner.com/en/information-technology/glossary/vm-virtual-machine
[35] https://www.techopedia.com/definition/25301/web-service

Title 2 High Level Principles

Principle 1 Proportionality

2.1.1 Without prejudice to specific criteria or requirements in sectoral level legislation and guidelines, the guidelines in this document are subject to the principle of proportionality. Their application should take into consideration the size, internal organisation and individual risk profile, as well as the nature, scope, complexity and riskiness of the Licence Holder's operation and of the services and products provided or intended to be provided, so that the objectives of regulatory requirements are effectively achieved.

2.1.2 In particular, governance arrangements should take into consideration the nature, scale and complexity of the Technology Arrangements, risks arising thereof, and the level of dependence on such Technology Arrangements for the implementation or execution of critical or important functions.

Principle 2 Principles-based consistency of outcomes

2.2.1 The Authority pursues an unwavering approach to regulatory compliance expected from all Licence Holders for consistency of outcomes across all sectors, irrespective of the Technology Arrangements employed. In view of technology dynamics from the perspective of continuous technology evolution and service models, the guidelines are principles-based and do not favour one type of technology or service model over another, as long as compliance obligations can be met. The principles-based approach also applies to ICT risk and security governance and control frameworks.

Principle 3 Information Assurance (IA) in Technology Arrangements

2.3.1 Without prejudice to the legal obligations set out in Regulation (EU) 2016/679 (EU GDPR) and Regulation (EU) 2018/1725 regarding the control and processing of personal data of natural persons, and any other applicable legal or regulatory requirements, communication and information systems must protect the data they handle in transit and at rest, and must only be accessible to authorised parties as and when needed.

2.3.2 Confidentiality, Integrity, Availability, Authentication and Non-repudiation should form the five pillars for IA[36] in the design of any Technology Arrangement implemented by a Licence Holder.

[36] Cited in Cyber Forensics Assurance (2010)

2.3.3 Confidentiality refers to the assurance that only authorised parties can access data. Information must be protected from disclosure to unauthorised individuals, systems or entities.

2.3.4 Integrity means that only authorised parties and software systems can modify data, and that the accuracy and completeness of information must be safeguarded during transmission and storage. Information must be protected from unauthorised modification or destruction.

2.3.5 Availability refers to the assurance that data will be accessible in a timely manner by authorised parties or software systems when needed, requiring IT resources and infrastructure to remain robust and fully functional even during adverse operating conditions, such as but not limited to, technical failures or when under a cyber-attack.

2.3.6 Authentication is the process of securely and accurately identifying and verifying the identity of a system, device or person requesting access to data, an information service, or other resource within a Technology Arrangement.

2.3.7 Non-repudiation is the ability to correlate, with high certainty, a recorded action with its originating individual, system, device or entity such that the validity of the action and ownership cannot be denied. It provides proof of the origin of data and its integrity.

Principle 4 Approach to cloud computing

2.4.1 The approach to adoption of cloud computing resources and services should be based on sound governance and management and should take into consideration the Guiding Principles for Cloud Computing Adoption and Use[37], issued by the global non-profit IT association ISACA, as outlined in clauses 2.4.2 to 2.4.7.

2.4.2 *The Enablement Principle:* Cloud computing planned as a strategic enabler, rather than as an outsourcing arrangement or technical platform.

2.4.3 *The Cost/Benefit Principle:* The benefits of cloud acquisition should be evaluated against a full understanding of the costs of cloud compared with the costs of other technology platform business solutions.

2.4.4 *The Enterprise Risk Principle:* The management of adoption and use of cloud should be taken from an Enterprise Risk Management (ERM) perspective.

2.4.5 *The Capability Principle:* The full extent of capabilities that cloud providers offer should be integrated with internal resources to provide a comprehensive technical support and delivery solution.

[37] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Guiding-Principles-for-Cloud-Computing-Adoption-and-Use.aspx

2.4.6 *The Accountability Principle:* The internal and cloud provider responsibilities should be clearly defined such that accountabilities are managed accordingly.

2.4.7 *The Trust Principle:* Trust results from the combined effect of organisational structure, culture, technical architectures, processes and the human factors that facilitate the deployment and use of technology in support of business functions. Trust should be built into all business processes that depend on cloud services, particularly by establishing clear Information Assurance (IA) requirements in the design of the Technology Arrangements.

Title 3 Technology Arrangements

Section 1 Essential characteristics of Cloud Computing

NIST[38] provides the five essential characteristics that define the cloud model as follows:

3.1.1 *On-demand Self-service:* Resources such as computer and network storage can be provisioned on-demand and are typically self-provisioned by the customer without requiring human interaction with the service providers.

3.1.2 *Broad Network Access:* Capabilities are available over the Internet or a private network and accessed through standard mechanisms.

3.1.3 *Resource Pooling:* In a multi-tenant model resources (e.g. storage, processing, memory, and network bandwidth), whether physical or virtual, are dynamically assigned and reassigned to serve multiple consumers of services according to demand. Consumers of such services generally have no control or knowledge over the exact location of the provided resources, other than specifying location at a high level of abstraction e.g. country and/or data centre region.

3.1.4 *Rapid Elasticity*: Provisioned resources can be rapidly scaled up or down, according to demand. Customers typically have the option to enable automatic scaling of resources, or to affect changes manually or programmatically.

3.1.5 *Measured Service:* Service usage, that is consumption or allocation of resource(s)/ service(s) provided, is metered using a unit of measure appropriate to the type of service (e.g. active user accounts, terabytes of provisioned storage, outbound data transfer over the Internet in GB/month). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of services.

3.1.6 *Cloud Infrastructure* is the collection of hardware and software that enables the above five essential characteristics of Cloud Computing.

Section 2 Cloud Computing Service Models

Cloud Computing is offered through the following service models:

3.2.1 *Infrastructure as a Service (IaaS):* The consumer of the service self-provisions processing (computer), storage, networks, and other fundamental computing resources in order to deploy and run arbitrary System, Programming and Application Software. The consumer does not manage or control the underlying Cloud Infrastructure but has full control over operating systems, storage, deployed applications, and

[38] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

possible limited control of select networking components such as host firewalls.

3.2.2 *Platform as a Service (PaaS):* The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools provided by the Cloud Service Provider (CSP). The consumer does not manage or control the underlying Cloud Infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. PaaS provides the building blocks such as managed database, development framework and middleware in a Technology Arrangement upon which developers write custom Application Software with the provided tools.

3.2.3 *Software as a Service (SaaS):* The capability provided to the consumer of the service is to use the provider's Application Software running on a Cloud Infrastructure. The applications are accessible from various client devices (e.g. laptops, tablets and smartphones), typically through a thin client interface such as a web browser. The consumer does not manage or control the underlying Cloud Infrastructure including network, servers, operating systems, storage, or even individual application capabilities, except for possibly limited user-specific application configuration settings.

3.2.4 *Anything as a Service (XaaS):* Cloud technology and service models are continuously evolving. Beyond the NIST-defined IaaS, PaaS and SaaS, industry players continuously innovate in the market to offer new concepts and services, such as Desktop as a Service (DaaS) and Identity and Access Management as a Service (IAMaaS). In all cases, this is about shifting away from on-premises infrastructure and operations in favour of outsourcing more functions or activities that are managed by a service provider, but which are relatively easily integrated in process chains as part of workflow orchestration through software integration and automation.

3.2.5 *Business Process as a Service (BPaaS):* Organisations have been outsourcing business tasks, functions or processes for decades. The nature of the delivery model is however changing rapidly through technology. Gartner[39] defines BPaaS as the delivery of business process outsourcing (BPO) services that are sourced from the cloud and constructed for multitenancy. Services are often automated, and where human process actors are required, there is no overtly dedicated labour pool per client. As a cloud service, the BPaaS model is accessed via Internet-based technologies, whether through a human interface, such as a web portal, or programmatically through Web services for integration in a Technology Arrangement. BPaaS typically sits on top of the other three foundational cloud services i.e. SaaS, PaaS and IaaS, and therefore takes the XaaS concept to a whole new level. An

[39] https://www.gartner.com/it-glossary/business-process-as-a-service-bpaas/

example of BPaaS in the financial services sector is Identity Verification as a Service, where Identity Verification is used as part of the Know Your Customer (KYC) and Anti-Money Laundering (AML)/Combating the Financing of Terrorism (CFT) procedures within an authorised entity through methods such as Electronic Identity Verification (eIDV) and/or biometrics (face verification/authentication).

Section 3 Cloud Computing Deployment Models

There are four prominent deployment models in the cloud that organisations opt for when it comes to leveraging cloud solutions. They are defined by NIST as follows (3.3.1 to 3.3.4):

3.3.1 *Private Cloud:* The Cloud Infrastructure is provisioned for the exclusive use by a single organisation comprising multiple consumers (e.g. the organisation's employees and/or its customers). It may be owned, managed, and operated by the organisation, a third party, or some combination of them, and it may exist on or off premises. Colocation is a private cloud deployment model where the organisation purchases or leases servers, networking equipment, software and rack space, all of which reside in a data centre managed by the colocation services provider.

3.3.2 *Community Cloud:* The Cloud Infrastructure is provisioned for exclusive use by a specific community of consumers from organisations that have shared interests and concerns (e.g. mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organisations in the community, or a third party, or some combination of them, and it may exist on or off premises.

3.3.3 *Public Cloud:* The Cloud Infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider.

3.3.4 NIST defines *Hybrid Cloud* as Cloud Infrastructure composed of two or more distinct Cloud Infrastructures (private, community, or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability. It typically refers to a cloud computing environment that uses a mix of on-premises private cloud and third-party private or public cloud services with orchestration between the platforms to form the underlying Cloud Infrastructure of a Technology Arrangement.

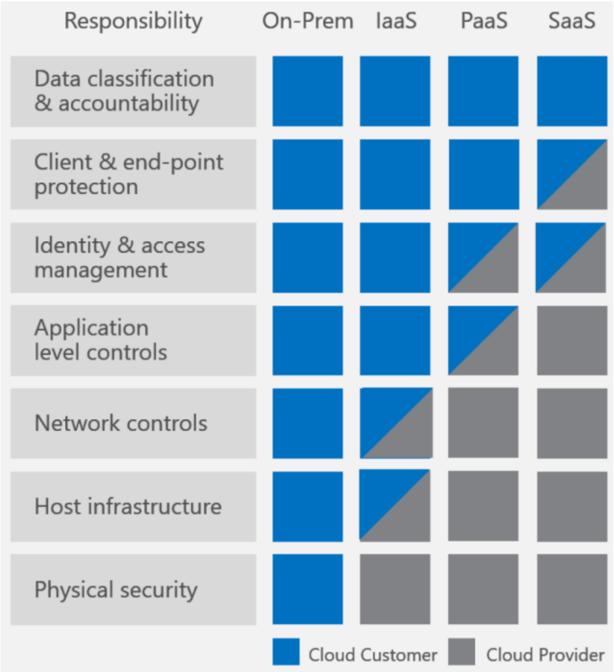
3.3.5 *Virtual Private Cloud (VPC):* Most leading public IaaS providers can offer enhanced isolation (see Section 5) among tenants by allocating compute, storage and network resources within a private IP network which is logically separated from traffic pertaining to other customers or CSP management traffic. The private network is typically accessed remotely by the customer through a VPN function by means of authentication and encrypted communication channels over the Internet or leased circuits. The same technology can be used to achieve a seamless Hybrid cloud environment where the on-premises network is extended to the VPC.

3.3.6 It is to be noted that SaaS/XaaS/BPaaS solutions are often built to be deployed as multi-tenant applications or suite of applications that is/are managed and operated by the solution vendor. Depending on the scale of the vendor's operation, the underlying Cloud Infrastructure is either deployed as a private cloud in one or more data centres, or more typically deployed as a Virtual Private Cloud in a public cloud leveraging IaaS and PaaS, taking benefit of the CSP's scale and global reach, even if the SaaS provider may also be a multinational.

The result is that in most cases, the use of Cloud services involves complex outsourcing and sub-contracting chains, and which therefore demands a well-defined shared responsibility model with respect to security and compliance obligations at every stage in the chain.

Section 4 Shared responsibilities for different cloud service models

3.4.1 In Technology Arrangements which are completely on premises, control and responsibility should rest entirely on the management of the firm. Control and responsibility start shifting towards the Cloud Service Provider, the higher the level of abstraction of the underlying layers as shown in the following diagram.



Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	🟦	🟦	🟦	🟦
Client & end-point protection	🟦	🟦	🟦	◩
Identity & access management	🟦	🟦	◩	◩
Application level controls	🟦	🟦	◩	⬛
Network controls	🟦	◩	⬛	⬛
Host infrastructure	🟦	◩	⬛	⬛
Physical security	🟦	⬛	⬛	⬛

🟦 Cloud Customer ⬛ Cloud Provider

Source: Microsoft[40]

[40] Microsoft Technet (4/4/2017) https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91

3.4.2 In the case of colocation (not shown in the diagram), responsibility is the same as in on premises deployment, except for data centre management, where the colocation provider is responsible for the latter's facilities and physical security. Some colocation providers also provide additional managed services such as connectivity and network protection (e.g. DDOS protection), in which case responsibility for network controls is also shared.

Section 5 Isolation in virtualised environments

3.5.1 While multi-tenancy provides material economic benefits through multiplexing physical resources (computing, networking, storage) and services among customers and distributing the resource costs accordingly, the practice introduces Information Assurance (IA) or cybersecurity risks and compliance challenges.

3.5.2 Isolation is a core security challenge in virtualised environments and cloud services. Cloud Infrastructures are generally designed and implemented in a way that mitigates against threats to data confidentiality, integrity and availability. Isolation measures implemented by CSPs at various layers and across different virtualised resources need to be understood.

3.5.3 In IaaS, the unit of software application packaging and isolation is the virtual machine (VM). Unlike SaaS and PaaS, where customers do not have permission to access underlying components of the service, IaaS customers have complete control on the rented services, and this increases the possibility of cross-VM side channel attack exploits[41]. IaaS users need to understand how compute, storage and network isolation is achieved, over and above tenant account isolation and isolation from CSP administrators, and furthermore, should implement a VPC architecture to further increase isolation.

3.5.4 Containers are a popular, more current, alternative to VMs in cloud deployments because they provide better portability across Cloud Infrastructures, are lightweight, and provide better computer performance. It must be noted, however, that containerisation only provides process-level isolation as containers share the host Operating System. This reduced level of isolation needs to be considered in risk-benefit analyses of IT architecture design in Technology Arrangements if the host operating system of choice does not provide the required level of cutting-edge resource isolation features within its kernel. Furthermore, it must be noted that where containers are deployed through a Container as a Service (CaaS) model, and not within a customer provisioned VM, the CSP takes over responsibility of the host operating system along with the rest of the underlying layers, including the container's control plane.

[41] Mohammad-Mahdi Bazm, Marc Lacoste, Mario Südholt, Jean-Marc Menaud. Isolation in Cloud Computing Infrastructures: New Security Challenges. Annals of Telecommunications - annales des télécommunications, Springer, In press. ⟨hal-01874206⟩

3.5.5 Tenant isolation architecture in SaaS/XaaS should be particularly understood as part of governance, risk and compliance assessments, because isolation levels vary significantly among solution vendors and service providers.

Tenant isolation can be implemented at account level at the application layer, with significant variations in the underlying layers e.g. separate database or separate tables/schemas per tenant account vs. shared database or shared schema/tables across multiple tenants. At the other end of the spectrum, different SaaS/XaaS tenants may not only be isolated at application and backend level but may also be isolated at virtual machine, container or VPC level, and even at IaaS tenant account level.

Section 6 Monolithic, Microservices and Serverless architectures

3.6.1 Legacy financial services monolithic core software platform architecture, or one enhanced with classic Enterprise Service Bus integration leveraging centralised storage, is proven in the field to be stable and largely cyber resilient but carries the burden of accumulated technical debt and software entropy.

3.6.2 Incumbents in the financial services industry may be faced with the dilemma of leaving the comfort zone of monolithic software architecture for newer, fine-grained, loosely coupled Microservices and/or Serverless architecture that enables firms to be agile, competitive and innovative in the fintech era, but which raises the need for a higher level of cybersecurity preparedness and cyber resilience.

3.6.3 The need for operating efficiency and agility, shorter time-to-market, consumption of diverse Web services provided by business partners and service providers, as well as those provided to a firm's downstream customers, and an IT architecture that must enable connectivity to anything, anywhere, any time in the financial services industry is a clear signal that fine-grained, loosely coupled architecture will inevitably become dominant over time. There is no one-size-fit-all architectural solution, but APIs are fast becoming a key competitive factor in the industry, and a loosely coupled architecture is a critical success factor for adoption. IT modernisation or greenfield deployments must be considered broadly, deeply and strategically.

3.6.4 Every architectural pattern has its advantages and disadvantages, and the approach needs to take into consideration the firm's business strategy, ICT management capabilities, risk appetite and tolerance. Furthermore, not all architectural patterns are suitable for any use case. Serverless designs, for example, are more suitable for short-lived, stateless applications at their current technology maturity level. It is recommended, therefore, that financial services operators consider the complexity of the intended Enterprise Architecture end-state if multiple architectural patterns are involved, the maturity of the different technologies, frameworks and tooling to be adopted, and their long-run suitability for the firm to achieve expected levels of governance, risk management, and regulatory compliance.

3.6.5 Major cloud service providers readily provide the infrastructure and tools for the implementation of Microservices and Serverless architecture in the cloud, with a high level of abstraction, for the implementation of cloud-native loosely coupled designs. Attention should be given to service provider lock-in risks, that would make porting out to a different service provider difficult, and which would therefore make it difficult for Licence Holders to meet relevant existing regulatory obligations related to outsourcing of critical or important functions with respect to the firm's ability to in-source or change outsourcing arrangements satisfactorily and in a timely manner if need be.

3.6.6 Licence Holders are also advised that the Authority has supervisory oversight obligations vis-à-vis systemic risk originating from concentration risks, including those resulting from outsourcing to a dominant service provider or closely connected service providers.

3.6.7 In view of 3.6.5 and 3.6.6, it is therefore being recommended that Licence Holders carefully consider Cloud portability in general, but especially:

a) the benefits and risks of combining Microservices with a well-established, mature container orchestration platform and application packaging framework if heading towards a loosely coupled architectural pattern;

b) reliance on any vendor proprietary software offered as PaaS and integrated in a Technology Arrangement serving a critical or important function, and where such software or middleware may not be readily offered as PaaS by other Cloud providers. This includes, but is not limited to, databases as a service (DBaaS);

c) the use of Identity and Access Management as a Service (IAMaaS/IDaaS), including Just-In-Time Privileged Access Management (JIT PAM);

d) Disaster recovery architecture in the Cloud which may include cloud-provider-specific elements embedded in the overall design of the Technology Arrangement.

3.6.8 It is recommended that the risks and benefits of the cloud-agnostic containerisation design approach, if applicable to a Licence Holder considering a technology refresh or greenfield deployment, are also weighed up even if the firm's technology modernisation strategy is exclusively based on an on-premises only policy for the foreseeable future, as this leaves options open for a hybrid cloud deployment or complete migration to the cloud in the future with reduced risk and effort.

Section 7 Unrestricted audit, on-site and remote access, and information gathering and investigations.

3.7.1 Technology Arrangements should be implemented in a way that guarantee all legal and regulatory compliance requirements, including competent authorities' rights to information gathering, right of access and right to audit (remote and on premises) irrespective of deployment method, to fulfil their legal obligations.

Section 8 Security Monitoring, DLP, eDiscovery, and forensic capabilities

3.8.1 Without prejudice to the principle of proportionality, Licence Holders should make use of SIEM tools for round-the-clock real-time analysis of logs and security alerts generated by applications and network infrastructure, whether on premises or in the cloud, and for correlation of security events which enables Licence Holders to get the bigger picture of cyber threats and indicate a security issue. Licence Holders operating complex Technology Arrangements should augment their security information and event management setup with security orchestration, automation and response (SOAR) and Cyber AI technology to improve security incident management by automating responses to low-level incidents, streamlining security operations and achieve higher efficiency and effectiveness.

3.8.2 In modern times of complex and distributed information architecture involving large volumes of on-site and off-site, structured and unstructured data, the implementation of Data Loss Prevention (DLP) technology within a Technology Arrangement as part of a data governance framework is critical for effective regulatory compliance and protection of data in use, in motion and at rest.

3.8.3 The mix of network, storage and endpoint DLP should be tailored according to the organisation's needs and specific Technology Arrangements. Classic on-premises DLP solutions may need to be supplemented with a Cloud Access Security Broker (CASB)[42] for effective risk and data governance that extends into the cloud. Furthermore, the DLP solution should ideally be enhanced with User and Entity Behaviour Analytics (UEBA)[43] that leverage pattern recognition, statistical analysis and Machine Learning to mitigate against complex breaches involving anomalous user behaviour.

3.8.4 Authorised entities should complement DLP with eDiscovery capabilities to efficiently and effectively facilitate the identification, preservation, collection, processing, review, analysis, production and presentation of Electronically Stored Information (ESI), comprising both structured or unstructured data, when responding to internal,

[42] https://www.gartner.com/it-glossary/cloud-access-security-brokers-casbs/
[43] https://www.gartner.com/reviews/market/user-and-entity-behavior-analytics

due diligence, litigation or regulatory requests in a timely and comprehensive manner.

3.8.5 The dynamic allocation and release of resources in elastic computing and highly virtualised environments, irrespective of whether deployed on premises or in the cloud, as well as the possibility of dynamic geographic spread of data at rest and in transit in Technology Arrangements involving Cloud Infrastructure, also increases the complexity of live or post mortem forensic investigations by law enforcement agencies or internal investigations, and the collection of forensically sound digital evidence. Licence Holders should therefore ensure that Technology Arrangements include the necessary tools (e.g. for taking forensically sound virtual machine images, or cloud-based storage snapshots), some of which may need to be provided by CSPs, infrastructure or middleware vendors, that facilitate such activities under an appropriate governance structure and documented procedures.

3.8.6 Without prejudice to orders that might be given by a court of law or a law enforcement agency during the course of any investigation, the documented procedures mentioned in 3.8.5 should contain sufficient information that helps investigators collect evidence in order of volatility if need be, such that as little data as possible is lost due to the passage of time.

3.8.7 Technical obstacles, contractual and/or geopolitical matters may result in unrealisable targets in planned Technical Arrangements proposed by entities seeking authorisation or existing Licence Holders planning migrations to new Technical Arrangements. These may also affect the Authority's ability to locate and/or retrieve relevant and meaningful data, in a timely and efficient manner, in the course of fulfilling its legal supervisory obligations, and to exercise its investigative and enforcement powers or proportionate enforcement action in the case of authorised Licence Holders found to be in breach of regulatory requirements.

Section 9 Consumption of cloud services over the Internet

3.9.1 The nature of the Internet needs to be kept in mind during the design of Technology Arrangements as firms have no control over the traffic that traverses the public Internet. The Internet backbone was designed decades ago for least-cost routing and not for best network performance. This can, and does at times, result in performance problems when cloud services are consumed over the public Internet.

3.9.2 Licence Holders should take into consideration Internet backbone limitations and implement appropriate network engineering solutions as part of their Technology Arrangements to mitigate against potential performance issues related to the nature of the Internet and the consumption of Cloud services. Not all parts of a complex Technology Arrangement may require the same type of network access or backhaul solution to the core network. The choice of technology or mix of technologies, such as but not limited to public Internet, MPLS, leased circuits, and SD-WAN overlay network solutions, that could be implemented as part of a Technology Arrangement, and the level of redundancy, should be included in cost/benefit and risk assessments, particularly in the case of critical or important functions.

Section 10 Artificial Intelligence (AI) and Machine Learning

3.10.1 AI and Machine Learning technology is increasingly being introduced in front-end and back-end operations across the financial services industry. The technology is therefore impacting processes, products and services, and markets. Use cases include Robo-Advisors, Chatbots, Algorithmic trading, Loan/Insurance underwriting, AML/CFT and fraud detection, and cybersecurity threat intelligence.

3.10.2 While the use of Machine Learning in conjunction with big data analytics increases automation opportunities, the technology may introduce legal, conduct, reputation, and overall ICT and security risks.

3.10.3 From a financial stability perspective, the adoption of AI systems, especially those employing Machine Learning methods and models, may increase dependence on third parties and potential concentration risks of systemically important players that fall outside the regulatory perimeter. Concentrated use of Machine Learning algorithms could, in theory, also amplify financial shocks in the market if such algorithms can be influenced by herd behaviour[44].

3.10.4 From a micro-prudential perspective, deficiencies in the governance of the use of AI and Machine Learning could lead to lack of clarity about responsibilities between authorised firms and service providers, as well as opportunities for insider or external advanced cybercriminal activity that exploits machine learning optimisation techniques and/or predictable behaviour patterns.

3.10.5 Authorised firms are expected to demonstrate that they understand and can manage effectively the risks introduced by AI, including Machine Learning, in software components of Technology Arrangements irrespective of whether such technology resides on-premises or in the cloud.

3.10.6 Licence Holders should ensure that, apart from guidelines under Title 4 regarding information security, and guidelines under Title 5 regarding outsourcing arrangements, and without prejudice to any applicable regulations and guidelines issued by competent authorities regulating AI, the use of AI in Technology Arrangements – including those used in fully outsourced business functions – should at least

[44] Artificial Intelligence and machine learning in financial services - Market developments and financial stability implications - 1 November 2017

meet the following conditions, subject to the principle of proportionality:

a) From a governance perspective, evidence should be available at all times to prove that the use of specific AI, including Machine Learning models, in decision-support or fully automated processes in critical or important functions can generate results that are reproducible, traceable and verifiable, using models that are interpretable and explainable, such that the Licence Holder can meet all regulatory obligations including those laid down in Regulation (EU) 2016/679 (GDPR) and the requirement for transparency and explainability to fulfil customers' rights and freedoms as data subjects needing to know how they were impacted by a decision involving automated data processing;

b) Auditable logs of automated recommendations or decisions should contain enough information to enable such data to be used to test logic leading to outcomes, and which therefore may be used to test for potential algorithmic bias, AI malfunction or malicious use of AI;

c) Thorough documentation of testing and training of Machine Learning algorithms outcomes under controlled conditions using unbiased and accurate data and feedback mechanisms is kept for supervisory oversight. Such data should be archived securely and read-only protected for future reference if necessary;

d) Fully documented and regularly audited controls are in place for periodic checking for:
   a. bias in algorithmic output;
   b. malfunctions; and
   c. malicious use of AI;
   in critical or important functions;

e) A documented migration or exit plan is in place in the case of potential irreversible malfunctioning of AI in critical or important functions.

3.10.7 The Management Body of Licence Holders retains full responsibility for compliance with all regulatory requirements and conditions for authorisation. Licence Holders should ensure that their Management Body is duly informed of relevant planned changes to Machine Learning algorithms, as well as what test data is being used for such process, where such data is being processed, and the outcomes according to 3.10.6 (a).

3.10.8 Licence Holders are further reminded of protection of data obligations, and the potential impact of a confidentiality breach or failure to ensure data availability and integrity on the Licence Holder and its clients, including but not limited to compliance with Regulation (EU) 2016/679 (GDPR). Licence Holders should ensure proper management, protection and disposal of personal and financial data, whether it is test or training data, or production data, especially in the case of multi-tenant cloud-based AI services.

3.10.9 AI technologies used by Licence Holders should respect the principle and legal obligation of equality and non-discrimination.

AI systems should be audited and monitored to ensure equality, fairness, accountability and robustness.

A human-centric approach to AI in financial services should be adopted, where decisions are ultimately taken by humans, not machines.

Persons designing, operating and using the results from AI processes should be trained to avoid discriminatory outcomes and pro-actively ensure equality in the design of algorithms, in the algorithmic inference and in the data feeding the algorithms.

Gender impact assessments should be conducted to analyse whether specific groups of women and men are directly or indirectly affected during all stages of the algorithmic process.

Title 4 ICT and Security Risk Management

Section 1 Subject matter and scope

4.1.1 Clauses under Title 4 specify the internal governance and risk management measures that Licence Holders should take to manage risks associated with Technology Arrangements, their operations, and data therein.

4.1.2 An ICT and Security Risk is defined by the EBA Guidelines on common procedures and methodologies for supervisory review and evaluation process of 19 December 2014 (EBA/GL/2014/13, amended by EBA/GL/2018/03) as a risk of loss due to breach of confidentiality, failure of integrity of systems and data, inappropriateness or unavailability of systems and data or inability to change information technology (IT) within a reasonable time and with reasonable costs when the environment or business requirements change (i.e. agility). This includes security risks resulting from inadequate or failed internal processes or external events including cyber-attacks or inadequate physical security. ICT and Security Risk Management is further defined by the EBA Guidelines on ICT and Security Risk Management (EBA/GL/2019/04).

4.1.3 Governance and Risk Management measures of outsourcing arrangements involving Technology Arrangements are addressed in more detail under Title 5.

4.1.4 ICT is a major enabler of business continuity, particularly through effective Disaster Recovery Planning, but Business Continuity Planning ('BCP') is broader in scope than the availability, continuity and recoverability of ICT services and information assets. Guidelines provided in this document in relation to business continuity are limited in scope to the management of ICT risk and not the broader BCP.

Section 2 Implementation and application

4.2.1 The guidelines under Title 4 set out the Authority's expectations with regard to ICT and Security Risk Management.

4.2.2 Where Licence Holders outsource elements of ICT and security risk management to the parent entity or to another subsidiary of the parent entity, the guidelines under Title 4, particularly Sections 3 and 4, should be read in conjunction with Section 2 under Title 5.

Section 3 ICT governance

4.3.1 The Management Body of the Licence Holder should ensure that there is an adequate internal governance and internal control framework in place covering ICT risk management as part of an overarching operational risk management framework, in accordance with all applicable legal and regulatory requirements, and sector-specific guidelines.

4.3.2 The Management Body should set clear roles and responsibilities on ICT management, cybersecurity/information security management, as well as business continuity management.

4.3.3 Senior Management should ensure that the organisation has enough human resources with the necessary skill sets to support the ICT operational needs, including effective ICT risk management on an ongoing basis, and to ensure the implementation of the ICT strategy. Senior Management should also ensure that all staff involved in ICT operations and ICT risk management receive continuing professional development, training, or (re)certification commensurate with the individuals' roles and responsibilities as required. Furthermore, Senior Management should ensure that all staff in the organisation are suitably trained, at least annually, on information security through cybersecurity awareness initiatives in accordance with the organisation's information security framework (see Section 4.7.29-4.7.31) to mitigate against a continuously evolving cybersecurity threat landscape, and to ensure compliance with all applicable Acts and Regulations, *inter alia*, Regulation (EU) 2016/679 (EU GDPR). Records of trainings carried out including evidence of attendance should be kept.

4.3.4 The Management Body should ensure that the budget allocated to fulfilling the requirements outlined in 4.3.3 is appropriate and sufficient within the constraints of, and to effectively implement risk management commensurate with, the appetite and tolerance for risk of the organisation.

4.3.5 The Management Body has overall accountability for setting, approving and overseeing the implementation of Licence Holders' ICT strategy as part of their overall business strategy as well as for the establishment of an effective risk management framework for ICT and security risks.

Section 4 ICT strategy

4.4.1 The ICT strategy should be aligned with the Licence Holder's overall business strategy and should define:

a) how Licence Holders' ICT should evolve to effectively support and participate in their business strategy, including the evolution of the organisational structure, ICT system changes and key dependencies with third parties;
b) how the ICT operations and ICT risk management organisational structure need to develop accordingly;
c) clear information security objectives, focusing on people, process and technology (i.e. ICT systems and ICT services).

4.4.2 Licence Holders should establish an implementation programme supported by a set of action plans that contain measures to be taken to achieve the objective of the ICT strategy, which should be communicated to all relevant staff (including third party providers) where applicable and on a need-to-know basis. The action plans should be periodically reviewed to ensure their relevance and appropriateness. Licence Holders should also establish a process to monitor and measure the effectiveness of the implementation of the ICT strategy which should be reviewed and updated on a regular basis.

Section 5 Use of third-party providers

4.5.1 Without prejudice to any sector-specific regulatory requirements and guidance, Licence Holders should follow the guidelines under Title 5 to ensure the effectiveness of risk mitigating measures and compliance requirements involving outsourcing arrangements.

Section 6 ICT Risk Management

4.6.1 The three lines of defence model ('3LOD') is an important part of the Basel Committee on Banking Supervision's 2011 Principles for the sound management of operational risk. It is adopted in EBA's Guidelines on internal governance under Directive 2013/36/EU (CRD IV).

4.6.2 Pillar 2 of Solvency II effectively delineates internal control and compliance as the second line of defence, as being separate from operational risk management practices and processes in place within functions responsible for operations on a day-to-day basis, while internal audit provides reasonable assurance as the third line of defence. ICP 8 of the Insurance Core Principles ('ICP')[45] adopted by the International Association of Insurance Supervisors ('IAIS'), of which the Authority is a signatory to the Multilateral Memorandum of Understanding, also advocates the use of 3LOD as an internal control system.

4.6.3 ESMA's "Guidelines on certain aspects of the MiFID compliance function requirements"[46], embrace the 3LOD model for internal control purposes. This approach has been carried forward in ESMA's Consultation Paper on "Guidelines on certain aspects of the MiFID II compliance function Requirements"[47].

4.6.4 *Organisation and objectives* Taking into consideration 4.6.1 to 4.6.3, Licence Holders should identify and manage their ICT risks according to the three lines of defence model or similar internal control framework in use at their organisation that is approved by the Authority, and that ensures similar outcomes as outlined further below in this section, without prejudice to the Principle of Proportionality, applicable Acts, Regulations, rules or sector-specific guidelines.

[45] https://www.iaisweb.org/page/supervisory-material/insurance-core-principles

[46] https://www.esma.europa.eu/sites/default/files/library/2015/11/2012-388_en.pdf

[47] https://www.esma.europa.eu/sites/default/files/library/cp_on_compliance_function_guidelines_for_publication.pdf

The ICT function(s) in charge of ICT systems, processes and security operations should have appropriate processes and controls in place to ensure that all risks are identified, analysed, measured, monitored, managed, reported and kept within the limits of the Licence Holder's risk appetite and that, the projects and systems they deliver and the activities they perform are in compliance with external and internal requirements.

Licence Holders should define and assign key roles and responsibilities, and relevant reporting lines, for the ICT and security risk management framework to be effective. For the avoidance of doubt, the control framework for ICT risks should be fully integrated into, and aligned with, the Licence Holder's overall risk management framework.

4.6.5 ICT functions in charge of Technology Arrangements, processes and security operations are responsible for managing risks they incur in conducting their activities on a day-to-day basis and should therefore have controls in place to mitigate such risks. These functions act as the first line of defence and should operate under the ICT risk oversight of an internal control function acting as a second line of defence.

4.6.6 The internal control function for ICT risk should be situated outside the function responsible for Technology Arrangements in order to further ensure independence and avoidance of conflicts of interest. While taking into consideration the principle of proportionality, the complex nature of cyber risk and the constantly evolving cybersecurity threat landscape necessitates cybersecurity specialist knowledge at the second line of defence, whether insourced or outsourced, that is sufficient to ensure effective oversight of cyber risk management operating at the first line of defence.

4.6.7 This control function should be directly accountable to the Management Body and responsible for monitoring and controlling adherence to the ICT and security risk management framework. It should ensure that ICT and security risks are identified, measured, assessed, managed, monitored and reported. It should scrutinise and challenge the first line of defence's management of ICT risks, including cyber risk identification and mitigation.

4.6.8 The internal audit function, following a risk-based approach, acting as the third line of defence should have the capacity to independently review and provide assurance of the compliance of all ICT and security-related activities and units of a Licence Holder with its policies and procedures and with external requirements.

4.6.9 The management framework governing ICT risk should include processes in place to:

a) enable management to determine an appropriate risk appetite for ICT risks;
b) identify and assess the ICT risks to which the Licence Holder is exposed;

c) define mitigation measures, including controls, to mitigate ICT risks;

d) monitor the effectiveness of these measures as well as the number of reported incidents affecting the ICT related activities, taking timely actions to correct the measures where necessary and track their implementation;

e) report to the Management Body on the ICT risks and controls;

f) identify and assess whether there are any ICT and security risks resulting from any major change in ICT system or ICT services, processes or procedures, and/or after any significant operational security incident.

4.6.10 The framework should be documented and continuously improved with 'lessons learned' during its implementation and monitoring.

4.6.11 Before any major change, that is a high risk change, in the Licence Holder's Technology Arrangements, processes or procedures, the first line of defence should identify and assess the ICT risks involved and implement mitigating measures as part of the change. Identification and assessment of ICT risks should also be carried out without undue delay after any significant operational or security incident. A significant operational incident is one which causes, or may cause, adverse impact on the provision of ICT services, or the quality of ICT services, including data integrity or availability, which is not due to a security incident.

4.6.12 Given its responsibility for ICT risk oversight, the function in charge of the second line of defence should ensure that the ICT risk framework is reviewed at least once a year. Any changes to the ICT risk framework should be approved by the Management Body.

4.6.13 Without prejudice to Principles 1 and 2 under Title 2, Licence Holders should adopt international corporate IT governance standards or best practice frameworks such as ISO/IEC 38500:2015 and COBIT[48] 5/COBIT 2019 respectively, which this Guidance document draws upon, to assist them in achieving organisational objectives for the governance and risk management of enterprise IT. COBIT provides an excellent framework for risk management and risk monitoring at the second and third lines of defence.

4.6.14 *Identification of functions, processes and assets*

Licence Holders should identify, establish and regularly update a mapping of their business functions, roles and supporting processes to identify the importance of each and their interdependencies related to ICT risks.

4.6.15 Additionally, Licence Holders should identify, establish and regularly update a mapping of the information assets supporting their business functions, and supporting processes, such as ICT systems, people, third parties and dependencies on other internal and external systems and processes, to be able to, at least, manage the information assets that

[48] The COBIT framework was created by ISACA.

support critical or important functions and processes identified in 4.6.14. Critical ICT systems and services are those that should fulfil at least one of the following conditions:

a) they support the core business operations and/or distribution channels of the Licence Holders;
b) they support essential governance processes and corporate functions, including risk management;
c) they fall under special legal, regulatory or commercial requirements that impose heightened availability, resilience, confidentiality or security requirements, possibility with mandated RTO and RPO objectives;
d) they process or store confidential or sensitive data to which unauthorised access could significantly impact the Licence Holder's reputation, financial results or the soundness and continuity of its business; and/or
e) they provide baseline functionalities that are vital for the adequate functioning of the Licence Holders (e.g. telecom and data connectivity services, ICT and cybersecurity services).

4.6.16 *Classification and risk assessment*

Licence Holders should categorise the identified business functions, supporting process, information assets, various ICT systems (software and hardware components) making up their Technology Arrangements, and other physical assets such as server rooms and workplaces, in terms of criticality based on the mapping outlined in 4.6.14 and 4.6.15.

4.6.17 Licence Holders should, at a minimum, determine confidentiality, integrity and availability requirements necessary to meet the nature and importance of the identified functions and processes. Information asset owners should be identified and given accountability for classification.

4.6.18 Licence Holders should review the adequacy of the classification of the information assets and relevant documentation, when risk assessments are performed.

4.6.19 Licence Holders should identify the ICT risks that impact the identified and classified business functions, supporting processes, and information assets, according to their criticality. This risk assessment should be carried out and documented, annually or at shorter intervals if required. Such risk assessments should also be performed on any major change of infrastructure, process or procedures affecting the business functions, supporting processes or information assets and consequently update the current risk assessment of Licence Holders. The depth, detail and intensity of the assessment should be proportionate to the size, structure and operational environment of the Licence Holders as well as the nature, scale and complexity of its activities.

4.6.20 *Risk mitigation*

Based on the risk assessments, Licence Holders should determine which measures are required to mitigate identified ICT risks to acceptable levels and whether changes are necessary to the existing business processes, control measures, and Technology Arrangements. Licence Holders should consider the time required to implement these changes and the time to take appropriate interim mitigating measures to minimise ICT and/or security risks to stay within the Licence Holder's ICT risk appetite.

4.6.21 Licence Holders should define and implement measures to mitigate identified ICT risks and protect information assets in accordance with their classification.

4.6.22 *Reporting* Risk Assessment results should be appropriately documented and reported to the Management Body in a timely manner, and, where applicable, to the Authority on an annual basis, or at shorter intervals if so determined by the Authority.

4.6.23 *Audit* The Licence Holder's governance, systems and processes related to the management of ICT risks and controls should be audited on a periodic basis by auditors having sufficient knowledge, skills and expertise in ICT risks and the nature of the Licence Holder's business to provide independent assurance of their effectiveness to the Management Body. The auditors should be independent from the Licence Holder's operations and any related conflicts of interest. The frequency and focus of such audits should be commensurate with the relevant ICT risks, and according to any Acts, Regulations, rules, or sector-specific guidelines.

4.6.24 ICT audits should be part of the Licence Holder's holistic audit plan as part of the Licence Holder's governance framework and approved by the Management Body. The audit plan and its execution, including audit frequency, should reflect and be proportionate to the inherent ICT risks of the Licence Holder's operations, and should be updated regularly.

4.6.25 A formal follow up process including provisions for the timely verification and remediation of critical security audit findings should be established.

4.6.26 *Continuous threat and vulnerability monitoring* Without prejudice to the provisions of 4.6.19 to 4.6.25 Licence Holders should ensure that they continuously monitor cybersecurity threats and vulnerabilities relevant to their business processes, supporting functions and information assets, and regularly review the risk scenarios impacting them. Threat monitoring is the analysis, assessment and review of audit trails and other information collected for the purpose of searching out system events that may constitute violations of system security[49]. Vulnerability analysis is the systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security

[49] https://csrc.nist.gov/glossary/term/threat-monitoring

measures, and confirm the adequacy of such measures after implementation[50]. Security monitoring is covered further in Section 7 from 4.7.14 to 4.7.17.

Section 7 Information security

4.7.1 *Security control framework*

There is no such thing as a one-size-fits-all approach to information security. Without prejudice to Principles 1 and 2 under Title 2, and sector-specific industry-driven frameworks such as PCI DSS, Licence Holders should, under the principle of proportionality, consider internationally recognised standards and frameworks such as ISO/IEC 27001:2017 (particularly in conjunction with 27002:2013 and/or 27017:2015), the NIST Cybersecurity Framework, or CIS Critical Security Controls and their security objectives, when implementing their security control framework.

4.7.2 *Information security policy*

Licence Holders should develop and document an information security policy, approved by the Management Body, that:

a) defines the high-level principles and rules to protect the confidentiality, integrity and availability of the Licence Holder's and its customers' information using a specific or hybrid security framework tailored to meet business objectives and regulatory requirements; and
b) should be based on the relevant results of the risk assessment process, as well as sector-specific compliance requirements.

4.7.3

As a minimum, the policy should include a description of the main roles and responsibilities for information security management and it should set out the requirements for people, processes and technology in relation to information security, recognising that staff at all levels have responsibilities in ensuring the Licence Holder's information security. The policy should ensure the confidentiality, integrity and availability of the Licence Holder's critical, logical and physical assets, resources and sensitive data whether at rest, in transit or in use. The information security policy should be communicated within the organisation and should apply to all employees. Relevant requirements from the information security policy should be communicated to third-party service providers, for example, in contractual agreements with such providers. In the case of Cloud service providers, particularly SaaS providers, where information security policy terms are set by the provider and are not negotiable, for example because of multi-tenancy, Licence Holders should ensure that the CSP's security policies, at least, meet the minimum requirements set out in the Licence's Holders information security policy as part of their pre-outsourcing assessment outlined in Section 10 under Title 5.

4.7.4

Based on the information security policy, Licence Holders should establish and implement security measures to mitigate the ICT risks they are exposed to. These measures should as a minimum include:

[50] https://csrc.nist.gov/glossary/term/vulnerability-analysis

a) independent information security function (section 4.7.5-4.7.6) and/or organisation and governance in accordance with paragraphs (section 4.6.5 – 4.6.8);
b) logical security (section 4.7.7);
c) physical security (section 4.7.9-4.7.11);
d) ICT operations security (section 4.7.12-4.7.13);
e) Security monitoring (section 4.7.14-4.7.17);
f) Information security reviews, assessment and testing (section 4.7.18 – 4.7.28);
g) Information security training and awareness (section 4.7.29-4.7.31).

4.7.5 *Information security function*

Licence Holders should establish, within their system of governance and in accordance with the proportionality principle, an information security function, with the responsibilities assigned to a designated person. Depending on the nature, scale, complexity and risk exposure of the Licence Holder's business, the function may require having a team of people reporting to the designated person to fulfil the function's obligations. Licence Holders should ensure the independence and objectivity of the information security function by appropriately segregating it from ICT operations processes (where the three lines of defence model is applied, this function should be a second line of defence function). In accordance with the Licence Holder's internal governance structure, Licence Holders should ensure that the information security function is not responsible for any internal audit. The function should report directly to the Management Body or the chair of the management function of the Management Body, that is Senior Management if applicable, according to the Licence Holder's internal governance structure.

4.7.6

The information security function should typically:

a) support the Management Body in defining and maintaining the information security policy and control its deployment;
b) monitor the implementation of the information security measures;
c) report and advise the Management Body regularly, and on an ad hoc basis as needed, on the status of information security, its developments, and risks to the Licence Holder;
d) ensure that the information security requirements are adhered to when using service providers;
e) ensure that all employees and third parties accessing information and systems are adequately informed of the information security policy, for example through information security training and awareness sessions;
f) coordinate operational or security incident examination and report relevant ones to the Management Body.

4.7.7 *Logical security*

Licence Holders should define, document and implement procedures for logical access control (identity and access management). These procedures should be implemented, enforced, monitored and periodically reviewed. The procedures should also include controls for monitoring anomalies, and should, at a minimum, implement the following (*note: the term 'user' also comprises technical users)*:

a) Need-to-know, Least Privilege and Segregation of Duties: Licence Holders should manage access rights to information assets and their supporting systems on a 'need-to-know' basis, including remote access. Users should be granted minimum access rights that are strictly required to execute their duties (principle of 'least privilege') i.e. to prevent unjustified access to a large set of data or that the allocation of combinations of access rights may be used to circumvent controls (principle of 'segregation of duties').

b) User accountability: Licence Holders should limit, as much as possible, the usage of generic and shared user accounts and ensure that users can be identified for the actions performed in the ICT systems.

c) Privileged access rights: Licence Holders should implement strong controls over privileged system access by strictly limiting and closely supervising staff with elevated system access entitlements (e.g. administrator accounts). Wherever feasible, and certainly in elastic/ephemeral cloud environments, a just-in-time privileged access model should be used where administrators elevate privilege by systematically requesting a new role assignment to obtain time-bound rights they need to perform an activity.

d) Remote access: In order to ensure secure communication and reduce risk, remote administrative access to critical ICT systems should be granted only on a need-to-know basis and when strong authentication solutions are used.

e) Logging of user activities: privileged users' activities, at a minimum, should be logged and monitored. Access logs should be secured to prevent unauthorised modification or deletion and retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets, in accordance with the provisions of 4.6.16-4.6.19, without prejudice to the retention requirements set out in EU and national law. Licence Holders should use this information to facilitate identification and investigation of anomalous activities that have been detected.

f) Access management: access rights should be granted, withdrawn or modified in a timely manner, according to predefined approval workflows involving the business owner of the information being accessed (information asset owner). In case of termination of employment access rights should be promptly removed.

g) Access recertification: access rights should be periodically reviewed to ensure that users do not possess excessive and/or unnecessary privileges and that access rights are removed when no longer required.

h) the granting, modification, withdrawal/removal of access rights should be documented in a way that facilitates comprehension and analysis.

i) User authentication methods: Licence Holders should enforce authentication methods that are sufficiently robust to adequately and effectively ensure that access control policies and procedures are complied with. Authentication methods should be commensurate with the criticality of ICT systems, the information or the process being accessed. This should as a minimum strong passwords or stronger authentication methods based on relevant risk (e.g. two-factor or multi-factor authentication for access that is fraud sensitive, allows access to highly confidential/sensitive information, or that could have material consequences for critical operations). Licence Holders subject to Directive (EU) 2015/2366 (PSD2) should ensure compliance with Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) and common and secure open standards of communication[51].

4.7.8
Electronic or programmatic access to data and ICT systems

Electronic access by applications to data and ICT systems should be limited to a minimum on an as-needed basis to provide the necessary service. While APIs play a crucial role in the hyperconnected fintech era, each additional API increases the attack surface. APIs therefore require protection through strong authentication and authorisation mechanisms, and encrypted communications. Without prejudice to the Authority's principles-based approach, and without prejudice to all applicable Acts, Regulations, rules, sector-specific guidelines and/or technical standards, Licence Holders should consider the following authorisation and authentication mechanisms for APIs:

a) OpenID Connect (OIDC) authentication over the OAuth 2.0 (RFC 6749) authorisation delegation protocol over TLS 1.3 encrypted transport for RESTful APIs. JSON Web Tokens (JWTs) can also be signed (RFC 7515) and encrypted (RFC 7516) for additional security.
b) SAML 2.0 with WS-Federation over HTTP protocol binding with TLS 1.3 encrypted transport, or SOAP binding with XML Digital Signature (XML-DSIG) and XML encryption 1.1, for legacy XML or SOAP based Web Services.

Licence Holders can refer to OpenID's Financial-grade API (FAPI) specifications[52] (currently in development) for further guidance on best practice additional API security. Licence Holders should also refer to ongoing developments in relation to the new Client Initiated Backchannel Authentication (CIBA) flow that replaces OAuth redirect mechanisms to support decoupled Strong Customer Authorisation flows under PSD2.

4.7.9
Physical security

Licence Holders' physical security measure should be defined, documented and implemented to protect its premises, data centres and sensitive areas from unauthorised access and from environmental hazards.

[51] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R0389&from=EN
[52] https://openid.net/wg/fapi/

4.7.10 Physical access to ICT systems should be permitted only for authorised individuals. Authorisation should be assigned in accordance with the staff's tasks and responsibilities, limited to individuals who are appropriately trained and monitored. Physical access should be regularly reviewed to ensure that unnecessary access is promptly revoked when not required.

4.7.11 Adequate measures to protect from environmental hazards should be commensurate with the importance of the buildings and the criticality of the operations or ICT systems located in these buildings.

4.7.12 *ICT operations security* Licence Holders should implement procedures to prevent occurrence of security issues in Technology Arrangements and should respectively minimise their impact on ICT service delivery. These procedures should include the following measures:

a) Identify potential vulnerabilities which should be evaluated and remediated by ensuring software and firmware are up to date, including any software provided by Licence Holders to its internal and external users, by deploying critical security patches or by implementing compensating controls;

b) Secure configuration baselines should be implemented for all systems, whether physical or virtualised, applications, and end-user computing equipment. System hardening should occur before any new device or application is added to the Licence Holder's production environment using pre-configured hardened images. Secure configuration baselines should be updated following patch fixes or software revisions. Automated configuration assessment tools (e.g. CIS-CAT) can be used to scan system's compliance to specific configurations and report compliance over time, identifying inconsistencies and providing remediation steps;

c) Network segmentation, implementation of data loss prevention systems (refer to Section 8 3.8.2-3.8.4 under Title 3), and encryption of network traffic were necessary should be implemented;

d) Protection of endpoints including servers, workstations and mobile devices should be implemented. Licence Holders should evaluate whether an endpoint meets the security standards defined by the Licence Holder before it is granted access to the corporate network;

e) Licence Holders should ensure that mechanisms are in place to verify the integrity of software, firmware, and data. Cryptographic hash functions or digital signatures can be used for verification purposes. File integrity monitoring (FIM) tools should be used for automated, real-time detection of unauthorised security-relevant changes to software, files or databases e.g. to mitigate against zero-day malware attacks undetected through other means, unauthorised changes to established system configuration changes, or unauthorised elevation of information system privileges. FIM tools should be integrated with the Licence Holder's SIEM tool (refer to Section

8 3.8.1 under Title 3) for Defence-in-depth threat intelligence, and detection of advanced or sophisticated threats. FIM integration with SIEM supports the objectives of Section 6 4.6.26 and 4.7.14 below;

f) Encryption of data at rest and in transit (in accordance with the data classification).

4.7.13 Furthermore, on an ongoing basis, Licence Holders should determine whether changes in the existing operational environment influence the existing security measures or require adoption of additional measures to mitigate related risks appropriately. These changes should be part of the Licence Holder's formal change management process, which should ensure that changes are properly planned, tested, documented, authorised and deployed.

4.7.14 *Security monitoring* Licence Holders should establish and implement policies and procedures to detect anomalous activities that may impact the Licence Holder's information security, and to respond to these events appropriately. As part of this continuous monitoring, Licence Holders should implement appropriate and effective capabilities for detecting and reporting physical or logical intrusion as well as breaches of confidentiality, integrity and availability of the information assets. The continuous monitoring and detection process should cover:

a) Relevant internal and external factors, including business and ICT administrative functions;

b) Transactions to detect misuse of access by third parties or other entities and internal misuse of access; and

c) Potential internal and external threats.

4.7.15 As mentioned in Section 6 4.6.26, Licence Holders should establish and implement processes and organisation structures to identify and constantly monitor security threats and also identify security vulnerabilities that could be used as attack vectors thereby potentially affecting the Licence Holder's ability to provide services, or which could result in unauthorised access to systems and information assets. Licence Holders should actively monitor technological developments to ensure that they are aware of security risks. They should also implement detective measures, for instance to identify possible information leakages, malicious code and other security threats, and known vulnerabilities for software and hardware, and check for corresponding new security updates.

4.7.16 The security monitoring process should also help Licence Holders to understand the nature of security incidents, to identify trends and to support the organisation's internal investigations.

4.7.17 A range of technologies (refer to Section 8 3.8.1-3.8.3 under Title 3) can be used to collect, manage and evaluate security data against multiple sources of security intelligence on a continuous basis, enabling Licence Holders to act on new information, security events and vulnerabilities in order to remediate and minimise the window of opportunity for attackers to exploit attack vectors. Continuous threat and vulnerability monitoring should be considered a first line of defence activity. ICT specialists at the first line of defence should establish actions and activities in relation to newly discovered risk vectors and their mitigation, with a priority that is proportionate to the severity of such risk vectors.

4.7.18 *Information security reviews, assessment and testing*

Licence Holders should perform a variety of different information security reviews, assessments and testing, to ensure effective identification of vulnerabilities in their Technology Arrangements. Specifically, Licence Holders may perform gap analyses against information security standards such as ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27017, compliance reviews, internal and external audits of the information systems, or physical security reviews. Furthermore, Licence Holders should consider good practices such as source code reviews (see 4.9.8), vulnerability assessments, penetration testing, and red team exercises[53]. Taking into consideration the principle of proportionality and a risk-based approach, the Authority may use its supervisory powers to carry out thematic reviews on Licence Holders' to assess their cyber defence capability. If deemed necessary, the Authority may engage with specific Licence Holders to carry out threat-led penetration testing (TLPT) through a formal process via an authorised red team in order to stress test the cyber-operational resilience of such Licence Holders.

4.7.19 Licence Holders should establish and implement an information security testing framework that validates their cybersecurity posture and ensure that this framework considers identified threats and vulnerabilities, identified through threat monitoring and the ICT risk assessment process.

4.7.20 The information security testing framework should ensure that tests:

a) are carried out by independent testers with sufficient knowledge, skills and expertise, e.g., holding certification in information security assessment (typically CREST CCSAS and CCSAM are preferred, with OSCP being the certification of choice for new starters in this field of work), in testing information security measures and not involved in the development of the information security measures; and
b) include vulnerability scans and penetration tests (including threat led penetration testing where necessary and appropriate) adequate to the level of risk identified with the business processes and systems.

4.7.21 Licence Holders should ensure that tests of security measures are conducted in the event of changes to Technology Arrangements, processes or procedures and if changes are made because of major

[53] The ESAs in Joint Advice of the European Supervisory Authority JC 2019 25, dated 10 April 2019, is considering a multi-staged approach to building a coherent cyber resilience testing framework across the EU based on TLPT testing given significant differences within financial sectors in terms of cyber maturity.

operational or security incidents or due to the release of new or significantly changed internet-facing critical applications.

4.7.22 Licence Holders should monitor and evaluate the results of the security tests, in order to update their security measures accordingly as necessary without undue delay in case of critical ICT systems.

4.7.23 Licence Holders should perform ongoing and repeated tests of the security measures. Without prejudice to all applicable Acts, Regulations, rules or sector-specific guidelines, as well as clause 4.7.23, for all critical ICT systems (as determined in 4.6.16), vulnerability assessments and penetration testing shall be performed by an independent party at least on an annual basis. Non-critical systems should be tested regularly on a risk-based approach, but at least every three years instead of annually provided:

a) such systems are fully in scope of the processes and procedures covered under 4.7.9 to 4.7.17;
b) such non-critical systems are logically isolated from critical systems and there is no interdependence or information exchange between any of the non-critical systems and critical systems.

4.7.24 The following infrastructure and systems should be considered critical for the purpose of vulnerability assessments and penetration testing:

- The Licence Holder's network at OSI Layers 2 and 3 and any virtualised network infrastructure in the cloud;
- Staging platforms for critical systems;
- All online systems used for technical operations, maintenance and infrastructure management, including SIEM and Cyber AI tools, DevOps tools, backup infrastructure, and online environmental control systems (access control and intruder alarm systems, power, cooling, fire suppression).

4.7.25 Cyber resilience testing covers a wide variety of tools and actions, ranging from a basic level of security testing to threat intelligence led penetration testing (TLPT). The level, breadth and depth of such testing should take into account the Licence Holder's size, internal organisation, the nature scope and complexity and riskiness of the services and products that it provides or intends to provide[54]. Licence Holders and prospective applicants are advised to consult with the Authority to ensure that cyber resilience testing meets supervisory expectations based on the Licence Holder's risk profile.

4.7.26 In the case of Payment Service Providers (PSPs), the testing framework should also encompass the security measures relevant to

a) payment terminals and devices used for the provision of payment services;

[54] Joint Advice on the costs and benefits of developing a coherent cyber resilience testing framework for significant market participants and infrastructures (10 April 2019)

b) payment terminals and devices used for authenticating the Payment Service User (PSU); and

c) devices and software provided by the PSP to the PSU to generate/receive an authentication code.

4.7.27 Based on the security threats observed and the changes made, testing should be performed to incorporate scenarios of relevant and known potential attacks.

4.7.28 Technology Arrangements may include sub-systems which are based on a shared responsibility cloud service model (refer to Section 4 under Title 3), for example SaaS. Penetration testing on such sub-systems by Licence Holders, or by third parties engaged by Licence Holders, should only be carried out on such sub-systems in agreement with the cloud service provider. The cloud provider's terms of service may prohibit such testing, particularly because the exercise can impact the service provided to other tenants. In such cases Licence Holders can rely on presentation of recent SOC 2 Type II reports (see Section 5 5.11.18 under Title 5) or similar for security and control effectiveness assurance purposes.

4.7.29
Information security training and awareness

The importance of ongoing training and cybersecurity awareness cannot be stressed enough. Licence Holders should establish a training programme, including periodic security awareness programmes, for all staff and contractors to ensure that they are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures to reduce human error, theft, fraud, misuse or loss and trained to address information security-related risks. Licence Holders should ensure that the training programme provides training for all staff members and contractors at least annually. Records of trainings carried out including evidence of attendance should be kept.

4.7.30 Licence Holders should ensure that staff members occupying key roles receive targeted information security training at least annually.

4.7.31 Licence Holders should establish and implement periodic security awareness programmes to educate their staff, including the Management Body, on how to address information security risks.

Section 8 ICT operations management

4.8.1 Licence Holders should manage their ICT operations based on documented and implemented processes and procedures (which, for PSPs, include the security policy document in accordance with Article 5(1)(j) of PSD2) that are approved by the Management Body. This set of documents should define how Licence Holders operate, monitor and control Technology Arrangements, including documenting critical ICT operations and should enable Licence Holders to maintain an up-to-date asset inventory.

4.8.2 Licence Holders should maintain and improve, when possible, the efficiency of their ICT operations, including but not limited to the need to consider how to minimise potential errors arising from the execution of manual tasks. Licence Holders should ensure that the performance of their ICT operations is aligned with the business requirements. Without prejudice to Principles 1 and 2 under Title 2, Licence Holders should use the Information Technology Infrastructure Library (ITIL) framework, or similar standards and frameworks, for effective, service level target-driven, IT service management.

4.8.3 Licence Holders should implement logging and monitoring procedures for critical ICT operations to allow for detection, analysis and correction of technical faults and errors.

4.8.4 Licence Holders should maintain an updated inventory of their ICT assets (including IT systems, network devices, database etc., whether implemented on premises or in the cloud, and whether owned or leased). The ICT asset inventory should store the configuration of the ICT assets and the links and interdependencies between the different ICT assets making up the Technology Arrangements, to enable a proper configuration and change management process.

4.8.5 The ICT asset inventory should be sufficiently detailed to enable the prompt identification of an IT asset, its location, security classification, IP address(es), and ownership. Interdependencies between assets should be documented to help in the response to security and operational incidents, including cyber-attacks.

4.8.6 Licence Holders should monitor and manage the life cycle of ICT assets to ensure that they continue to meet and support business and risk management requirements. Licence Holders should ensure that the ICT assets are supported by their external and internal vendors and developers, as necessary, and that all relevant patches and upgrades are applied based on a documented process. The risks stemming from outdated or unsupported ICT assets should be assessed and mitigated. Decommissioned ICT Assets should be safely processed and disposed of.

4.8.7 Licence Holders should implement performance and capacity planning and monitoring processes to prevent, detect and respond to important performance issues of ICT systems and ICT capacity shortages in a timely manner such that sustained breach of performance service levels is avoided.

4.8.8 Licence Holders should define and implement data and ICT systems backup and restoration procedures to ensure that they can be recovered as required. The scope and frequency of backups should be set in line with business recovery requirements and the criticality of the data and the ICT systems, assessed according to the performed risk assessment. Testing of the backup and restoration procedures, including ensuring that the procedures are in line with the information security policy, should be undertaken on a periodic basis.

4.8.9 Licence Holders should ensure that data and ICT systems backups are stored in one or more locations out of the Licence Holder's primary site for ICT operations – whether on premises and/or cloud. Offsite storage, whether online or offline, should be stored securely and is sufficiently remote from the primary site so they are not exposed to the same risks. Licence Holders should also consider virtual machine snapshots to different regions from cloud-based production environment.

4.8.10 *ICT incident and problem management*

Licence Holders should establish and implement an incident and problem management process to monitor and log operational and security ICT incidents, and to enable them to continue or resume business functions and processes in a timely manner, when disruptions occur. Licence Holders should determine appropriate criteria and thresholds for classifying an event as an operational or security incident, as set out in the 'Definitions' section under Title 1, as well as early warning indicators that should serve as an alert to enable early detection of these incidents.

4.8.11 To minimise the impact of adverse events and enable timely recovery, Licence Holders should establish appropriate processes and organisation structures to ensure the consistent and integrated monitoring, handling and follow-up of operational and security incidents to ensure that the root causes are identified and eliminated preventing the occurrence of repeated incidents. The incident and problem management process should establish:

a) The procedures to identify, track, log, categorise and classify incidents according to a priority based on business criticality;
b) The roles and responsibilities for different incident scenarios (errors, malfunctioning systems, cyber-attacks);
c) A problem management procedure to identify, analyse and solve the root cause behind one or more incidents – Licence Holders should analyse operational or security incidents likely to affect them that have been identified or have occurred within and/or outside the organisation. Licence Holders should consider key lessons learned from these analyses and update operational processes and procedures and/or security measures accordingly;
d) Effective internal communication plans, including incident notification and escalation procedures – covering also security-related customer complaints – to ensure that:
    i. Incidents with a potentially high adverse impact on critical ICT systems and ICT services are reported to the firm's most senior management team and the ICT senior management;
    ii. The Management Body is informed on an ad-hoc basis in case of significant incidents and at least, informed of the impact, reaction and additional controls defined because of the incidents.

e) An incident response procedure to mitigate the impacts related to the incidents and to ensure that the impacted service(s) become operational in a timely manner, within established service level targets and Recovery Time Objectives (RTO) / Recovery Point Objectives (RPO), and that cyber threat neutralisation and recovery is effective and secure.

f) Specific internal and external communication plans for critical business functions and processes;

   i. To collaborate with relevant internal and external stakeholders to effectively respond to and recover from the incident;

   ii. To provide timely information to external parties (e.g. customers, other market participants, the Authority and other competent authorities) where applicable, as appropriate and in line with applicable regulation.

Without prejudice to any incident reporting obligations within the relevant Acts, Regulations, rules or sector-specific guidelines, Licence Holders are expected to report major ICT-related incidents to the Authority without undue delay.

Section 9 ICT Project and Change Management

4.9.1 *ICT project management*

Licence Holders should implement a programme and/or project governance process that defines roles, responsibilities and accountabilities to effectively support the implementation of the ICT strategy.

4.9.2

Licence Holders should appropriately monitor and mitigate risks deriving from the portfolio of ICT projects, considering also risks that may result from interdependencies between different projects and from dependencies of multiple projects on the same resources and/or expertise.

4.9.3 *Project portfolio management*

Subject to the Principle of Proportionality, Licence Holders should establish and implement an ICT projects portfolio management (also known as programme management) framework, which at a minimum, defines the organisation's approach to:

a) Programme Management i.e. structure, roles and responsibilities e.g. through a Project Management Office (PMO);

b) Projects pipeline management and change control;

c) Project management methodology;

d) Resource management;

e) Risk management taking into consideration the project management methodology;

f) Programme reporting, performance metrics, dashboards, update frequencies and escalation policy;

g) Post-project lessons learnt.

Licence Holders should establish and implement an ICT project management policy that includes as a minimum:

a) project objectives;
b) roles and responsibilities;
c) a project risk assessment;
d) a project plan, timeframe and steps;
e) key milestones;
f) change management requirements,

and ensures that information security requirements are analysed and approved by a function that is independent from the development function.

Licence Holders should ensure that all areas impacted by an ICT project are represented in the project team and that the project team has the knowledge required to ensure secure and successful project implementation.

4.9.4 With reference to 4.9.3 (f), the establishment and progress of ICT projects and their associated risks should be reported to Senior Management, and the Management Body depending on the importance and size of the ICT projects, regularly and on an ad hoc basis, individually or aggregated, as appropriate. The Licence Holder's overall risk management framework should include project risk oversight.

4.9.5 Under the principle of proportionality and a principles-based approach, the Authority does not recommend one project management methodology over another. Licence Holders should pursue a Waterfall approach or an Agile methodology that fits their scale, complexity, and nature of their business, provided that:

a) The firm can systematically achieve the desired outcomes of the ICT strategy in line with the business strategy through the defined portfolio of projects within the time frames and budget set in the strategy, and within the risk appetite for ICT risks in accordance with the risk appetite of the Licence Holder;
b) Information security requirements are analysed and approved, and vulnerabilities assessed and mitigated before putting code into production, by a function that is independent from the development team;
c) Procurement management policies should be defined, based on best practices of the adopted project management methodology, and taking into consideration the guidelines under Title 5 in relation to outsourcing;
d) Agile, incremental or iterative implementations of product development remain fully compliant with all applicable Acts, Regulations, rules or sector-specific guidelines and/or technical standards, supervisory reporting requirements and guidelines at all times;
e) All roles and responsibilities of project team members, project managers, scrum masters, project or product owner, and other

involved stakeholders, depending on the methodology used and specific projects, are defined and documented;

f) All stakeholders or functional areas impacted by an ICT project are involved in the project through representatives or team members as required that have adequate knowledge and sufficient delegation of authority to ensure secure and successful achievement of the project implementation.

4.9.6
ICT systems acquisition and development

Licence Holders should develop and implement a process governing the acquisition, development and maintenance of ICT systems in order to ensure the confidentiality, integrity, availability of the data to be processed are comprehensibly assured and the defined protection requirements are met. This process should be designed using a risk-based approach.

4.9.7

Where bespoke software development or software customisation is involved, whether developed in-house or externally by a third party, Licence Holders should ensure that it follows a process designed using a risk-based approach. The following may be considered:

a) Software Development Life Cycle (SDLC). Not all SDLCs address software security in detail. ISO/IEC 27034 provides comprehensive security processes and activities that can be integrated into any SDLC. Licence Holders can also be guided by NIST's Secure Software Development Framework (SSDF)[55] (currently a white paper draft). Adoption of Secure SDLC frameworks (S-SDLC) such as OWASP SAMM, Microsoft SDL or PCI Secure SLC provide an effective and measurable way for Licence Holders to analyse their software security posture;

b) Payment Application Data Security Standard (PA DSS), technical implementation in terms of computer programming based on general software security principles, coding practices and standards such as OWASP and SEI CERT;

c) Quality assurance, testing, approval and release into production carried out according to best practice or standards.

With respect to 4.9.7 (a), without prejudice to sector-specific compliance requirements, and irrespective of the adopted SDLC model, baseline[56] non-functional requirements should be made known to the development team at the outset even where an iterative or incremental development approach is involved.

4.9.8
Software Security Assurance

With respect to 4.9.7 (c), in order to find critical defects and security weaknesses in code while it is written, secure code review must be an integral part of code verification along the SDLC, irrespective of whether software development is carried out in-house or outsourced. Proprietary source code should be run through a Static Application

[55] NIST "Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF) – June 11, 2019

[56] Baseline in this context refers to those non-functional requirements that apply across the entire solution, for example, information security requirements in-line with the information security policy to ensure that the software is secure-by-design.

Security Testing (SAST) tool as part of source code review, ideally every time code is checked in the version control system used by the developers. Software Composition Analysis (SCA) should also be used throughout the SDLC where open source components are used in the code base.

4.9.9 The complexity of software projects is continuously increasing. The use of Black Box and White Box testing should be aligned to the development methodology and context-specific circumstances. Where an Agile methodology is involved, quality assurance must be part of the day to day development and Licence Holders should ensure that testing is carried out at each iteration, with tests and analysts/business owners working very closely with the developers to ensure continuous feedback, using a defined Agile testing methodology such as Test-Driven Development (TDD), Acceptance Test-Driven Development (ATDD) or Behaviour-Driven Development (BDD). Without prejudice to all applicable Acts, Regulations, rules or sector-specific guidelines, as well as, the principle of proportionality, Licence Holders should also consider using of the set of international software testing standards under ISO/IEC 29119.

4.9.10 The use of automated testing software in conjunction with manual testing for Black Box testing is encouraged to maximise risk coverage, faster time-to-market and efficiency.

4.9.11 Without prejudice to a principles-based outcome, as well as sector-specific Acts, Regulations, rules or sector-specific guidelines, Licence Holders should attain OWASP 4.0 Verification Level 3 (Advanced) from an independent third-party for any software application that enables a critical or important business function or service involving personal, financial data or transactional data, or where a Licence Holder's operation could be jeopardised. ASVS 4.0 Level 2 (Standard) should be considered sufficient for any other use where the application processes or contains personal or business confidential information.

4.9.12 *Continuous Integration, Continuous Delivery, Continuous Deployment*

Cutting edge software engineering in agile methodologies combined with modern IT operations nowadays enables much shorter and more frequent development life cycles. While the benefits are evident, Licence Holders need to consider CI-CD (a combined practice of Continuous Integration and Continuous Delivery and/or Continuous Deployment) as part of their risk-based approach to ICT strategy execution. ASVS 4.0 caters for CI-CD environments and cloud deployments including serverless architectures if implemented and followed rigorously when end-to-end control of the full SDLC is possible e.g. in-house development. When considering integrating PaaS and SaaS components operating under a CI-CD deployment model by third-party providers in Technology Arrangements that serve critical or important business functions or services, Licence Holders should, however, consider carefully if the level of software quality assurance, especially software security assurance, that can be met and sustained by the service provider, is within the Licence Holder's risk appetite in accordance with the risk appetite of the organisation. Where a CI-CD deployment model of a relatively small third-party service component out of the overall Technology Arrangement is tolerated, Licence Holders should, nevertheless, have processes in place to follow closely and assess the impact of the service provider's product roadmap as well as their incident notification procedure.

4.9.13 Licence Holders, in general, should implement logically separate ICT environments to ensure adequate segregation of duties and to mitigate the impact of unverified and unvalidated changes to production systems. Specifically, Licence Holders should ensure segregation of production environments from development, testing and other non-production environments.

4.9.14 When applicable, regression testing should be performed to ensure that new code deployed as a change requirement, a new feature, or to fix a defect, security or performance issue, does not break or alter other existing features or behaviours within a Technology Arrangement. Such testing involves the re-execution of some or all previously executed test cases in a prior deployment. The staging or testing environment for such tests should adequately reflect the production environment so that the behaviour of the ICT systems in the production environment can be predicted and sufficiently tested.

4.9.15 All functional and non-functional requirements, as well as their corresponding test cases, should be clearly defined and approved by the relevant business owner and ICT management.

4.9.16 Licence Holders should ensure that measures are in place to mitigate the risk of unintentional alteration or intentional manipulation of the ICT systems during development and implementation in the production environment.

4.9.17 Licence Holders should implement measures to protect the integrity of source code of ICT systems that is developed in-house. They should also document the development, implementation, operation, and/or configuration of the ICT systems in a sufficiently comprehensive manner to reduce unnecessary dependency on subject matter experts. The documentation of ICT systems should contain, where applicable, at least user documentation, technical system documentation and operational procedures as applicable.

4.9.18 *Business managed application software*

Business managed applications or end user computing applications, such as spreadsheet or desktop database software, may end up being used by business functions to fill gaps in critical or important business processes that are not addressed by enterprise application software within a Technology Arrangement. The use of such business managed applications is generally seen as an ICT and their use should be minimised through improved ICT project pipeline and demand management and ICT strategy refreshes.

4.9.19 Where development or use of ICT systems managed by business function's end users outside the ICT organisation as a stop gap measure is unavoidable, Licence Holders should ensure that such development is carried out according to established processes for acquisition and development of ICT systems, governance frameworks, and in full conformance with all applicable Acts, Regulations, rules or sector-specific guidelines. Licence Holders should maintain a register of such applications that support critical or important business functions or processes and should have concrete plans in place to provide alternative robust solutions to reduce such risks.

4.9.20 *Robotic Process Automation (RPA) and Workflow Automation tools.*

Deployed as enterprise tools according to, and within, the Licence Holder's ICT governance and risk management frameworks, Robotic Process Automation (RPA) systems, as well as modern graphical workflow automation software, offer significant potential to reduce time-consuming, repetitive manual processes, streamline business processes, and in certain cases can also be used as an alternative to traditional systems integration. Licence Holders should, however, consider the risks involved in empowering end users, even if limited to 'power users'[57] within business functions, with rights and system privileges to implement automation activities and business workflows without effective controls in place to ensure ICT governance, effectiveness of the Licence Holder's risk management framework including information security policy. Licence Holders should therefore not extend elevated rights to end users to create and modify automation and workflow activities and tasks respectively unless suitable controls and proper change management can be ensured.

4.9.21 *Shadow IT*

Shadow IT, or the use of hardware or software by an employee or business functions without the knowledge of ICT operations and security teams within the organisation, has grown because of the proliferation of cloud services, particularly SaaS. While the end user or departmental intent for resorting to shadow IT may be driven by legitimate business needs to fill gaps in Technology Arrangements or unaddressed requirements, the risks involved across all ICT risk categories can be material. While containment strategies for on premises shadow IT are mature and generally achievable through the use of readily available enterprise features in operating systems that allow ICT operations teams to control the working environment of named user and computer accounts, Licence Holders may need to address gaps in their ICT controls by investing in Cloud Access Security Brokers (CASBs) as mentioned in Section 8 under Title 3 to address SaaS abuse.

4.9.22 *ICT change management*

Without prejudice to authorised risk appetite towards appropriately controlled third-party services provided under a CI-CD model in an overall Technology Arrangement (see 4.9.12), Licence Holders should establish and implement an ICT change management process to ensure that all changes to ICT systems are recorded, assessed, tested,

[57] A user within a non-ICT related business function, who uses advanced features in software applications.

approved, implemented, and verified in a controlled manner. Licence Holders should handle the changes during emergencies (i.e. changes that must be introduced as soon as possible) following procedures that provide adequate safeguards.

4.9.23 Licence holders should determine whether changes in the existing operational environment influence the existing security measures or require adoption of additional measures to mitigate the risk involved. These changes should be part of the Licence Holder's formal change management process, which should ensure that changes are properly planned, testing, documented and authorised.

Section 10 Business continuity management

4.10.1 Licence Holders should have business continuity arrangements as part of their operational risk management framework, in accordance with all applicable Acts, Regulations, rules or sector-specific guidelines, and having regard to the nature, scale and complexity of their business. As part of sound business continuity management, Licence Holders should conduct business impact analysis (BIA) by analysing their exposure to severe business disruptions and assessing their potential impacts (including on confidentiality, integrity and availability), quantitatively and qualitatively, using internal and/or external data (e.g. third party provider data relevant to a business process or publicly available data that may be relevant to the BIA) and scenario analysis. The BIA should also consider the criticality of the identified and classified business functions, supporting processes, third parties and information assets, and their interdependencies. BIAs should result in Business Continuity Plans (BCPs) based on a range of plausible risk scenarios, including extreme ones such as major cyber-attacks or a systemic failure of a cloud service provider upon which critical or important Licence Holder functions depend. BCPs should be documented and approved by the Management Body.

4.10.2 Licence Holders should ensure that ICT systems and services, and their interdependencies within their Technology Arrangements are aligned with the BIA and designed for a level of operational resilience commensurate with the critically of the business functions they serve, as identified and classified in accordance with Section 6 4.6.14-4.6.15 under Title 4.

Licence Holders should put BCPs in place to ensure that they can react appropriately to potential failure and cyber-attack scenarios and that they are able to recover the operations of their critical business activities after disruptions within a recovery time objective (RTO, the maximum time within which a system or process must be restored after an incident) and a recovery point objective (RPO, the maximum time period during which it is acceptable for data to be lost in the event of an incident). In cases of severe business disruption that trigger specific business continuity plans, Licence Holders should prioritise business continuity actions using risk-based approach, which can be based on risk assessments carried out.

4.10.3
Disaster response and recovery plans

Licence Holders should ensure that the broader set of BCPs with the organisation's operational risk management framework include Technology Disaster Response and Recovery (DR) plans that:

a) specify what conditions may prompt activation of a DR plan to ensure the availability, continuity and recovery of, at least, critical ICT systems and ICT services identified in accordance with Section 6 of Title 4;
b) specify what actions should be taken to ensure recovery of systems, applications and data in Technology Arrangements within established Recovery Time Objectives and Recovery Point Objectives following a disruption that triggers a specific BCP, while safeguarding information security. Licence Holders should prioritise DR actions using a risk-based approach, taking into consideration:
    i. the importance of recovering operations of critical business functions, supporting processes, information assets and their interdependence (including potential adverse effects on the financial system if applicable);
    ii. breach or imminent breach of personally identifiable information and financial data;
    iii. Resuming financial transaction processing, including execution of pending transactions, if applicable, according to relevant Acts, Regulations, rules or sector-specific guidelines;
    iv. short-term (stopgap) versus long-term recovery options, taking into consideration i-iii above as well as the collection of forensically sound digital evidence (see Section 8 3.8.5 under Title 3) if relevant to the incident;
c) Consider alternative options where recovery may not be feasible in the short-term because of costs, risks, logistics, or unforeseen circumstances.

4.10.4

Licence Holders should ensure that DR plans are documented and made available to the business and support units, and readily accessible in case of an emergency. Licence Holders should also have contingency plans in case the documented response and recovery plans might not be electronically accessible as a result of an incident.

4.10.5
Testing of DR plans

Licence Holders should test their BCPs, and ensure that the operation of their critical business processes and activities, business functions, roles and assets (e.g. information assets) and ICT assets and their interdependencies (including those provided by service providers) are tested regularly based on the Licence Holders' risk profile. Without prejudice to all applicable Acts, Regulations, rules or sector specific guidelines, regarding business continuity, Licence Holders should test their BCPs at least annually.

Licence Holders' testing of their BCPs should demonstrate that they are capable of sustaining the viability of the business until critical operations are re-established at a predefined service level or impact tolerance.

Tests should include, but not be limited to:

a) switching operations to, and back from, secondary infrastructure at the Licence Holder's remote DR site or a cloud-based DR service as applicable depending on the Licence Holder's Technology Arrangement architecture;

b) challenging the assumptions on which the DR plans are based, including governance arrangements and crisis communications plans;

c) verifying the ability of the Licence Holder's staff, and third parties where outsourced services are involved, to respond adequately to the scenarios under test.

Test results should be documented and any identified deficiencies resulting from the tests should be analysed, addressed and reported to the Management Body.

4.10.6 *Updating DR plans*

BCPs should be updated regularly, based on testing results, current threat intelligence and lessons learned from previous events. Any relevant changes in recovery objectives (including RTO and RPO) and/or changes in business processes and activities, business functions, roles and assets (e.g. information assets and ICT assets, should also be included.

4.10.7 *Crisis communications*

In the event of a disruption or emergency, and during the implementation of the BCPs, Licence Holders should ensure that they have effective crisis communications measures in place so that all relevant internal and external stakeholders, including the Authority and other competent authorities as applicable, and also external service providers, are informed in a timely and appropriate manner.

Title 5 Outsourcing Arrangements

Section 1 Subject matter and scope

5.1.1 Clauses under Title 5 specify the internal governance arrangements, including sound risk management, that Licence Holders should implement when they outsource functions, in particular the outsourcing of critical or important functions, in a Technology Arrangement or an outsourced business function or process that is delivered as a Cloud Service (e.g. BPaaS).

5.1.2 Without prejudice to clauses 1.1.8, 1.1.9 and 1.1.10 under Title 1 and 2.1.1, 2.1.2 under Title 2, the guidance provided under Title 5 draws on good practices and requirements set out in guidelines EBA/GL/2019/02 and EIOPA-BoS-19/270, so as to define the Authority's cross-sectoral baseline expectations related to outsourcing arrangements within the scope defined in 5.1.1 under Title 5.

Section 2 Implementation and application

5.2.1 These guidelines under Title 5 set out the Authority's expectations with regard to Outsourcing Arrangements.

5.2.2 These outsourcing guidelines should also apply on a sub-consolidated and consolidated basis, taking into account the prudential scope of consolidation and applicable Acts, Regulations, rules or sector-specific guidelines. For this purpose, parent entities should ensure that internal governance arrangements, processes and mechanisms in their subsidiaries, are consistent, well integrated and adequate for the effective application of these guidelines at all relevant levels.

5.2.3 Licence Holders, in accordance with 5.2.2, and institutions that are members of an institutional protection scheme and that use centrally provided governance arrangements, should comply with the following, provided no waiver has been granted by the Authority in accordance with applicable legislation:

a) where Licence Holders have outsourcing arrangements with service providers within the group, the Management Body of those Licence Holders retains, also for these outsourcing arrangements, full responsibility for compliance with all regulatory requirements and the effective application of these guidelines;

b) where Licence Holders outsource the operational tasks of internal control functions to a service provider within the group, for the monitoring and auditing of outsourcing arrangements, Licence Holders should ensure that, also for these outsourcing arrangements, those operational tasks are effectively performed, including the receiving of appropriate reports;

c) where operational monitoring of outsourcing is centralised (e.g. as part of a master agreement for the monitoring of outsourcing arrangements) with a central body or service provider within the group, Licence Holders should ensure that, at least for outsourced critical or important functions, both independent monitoring of the service provider and appropriate oversight by each Licence Holder is possible, including by receiving, at least annually and upon request from the centralised monitoring function reports that include, at least, a summary of the risk assessment and performance monitoring. In addition, Licence Holders should receive a summary of the relevant audit reports for critical or important outsourcing, and upon request, the full audit report;

d) Licence Holders should ensure that their Management Body will be duly informed of relevant planned changes regarding service providers that are monitored centrally and the potential impact of these changes on the critical or important functions provided, including a summary of the risk analysis, including legal risks, compliance with regulatory requirements and the impact on service levels, in order for them to assess the impact of these changes;

e) where the register of all existing outsourcing arrangements, as referred to in 5.9.1, is established and maintained centrally within a group or institutional protection scheme, the Authority and Licence Holder should be able to obtain the Licence Holder's individual register without undue delay. This register should include all outsourcing arrangements, including outsourcing arrangements with service providers inside that group or institutional protections scheme;

f) where a Licence Holder relies on an exit plan for a critical or important function that has been established at group level, within the institutional protections scheme or by the central body, Licence Holders should receive a summary of the plan and be satisfied that the plan can be effectively executed.

5.2.4 The provisions of these guidelines should be applied by the parent entity and its subsidiaries or by the central body and its affiliates, where waivers have been granted by the Authority to that effect. Licences Holders that are subsidiaries of parent firms in a Member State to which no waivers have been granted should comply with these guidelines on an individual basis.

Section 3 Assessment of outsourcing arrangements

5.3.1 Licence Holders should establish whether an arrangement with a third party falls under the definition of outsourcing. Within this assessment, consideration should be given to whether the outsourced function (or part thereof) is performed on a recurrent or an ongoing basis and whether this function (or part thereof) would normally fall within the scope of functions that would, or could, realistically be performed by

Licence Holders, even if the Licence Holder has not performed this function in the past.

5.3.2 Where an arrangement with a service provider covers multiple functions, Licence Holders should consider all aspects of the arrangements within their assessment, e.g. if the service provided includes the provision of data storage infrastructure and the backup of data, both aspects should be considered together.

5.3.3 The Licence Holder should determine the nature, scale and complexity of arrangements with third parties, taking into consideration the principle of proportionality and materiality of the function outsourced, irrespective of whether those third parties are cloud service providers or not.

5.3.4 As a general principle, Licence Holders should not consider the following as outsourcing:

a) a function that is legally required to be performed by a service provider, e.g. statutory audit;

b) market information services (e.g. provision of data by Bloomberg, Moody's, Standard & Poor's, Fitch);

c) global network infrastructures (e.g. Visa, Mastercard);

d) global financial messaging infrastructures that are subject to oversight by relevant authorities;

e) the acquisition of services that would otherwise not be undertaken by the Licence Holder (e.g. support and maintenance of the cooling system in a Licence Holder's data centre, and utilities such as electricity and telephony).

5.3.5 Licence Holders should always consider a function as critical or important, in the following situations:

a) where a defect or failure in its performance would materially impair their continuing compliance with the conditions of their authorisation by the Authority under all legal or regulatory obligations, Licence Holders are subject to in the sector(s) they operate in[58] and including all legal and regulatory obligations whose supervisory oversight is carried out by other competent authorities e.g. Regulation (EU) 2016/679 (EU GDPR);

b) where a defect or failure in its performance would materially impair their financial performance, or the soundness or continuity of their financial services and activities;

c) when operational tasks of internal control functions are outsourced (e.g. managed cybersecurity service for small and medium-sized businesses), unless the assessment establishes that a failure to provide the outsourced function or the inappropriate provision of the outsourced

[58] For example, Directive 2013/36/EU, Regulation (EU) No 575/2013, Directive 2014/65/EU, Directive (EU) 2015/2366, Directive 2009/110/EC, Directive (EU) 2009/138/EC and their regulatory obligations.

function would not have an adverse impact on the effectiveness of the internal control function;

d) when they intend to outsource a business function to an extent that would require authorisation by the Authority (e.g. a critical or important function implemented as BPaaS);

e) functions that are necessary to perform activities of core business considered to be critical or important, unless failure to provide the outsourced function or the inappropriate provision of the outsourcing function would not have an adverse impact on the operational continuity of the core business function.

5.3.6 When assessing whether an outsourcing arrangement relates to a function that is critical or important, Licence Holders should consider, together with the outcome of the risk assessment outlined in 5.10.4 to 5.10.8, at least the following factors:

a) whether the outsourcing arrangement is directly connected to the provision of the financial services for which they are authorised;

b) the potential impact of any disruption to the outsourced function or failure of the service provider to provide the service at the agreed service levels on a continuous basis, depending on the service provider's:

   i. Short- and long-term financial resilience and viability, including, if applicable, its assets, capital, costs, funding, liquidity, profits and losses;

   ii. Business continuity and operational resilience;

   iii. Operational risk, including conduct, information and communication technology (ICT) and legal risks;

   iv. Reputational risks and strategic risks;

   v. Where applicable, recovery and resolution planning, resolvability and operation continuity in an early intervention, recovery or resolution situation;

c) The potential impact of the outsourcing arrangements on the service provider's ability to:

   i. Identify, monitor and manage all risks;

   ii. Comply with all legal and regulatory requirements;

   iii. Conduct appropriate audits regarding the outsourced function;

d) The potential impact of the services provided to its clients;

e) All outsourcing arrangements, that is, the Licence Holder's aggregated exposure to the same service provider and the potential cumulative impact of outsourcing arrangements in the same business area;

f) The size and complexity of any business affected;

g) The cost of the outsourcing activity as a proportion of total operating and ICT costs of the authorised firm;

h) The possibility that the proposed outsourcing arrangement might be scaled up without replacing or revising the underlying agreement;

i) The ability to transfer the proposed outsourcing arrangements to another service provider, if necessary or desirable, both contractually and in practice, including the estimated risks, impediments to business continuity, costs and time frame for doing so ('substitutability');

j) The ability to reintegrate (in-source) the outsourced function into the Licence Holder's operation, if necessary or desirable;

k) The protection of data and the potential impact of a confidentiality breach or failure to ensure data availability and integrity on the Licence Holder and its clients, including but not limited to compliance with Regulation (EU) 2016/679 (GDPR).

Section 4 Governance framework – sound governance arrangements

5.4.1 Risks caused by arrangements with third parties should fall under the Licence Holders' holistic risk management framework extending across all business lines and internal units. This should also enable Licence Holders to make well-informed decisions on risk-taking and ensure that risk management measures are appropriately implemented, including those related to cyber risks.

5.4.2 Licence Holders should identify, assess, monitor and manage all risks resulting from arrangements with third parties to which they are or might be exposed, including outsourcing arrangements. The risks, in particular the operational risks of all arrangements with third parties should be assessed as outlined in 5.10.4 to 5.10.8.

5.4.3 Licence Holders should ensure that outsourcing arrangements comply with all requirements under Regulation (EU) 2016/679.

5.4.4 Licence Holders which are also identified as Operators of Essential Services (OES) under Article 2 of L.N. 216 of 2018 "Measures for High Common Level of Security of Network and Information Systems Order, 2018", that transposes Directive (EU) 2016/1148 (NIS – Directive on security of network and information systems), should ensure that the outsourcing arrangements do not, in any way, reduce the Licence Holder's capabilities to meet the regulatory obligations as an OES.

5.4.5 Outsourcing arrangements cannot result in the delegation of the Management Body's responsibilities. Licence Holders shall remain fully responsible and accountable for complying with all their regulatory obligations, and should be able to oversee the outsourcing of critical or important functions, regardless of operational controls and responsibilities defined in a shared responsibility model in the deployment of cloud services (see Section 4 under Title 3 "Shared responsibilities for different cloud service models").

5.4.6 The decision to enter an outsourcing arrangement involving critical or important functions should be taken by the Licence Holder's Management Body. That decision should be based on a thorough risk assessment including all relevant risks implied by the arrangement such as IT and operational risks, business continuity risk, legal and compliance risk, concentration risk and, where applicable, risks associated to the data migration and/or the IT implementation phase.

5.4.7 The Management Body should always be fully responsible and accountable for at least:

a) Ensuring that the Licence Holder meets on an ongoing basis the conditions with which it must comply to remain authorised, including any conditions imposed by the Authority;

b) The internal organisation of the Licence Holder;

c) The identification, assessment and management of conflicts of interest;

d) The setting up of the Licence Holder's strategies and policies;

e) Overseeing the day-to-day management of the authorised firm, including the management of all risks associated with outsourcing; and

f) The oversight role of the Management Body in its supervisory function, including overseeing and monitoring management decision-making.

5.4.8 Outsourcing should not lower the suitability requirements applied to the members of an authorised entity's Management Body, directors or persons responsible for the management of the authorised firm and key function holders, including roles such as Chief Information Officer or Chief Information Security Officer, or their equivalent. Authorised firms should have adequate competence and sufficient and appropriately skilled resources to ensure appropriate management and oversight of outsourcing arrangements.

5.4.9 Licence Holders should:

a) Clearly assign the responsibilities for the documentation, management and control of outsourcing arrangements;

b) Allocate sufficient resources to ensure compliance with all legal and regulatory requirements, these guidelines, and the documentation and monitoring of all outsourcing arrangements.

5.4.10 Licence Holders should maintain at all times sufficient substance for the effective management of Technology Arrangements. To this end, they should:

a) Meet all the conditions of their authorisation at all times, including the Management Body effectively carrying out its responsibilities set out in 5.4.7;

b) Retain a clear and transparent organisational framework and structure that enables them to ensure compliance with legal and regulatory requirements;

c) Where operational tasks of internal control functions are outsourced (e.g. in the case of intragroup outsourcing), exercise appropriate oversight and be able to manage the risks that are generated by the outsourcing of critical or important functions; and

d) Have sufficient resources and capacities to ensure compliance with points (a) to (c).

5.4.11 When outsourcing, Licence Holders should at least ensure that:

a) They can take and implement decisions related to their business activities and critical or important functions, including those that have been outsourced;

b) They maintain the orderliness of the conduct of their business and the financial services they provide;

c) The risks related to current and planned outsourcing of Technology Arrangements are adequately identified, assessed, managed and mitigated;

d) Appropriate confidentiality arrangements are in place regarding data and other information;

e) An appropriate flow of relevant information with service providers is maintained;

f) With regards to the outsourcing of critical or important functions, they can undertake at least one of the following actions, within an appropriate time frame:

i. Transfer the function to alternative service providers;

ii. Reintegrate the function; or

iii. Discontinue the business activities that are depending on the function;

g) Where personal data are processed by service providers located in the EU and/or third countries, appropriate measures are implemented, and data are processed in accordance with Regulation (EU) 2016/679.

5.4.12 Licence Holders, where appropriate, should reflect the changes on their risk profile due to outsourcing arrangements within their own regulatory risk assessment framework.

5.4.13 The use of cloud services should be consistent with the Licence Holder’s strategies (e.g. IT strategy) and internal policies and processes which should be updated, if need be.

Section 5 Governance framework – outsourcing policy

5.5.1 The Management Body of a Licence Holder that has outsourcing arrangements in place or plans on entering into such arrangements should approve, regularly review and update a written outsourcing policy and ensure its implementation, as applicable, on an individual or group basis. The outsourcing policy should be in accordance with relevant sectoral guidelines on internal governance.

5.5.2 The policy should include the main phases of the life cycle of outsourcing arrangements and define the principles, roles and responsibilities, and processes in relation to outsourcing. In particular, the policy should cover at least:

a) The responsibilities of the Management Body (see 5.4.7), including its involvement in the decision-making on outsourcing of critical or important functions;

b) The involvement of business lines, IT function, internal control functions and other individuals in respect of outsourcing arrangements;

c) The planning of outsourcing arrangements, including:

i. The identification of business requirements regarding outsourcing arrangements;

ii. The criteria, including those referred in 5.3.1 to 5.3.6, and processes for identifying critical or important functions;

iii. Risk identification, assessment and management in accordance with 5.10.4 to 5.10.8;

iv. Due diligence checks on prospective service providers, including the measures required under 5.10.9 to 5.10.13;

v. Procedures for the identification, assessment management and mitigation of potential conflicts of interest, in accordance with 5.6.1 to 5.6.3 (Section 6);

vi. Business continuity planning in accordance with 5.7.1 and 5.7.2 (Section 7);

vii. The approval process of new outsourcing arrangements;

d) The implementation, monitoring and management of outsourcing arrangements, including:

i. The ongoing assessment of the service provider's performance in line with 5.12.1 to 5.12.6 (Section 12);

ii. The procedures for being notified and responding to changes to an outsourcing arrangement or service provider (e.g. to its financial position, organisational or ownership structures, sub-outsourcing);

iii. The independent review and audit of compliance with legal and regulatory requirements and policies;

iv. The renewal process;

e) The documentation and record-keeping, taking into account the requirements in 5.9.1 to 5.9.9 (Section 9);

f) Documented exit strategies and termination process, including a requirement for a documented exit plan for each critical or important function to be outsourced where such an exit is considered possible considering possible service disruptions or the unexpected termination of an outsourcing agreement.

5.5.3 The outsourcing policy should differentiate between the following:

a) Outsourcing of critical or important functions and other outsourcing arrangements;

b) Outsourcing to service providers that are authorised by a competent authority and those that are not;

c) Intragroup outsourcing arrangements, outsourcing arrangements within the same institutional protection scheme (where applicable, and including entities fully owned individually or collectively by institutions within the institutional protection scheme) and outsourcing to entities outside the group; and

d) Outsourcing to service providers located within a Member State and third countries.

5.5.4 Licence Holders should ensure that the policy covers the identification of the following potential effects of critical or important outsourcing arrangements and that these are taken into account in the decision-making process:

a) The Licence Holder's risk profile;

b) The ability to oversee the service provider and to manage the risks;

c) The business continuity measures; and

d) The performance of their business activities.

Section 6 Governance framework – conflicts of interest

5.6.1 Licence Holders should identify, assess and manage conflicts of interest regarding their outsourcing arrangements.

5.6.2 Where outsourcing creates a material conflict of interest, including between entities within a group or institutional protection scheme, Licence Holders need to take appropriate measures to manage those conflicts of interest.

5.6.3 When functions are provided by a service provider that is part of a group or a member of an institutional protection scheme, or that is owned by the Licence Holder, group or institutions that are members of an institutional protection scheme, the conditions, including financial conditions, for the outsourced service should be set at arm's length. However, within the pricing of services synergies resulting from providing the same or similar services to several Licence Holders with a group or an institutional protection scheme may be factored in, as long as the service provider remains viable on a stand-alone basis; with a group this should be irrespective of the failure of any other group entity.

Section 7 Governance framework – business continuity plans

5.7.1 Licence Holders should have in place, maintain and periodically test appropriate business continuity plans with regard to outsourced critical or important functions. Licence Holders within a group or institutional protection scheme may rely on centrally established business continuity plans regarding their outsourced functions.

5.7.2 Business continuity plans should consider the possible event that the quality of the provision of the outsourced critical or important function deteriorates to an unacceptable level or fails. Such plans should also take into account the potential impact of the insolvency or other failures of service providers and, where relevant, political risk in the service provider's jurisdiction.

Section 8 Governance framework – internal audit function

5.8.1 The internal audit function's activities should cover, following a risk-based approach, the independent review of outsourced activities. The audit plan and programme should include, in particular, the outsourcing arrangements of critical or important functions.

5.8.2 With regard to the outsourcing process, the internal audit function should at least ascertain:

a) That the firm's framework for outsourcing, including the outsourcing policy, is correctly and effectively implemented and is in line with the applicable Acts, Regulations, rules or sector-specific guidelines, the risk strategy and the decisions of the Management Body;

b) The adequacy, quality and effectiveness of the assessment of the criticality or importance of functions;

c) The adequacy, quality and effectiveness of the risk assessment for outsourcing arrangements and that the risks remain in line with the firm's risk strategy;

d) The appropriate involvement of governing bodies; and

e) The appropriate monitoring and management of outsourcing arrangements.

Section 9 Governance framework – documentation requirements

5.9.1 As part of their risk management framework, Licence Holders should maintain an updated register of information on all outsourcing arrangements at the authorised firm and, where applicable, at sub-consolidated and consolidated levels, as set out in 5.2.2 to 5.2.4, and should appropriately document all current outsourcing arrangements, distinguishing between the outsourcing of critical or important functions and other outsourcing arrangements. Taking into account national regulation and the principle of proportionality, Licence Holders should maintain the documentation of past or terminated outsourcing arrangements within the register and the supporting documentation for a predefined retention period.

5.9.2 Taking into account the principle of proportionality (Principle 1 under Title 1), as well as Section 2, 5.2.2 to 5.2.4, under Title 5, for Licence Holders within a group, with respect to Licence Holders permanently affiliated to a central body or that are members of the same institutional scheme if applicable, the register may be centrally kept.

5.9.3 The register should include at least the following information for all existing outsourcing arrangements:

a) A reference number for each outsourcing arrangement;

b) The start date, as applicable, the next contract renewal date, the end date and/or notice periods for the service provider and for the Licence Holder;

c) A brief description of the outsourced function, including the data that are outsourced and whether or not personal data (e.g. by providing a yes or no in a separate data field) have been transferred or if their processing is outsourced to a service provider;

d) A category assigned by the Licence Holder that reflects the nature of the function as described under point (c) (e.g., information technology (IT), control function), which should facilitate the identification of different types of arrangements;

e) The name of the service provider, the corporate registration number, the legal entity identifier (where available), the registered address and other relevant contact details, and the name of its parent company (if applicable);

f) The country or countries where the service is to be performed, including the location (i.e. country or region) of the data;

g) Whether or not (yes/no) the outsourced function is considered critical or important, including, where applicable, a brief summary of the reasons why the outsourced function is considered critical or important, and if so, its interconnections with any other critical or important functions;

h) In the case of outsourcing to a cloud service provider, the cloud service model(s) (e.g. laas, PaaS, SaaS) and deployment models, i.e. public/private/hybrid/community, and the specific nature of the data to be held and the locations (i.e. countries or regions) where such data will be stored;

i) The data of the most recent assessment of the criticality or importance of the outsourced function.

5.9.4 For the outsourcing of critical or important functions (material outsourcing), the register should include at least the following additional information:

a) In case of groups, other Licence Holders/Firms within the scope of the prudential consolidation or institutional protection scheme, where applicable, that make use of the outsourcing;

b) Whether or not the service provider or sub-service provider is part of the group or a member of the institutional protection scheme, or is owned by authorised firms within the group, or is owned by members of an institutional protection scheme;

c) The date of the most recent risk assessment and a brief summary of the main results;

d) The decision-making body (e.g. the Management Body) in the authorised firm that approved the outsourcing arrangement;

e) The governing law of the outsourcing arrangement;

f) The dates of the most recent and next scheduled audits, where applicable;

g) Where applicable, the name of any sub-outsourcers to which material parts of a critical or important function are sub-contracted, including the countries where the sub-contractors are registered, where the service will be performed and, if applicable, the location (i.e. country or region) where the data will be stored and/or processed;

h) An outcome of the assessment of the service provider's substitutability (as easy, difficult or impossible), the possibility of reintegrating a critical or important function into the authorised firm or the impact of discontinuing the critical or important function;

i) Identification of alternative service providers in line with point (h);

j) Whether the outsourced critical or important function supports any business operations that are time-critical;

k) The estimated annual costs;

l) Whether the cloud provider has a business continuity plan that is suitable for the services provided to the Licence Holder in line with regulatory requirements;

m) A description of resources employed by the Licence Holder for monitoring outsourced activities in the cloud if applicable (i.e. number of resources and their skills);

n) Whether the Licence Holder has a written exit strategy (yes/no) in case of termination by either party or disruption of services by the cloud service provider, and reference to such document.

5.9.5 Licence Holders should, upon request, make available to the Authority either the full register of all existing outsourcing arrangements or sections specified thereof, such as information on all outsourcing arrangements falling under one of the categories referred to in point 5.9.3. (d), a copy of the outsourcing agreement(s), and related information on the periodical assessment performed, or any parts thereof. Licence Holders should provide the register or parts thereof as requested in a processable electronic form (e.g. a commonly used database format, or comma separated values).

5.9.6 Licence Holders should, upon request, make available to the Authority all information necessary to enable it to execute the effective supervision of the authorised firm, including, where required, a copy of the outsourcing agreement.

5.9.7 Without prejudice to their legal obligations, authorised firms should adequately inform the Authority in writing in a timely manner or engage in a supervisory dialogue with it about the planned outsourcing of critical or important functions and/or where an outsourced function has become critical or important, and provide at least the information specified in 5.9.3 and 5.9.4, in addition to a draft version of the outsourcing arrangement.

5.9.8 Authorised firms should inform the Authority in a timely manner of material changes and/or severe events regarding their outsourcing arrangements that could have a material impact on the continuing provision of their business activities.

5.9.9 Licence Holders should appropriately document the assessments made under Title 5 Section 10 (outsourcing process) and the results of their ongoing monitoring (e.g. performance of the service provider, compliance with agreed service levels, other contractual and regulatory requirements, updates to the risk assessment).

Section 10 Outsourcing process – Pre-outsourcing analysis

5.10.1 Before entering into any outsourcing arrangements, Licence Holders should:

a) Assess if the outsourcing arrangement concerns a critical or important function, as set out in 5.3.5 and 5.3.6 under Title 5;

b) Assess if the supervisory conditions for outsourcing set out in 5.10.2 and 5.10.3 are met;

c) Identify and assess all the relevant risks of the outsourcing arrangement as outlined in 5.10.4 to 5.10.8;

d) Undertake appropriate due diligence on the prospective service provider in line with the guidance provided in 5.10.9 to 5.10.13;

e) Identify and assess conflicts of interest that the outsourcing may cause in line with Section 6 of Title 5 and relevant regulations.

5.10.2 *Supervisory conditions for outsourcing* Licence Holders should ensure that outsourcing of functions that require authorisation or registration by the Authority to a service provider located in Malta or another Member State, takes place only if one of the following conditions is met:

a) The service provider is authorised or registered by a competent authority to perform such activities; or

b) The service provider is otherwise allowed to carry out those activities in accordance with the relevant national legal framework.

5.10.3 Licence Holders should ensure that outsourcing of functions that require authorisation or registration by the Authority to a service provider located in a third country (that is outside the European Union), takes place only if all the following conditions are met:

a) The service provider is authorised or registered to provide the outsourced activity in the third country and is supervised by a relevant competent authority in that third country (referred to as a 'supervisory authority');

b) There is an appropriate cooperation agreement, e.g. in the form of a memorandum of understanding or college agreement, between the Authority and the supervisory authorities responsible for the supervision of the service provider; and

c) The cooperation agreement referred to in point (b) should ensure that the Authority is able to, at least:

i. Obtain, upon request, the information necessary to carry out its supervisory tasks as it is required to do under relevant and applicable sectoral legislation;

ii. Obtain appropriate access to any data, documents, premises or personnel in the third country that are relevant for the performance of its supervisory powers;

iii. Receive, as soon as possible, information from the supervisory authority in the third country for investigating any and apparent breaches to regulatory requirements; and

iv. Cooperate with the relevant supervisory authority in the third country on enforcement in the case of a breach of the applicable regulatory requirements and national laws in Malta. Cooperation should include, but not necessarily be limited to, receiving information on potential breaches of the applicable regulatory requirements from the supervisory authorities in the third country as soon as is practicable.

5.10.4 *Risk assessment of outsourcing arrangements*

Licence Holders should assess the potential impact of outsourcing arrangements on their operational risk and whether the outsourcing would materially affect the risk profile. Licence Holders should therefore consider the assessment results when deciding if the function should be outsourced to a service provider and should take appropriate steps to avoid undue additional operational risks before entering into such outsourcing arrangements. In performing such assessment, where relevant, a Licence Holder should take into account the possible extension and foreseen changes to the outsourcing arrangement.

5.10.5 The assessment should include, where appropriate, scenarios of possible risk events, including high-severity operational risk events. Within the scenario analysis, authorised firms should assess the potential impact of service outages or service failures, and inadequate services i.e. falling below the agreed service levels, including the risks caused by processes, systems, people or external events, on the Licence Holder's:

a) Continuous compliance with the conditions of their authorisation and all applicable regulatory obligations;

b) Short and long-term financial and solvency resilience and viability;

c) Business continuity and operational resilience;

d) Operational risk, including conduct, information and communication technology (ICT), cyber and legal risks;

e) Reputational and strategic risks;

f) Recovery and resolution planning, resolvability and operational continuity in an early intervention, recovery or resolution situations, where applicable.

Taking into consideration the principle of proportionality, Licence Holders should document the analysis performed and their results and should estimate the extent to which the outsourcing arrangement would increase or decrease their operational risk. Small and non-complex authorised firms may use qualitative risk assessment approaches, while large or complex Licence Holders should have a more sophisticated approach, including, where available, the use of registered internal (specific to the Licence Holder) and external loss data (specific to the sector) to inform the scenario analysis.

5.10.6 Within the risk assessment, Licence Holders should also take into account the expected benefits and costs of the proposed outsourcing agreement, including weighing any risks that may be reduced or better managed against any risks that may arise as a result of the proposed outsourcing arrangement, taking into account at least:

a) Concentration risks, including from:

i. Outsourcing to a dominant service provider that is not easily substitutable; and

ii. Multiple outsourcing arrangements with the same service provider or closely connected service providers;

b) The aggregated risks resulting from outsourcing several functions across the authorised firm and, in the case of groups of Licence Holders or institutional protection schemes, the aggregated risks on a consolidated basis or on the basis of the institutional protection scheme;

c) In the case of significant credit institutions, the step-in risk, i.e. the risk that may result from the need to provide financial support to a service provider in distress or to take over of its business operations; and

d) The measures implemented by the Licence Holders and by the service provider to manage and mitigate the risks.

5.10.7 Where the outsourcing arrangement includes the possibility that the service provider sub-outsources critical or important functions to other service providers, Licence Holders should take into account:

a) The risks associated with sub-outsourcing, including the additional risks that may arise if the sub-contractor is located in a third country or a different country from the service provider;

b) The risk that long and complex chains of sub-outsourcing reduce the ability of Licence Holders to oversee the outsourced critical or important function and the ability of competent authorities to supervise them.

The risk management system applied by the Licence Holder should think about the risks related to sub-outsourcing. If the risk is considered too high, the Licence Holder should not accept sub-outsourcing to a specific sub-outsourcer or third party.

5.10.8 When carrying out the risk assessment prior to outsourcing and during ongoing monitoring of the service provider's performance, Licence Holder should, at least:

a) Identify and classify the relevant functions and related data and systems as regards their sensitivity and required security measures;

b) Conduct a thorough risk-based analysis of the functions and related data and systems that are being considered for outsourcing or have been outsourced as part of a Technology Arrangement's overall design, and address the potential strategic and operational risks, including legal, ICT, compliance and reputational risks, and the oversight limitations related to the countries where the outsourced services are or may be provided and where the data are or are likely to be stored;

c) Consider the risks arising from the use of cloud services (i.e. Iaas/PaaS, SaaS, XaaS) and deployment models (i.e. public/private/hybrid/community), and where applicable, assess the risks arising from the migration and/or the implementation;

d) Consider the consequences of where the service provider is located (within or outside the EU) including the context of assuring compliance of the provided services with applicable EU and national laws, external and internal regulations and standards adopted by the Licence Holder;

e) Consider the political stability and security situation of the jurisdictions in question, including:

   i. The laws in force, including laws on data protection;
   ii. The law enforcement provisions in place; and
   iii. The insolvency law provisions that would apply in the event of a service provider's failure and any constraints that would arise in respect of the urgency recovery of the Licence Holder's data in particular;

f) Define and decide on an appropriate level of protection of data confidentiality, of continuity of the activities outsourced and of the integrity and traceability of data and systems in the context of the intended outsourcing. Licence Holders should also consider specific measures, where necessary, for data in transit, data in memory and data at rest, such as the use of encryption technologies in combination with appropriate key management architecture; and a sound user and access management process;

g) Consider whether the service provider is a subsidiary or parent entity of the Licence Holder, is included in the scope of accounting consolidation or is a member of, or owned by, the authorised firms that are members of an institutional protection scheme and, if so, the extent to which the authorised firm controls the service provider or has the ability to influence its actions.

5.10.9 *Due diligence*

Before entering into an outsourcing arrangement and considering the operational risks related to the function to be outsourced, Licence Holders should perform a due diligence in their selection and assessment process, applying criteria defined by their written outsourcing policy to ensure the suitability of the service provider.

5.10.10 With regard to critical or important functions, Licence Holders should ensure that the service provider has the business reputation, appropriate and sufficient abilities, the expertise, the capacity, the resources (e.g. human, IT, financial), the organisational structure and, if applicable, the required regulatory authorisation(s) or registration(s) to perform the function(s) in a reliable and professional manner to meet its obligations over the duration of the draft contract.

Where appropriate, evidence or certificates based on common relevant standards, such as but not limited to ISO / IEC 2700X, SOC2 Type II reports and/or internal reports can be used to support the due diligence performed.

5.10.11 Additional factors to be considered when conducting due diligence on a potential service provider include, but are not limited to:

a) Its business model, nature, scale, complexity, financial situation, ownership and group structure;

b) The long-term relationships with service providers that have already been assessed and performed services for the Licence Holder;

c) Whether the service provider is a parent entity or subsidiary of the authorised firm, is part of the accounting scope of consolidation of the firm or is a member of, or is owned by, authorised entities that are members of the same institutional protections scheme to which the Licence Holder belongs;

d) Whether or not the service provider is supervised by competent authorities.

5.10.12 Where outsourcing involves the processing of personal or confidential data, Licence Holders should be satisfied that the service provider implements appropriate technical and organisational measures to protect the data.

5.10.13 Licence Holders should take appropriate steps to ensure that service providers act in a manner consistent with their values and code of conduct. In particular, with regard to service providers located in third countries and, if applicable, their sub-contractors, Licence Holders should be satisfied that the service provider acts in an ethical and socially responsible manner and adheres to international standards on human rights (e.g. the European Convention of Human Rights), environmental protection and appropriate working conditions, including the prohibition of child labour.

Section 11 Outsourcing process – Contractual phase

5.11.1 The rights and obligations of the Licence Holder and the service provider should be clearly allocated and set out in a written agreement.

5.11.2 In additional to any applicable legal and regulatory requirements, the outsourcing agreement for critical or important functions should at least include:

a) A clear description of the outsourced function to be provided, including the type of support services;

b) The start date, and as applicable, the next contract renewal date, the end date and/or notice periods for the service provider and the Licence Holder;

c) The court jurisdiction and the governing law of the agreement;

d) The parties' financial obligations, including the service provider's pricing model;

e) The parties' operational obligations and responsibilities (for example, in the case of user and access management or incident management);

f) Whether the sub-outsourcing of a critical or important function, or material parts thereof, is permitted and if so, the conditions specified in 5.11.3 to 5.11.7 that sub-outsourcing is subject to;

g) The location(s) (i.e. regions or countries) where the critical or important function will be provided and/or where relevant data will be kept and processed, including the possible storage location, and the conditions to be met, including a requirement to notify the Licence Holder if the service provider proposes to change the location(s);

h) Provisions regarding the accessibility, availability, integrity, confidentiality, privacy and safety of relevant data, as specified in 5.11.8 to 5.11.11;

i) The right of the Licence Holder to monitor the service provider's performance on an ongoing basis;

j) The agreed service levels, which should include precise quantitative and qualitative performance targets for the outsourced function, that are directly measurable by the Licence Holder, to allow for timely and independent monitoring of the service(s) received, so that appropriate corrective action can be taken without undue delay if the agreed service levels are not met;

k) The reporting obligations of the service provider to the Licence Holder, including the communication by the service provider of any development that may have a material impact on the service provider's ability to effectively carry out the critical or important function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements and, as appropriate, the obligations to submit reports of the internal audit function of the service provider;

l) Whether the service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;

m) The requirements to implement and test business contingency plans;

n) Provisions that ensure that the data that are owned by the Licence Holder can be accessed in the case of the insolvency, resolution or discontinuation of business operations of the service provider;

o) The obligation of the service provider to cooperate with the competent authorities and resolution authorities of the Licence Holder, including other persons appointed by them;

p) For institutions, a clear reference to the powers of Malta's Resolution Committee within the Malta Financial Services Authority, assigned to it by the Resolution Authority for taking resolution decisions pursuant to the MFSA Act and the Recovery and Resolution Regulations - L.N. 301 of 2015 under the Malta Financial Services Act (cap. 330), in line with the Bank Recovery and Resolution Directive – Directive 2014/59/EU (BRRD), particularly Articles 68 and 71, and a clear description of the 'substantive obligations' of the contract in the sense of Article 68;

q) The unrestricted right of the Licence Holder and the Authority to inspect and audit the service provider with regard to, in particular, the critical or important outsourced function, as specified in 5.11.12 to 5.11.24;

r) Termination rights, as specified in 5.11.25 to 5.11.26.

5.11.3 *Sub-outsourcing of critical or important functions*

The outsourcing agreement should specify whether or not sub-outsourcing of critical or important functions, or material parts thereof, is permitted.

5.11.4

If sub-outsourcing of critical or important functions is permitted, Licence Holders should determine whether the part of the function to be sub-outsourced is, as such, critical or important (i.e. a material part of the critical or important function, and, if so, record it in the register.

5.11.5

If sub-outsourcing of critical or important functions is permitted, the written agreement should:

a) Specify any types of activities that are excluded from sub-outsourcing;

b) Specify the conditions to be complied with in the case of sub-outsourcing;

c) Specify that the service provider is obliged to oversee those services that it has sub-contracted to ensure that all contractual obligations between the service provider and the Licence Holder are continuously met;

d) Require the service provider to obtain prior specific or general written authorisation from the Licence Holder before sub-outsourcing data[59];

e) Include an obligation of the service provider to inform the Licence Holder of any planned sub-outsourcing, or material changes thereof, in particular where that might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. This includes planned significant changes of sub-contractors and to the notification period; in particular, the notification period to be set should allow the outsourcing Licence Holder at least to carry out a risk assessment of the proposed changes and to object to changes before the planned sub-outsourcing, or material changes thereof, come into effect;

f) Ensure, where appropriate that the Licence Holder has the right to object to intended sub-outsourcing, or material changes thereof, or that explicit approval is required;

g) Ensure that the Licence Holder has the contractual right to terminate the agreement in the case of undue sub-outsourcing, e.g. where the sub-outsourcing materially increases the risks for the Licence Holder or where the service provider sub-outsources without notifying the Licence Holder.

5.11.6 The Licence Holder should agree to sub-outsourcing only if the sub-contractor undertakes to:

a) Comply with all applicable Acts, Regulations, rules or sector-specific guidelines and contractual obligations, including the security of data and systems; and

b) Grant the Licence Holder and the Authority the same contractual rights of access and audit as those granted by the service provider.

5.11.7 Licence Holders should ensure that the service provider appropriately oversees the sub-service providers, in line with the policy defined by the Licence Holder. If the sub-outsourcing proposed could have material adverse effects on the outsourcing arrangement of a critical or important function or would lead to a material increase of risk, including where the conditions of 5.11.6 would not be met, the Licence Holder should exercise its right to object to the sub-outsourcing, if such a right was agreed, and/or terminate the contract.

5.11.8 *Security of data and systems* Licence Holders should ensure that service providers comply with appropriate IT security and data protection standards.

[59] See Article 28 of Regulation (EU) 2016/679 (GDPR)

5.11.9 Licence Holders should define within the outsourcing agreement data and system security objectives that are appropriate, proportionate and that, as a minimum, meet the requirements set out in the Licence Holder's Information Security Policy (refer to Section 4, 4.7.2-4.7.4 under Title 4). If the Licence Holder's Information Security Policy document cannot be shared with the service provider and referenced in the agreement even under a non-disclosure agreement because of its data classification, the outsourcing agreement should at least include written provisions and security objective obligations that are at least at par with relevant requirements set out in the Information Security Policy. Licence Holders should monitor compliance with these requirements on an ongoing basis. For this purpose, Licence Holders, prior to outsourcing to service providers, on the basis of the risk assessment performed in accordance with 5.10.4 to 5.10.8, should:

a) Consider the design of the overall Technology Arrangement and outsourced component(s) or services, taking into consideration all factors listed in 5.10.8;

b) Ensure that network traffic availability (also by taking into consideration Section 9 3.9.2 under Title 3) and expected capacity are guaranteed, where applicable and feasible;

c) Define and decide on proper continuity requirements ensuring adequate levels at each level of the technological chain, where applicable;

d) Define specific processes by the Licence Holder and the service provider to ensure an overall sound management of the incidents that may occur, including provisions for timely incident reporting and escalations;

e) Agree on a data residency policy with service providers which sets out the countries where the Licence Holder's data can be stored, processed and managed. This policy should be reviewed periodically, and the Licence Holder should be able to verify compliance of the service provider with such policy; and

f) Monitor the level of fulfilment of the requirements to the efficiency of control mechanisms implemented by the service provider that would mitigate the risks related to the provided services.

5.11.10 In the case of outsourcing to cloud service providers and other outsourcing arrangements that involve the handling or transfer of personal or confidential data, Licence Holders should adopt a risk-based approach to data storage and data processing location(s) (i.e. country or region) and information security considerations.

5.11.11 Without prejudice to the requirements under Regulation (EU) 2016/679 (GDPR), Licence Holders, when outsourcing (in particular to third countries), should take into account differences in national provisions regarding the protection of data. Licence Holders should ensure that the outsourcing agreement includes the obligation that the service provider protects confidential, personal or otherwise sensitive information and complies with all legal requirements regarding the protection of data that apply to the Licence Holder (e.g. the protection of personal data, adherence to a predefined data retention policy, and that secrecy or similar legal confidentiality duties with respect to clients' information, where applicable, are observed).

5.11.12 *Access, information and audit rights*

Licence Holders should ensure within the written outsourcing arrangements that the internal audit function is able to review the outsourcing function using a risk-based approach.

5.11.13 Regardless of the criticality or importance of the outsourced function, the written outsourcing arrangements between Licence Holders and service providers should refer to the information gathering and investigatory powers of competent authorities and resolution authorities with regard to service providers located in a Member State and should also ensure those rights with regard to service providers located in third countries.

5.11.14 With regard to the outsourcing of critical or important functions, Licence Holders should ensure within the written outsourcing agreement that the service provider grants them and the Authority, including the Resolution Authority if applicable, and any other person appointed by them or the competent authorities, the following:

a) Full access to all relevant business premises (e.g. head offices and operation centres), including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the service provider's external auditors ('access and information rights'); and

b) Unrestricted rights of inspection and auditing related to the outsourcing arrangement ('audit rights'), to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements.

5.11.15 For the outsourcing of functions that are not critical or important, Licence Holders should ensure the access and audit rights as set out in 5.11.14, on a risk-based approach, considering the nature of the outsourced function and the related operational and reputational risks, its scalability, the potential impact on the continuous performance of its activities and the contractual period. Licence Holders should take into account that functions may become critical or important over time.

5.11.16 Licence Holders should ensure that the outsourcing arrangement or any other contractual arrangements does not impede or limit the effective exercise of the access and audit rights by them, and competent authorities or third parties appointed by the Licence Holders or competent authorities to exercise these rights.

5.11.17 Licence Holders should exercise their access and audit rights, determine the audit frequency and areas to be audited on a risk-based approach and adhere to relevant, commonly accepted, national and international audit standards. In determining the frequency of audit assessment, the Licence Holder should consider the nature and extent of risk and impact on the Licence Holder from the outsourcing arrangements.

5.11.18 Without prejudice to their final responsibility regarding outsourcing arrangements, Licence Holders may use:

a) Pooled audits organised jointly with other clients of the same service provider, and performed by these clients or by a third party appointed by them, to use audit resources more efficiently and to decrease the organisational burden on both the clients and the service provider;

b) Third-party certifications and third-party or internal audit reports made available by the service provider. Without prejudice to principles-based consistency of outcomes, Licence Holders should seek ISO/IEC 27001:2017 certification (or newer) or similar standard in terms of information security management baseline for all service providers. In addition, in the case of Cloud Service Providers, Licence Holders should seek additional assurance through ISO/IEC 27017:2015 (Code of practice for information security controls based on ISO/IEC 27002 for cloud services) and/or a SOC2 Type II report, ideally through a CSA STAR[60] Level 2 attestation (preferred over certification) or equivalent. Cloud Service Providers having ISO 27018:2014 or ISO 27018:2019 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors) certification, or similar standard, provide an additional level of assurance in terms of GDPR compliance.

5.11.19 For the outsourcing of critical or important functions, Licence Holders should assess whether third-party certifications and reports as referred to in 5.11.18 (b) are adequate and sufficient to comply with their regulatory obligations and should not rely solely on these reports over time. Certifications such as PCI DSS may also be required to fulfil sector-specific regulatory obligations or commercial requirements and should therefore also be taken into consideration when considering different service providers.

5.11.20 Licence Holders should make use of the method referred to in 5.11.18 (b) only if they:

a) Are satisfied with the audit plan for the outsourced function;

b) Ensure that the scope of the certification or audit report covers the systems (i.e. processes, applications,

[60] Cloud Security Alliance®: Security, Trust Assurance & Risk Registry

infrastructure, data centres, etc.) and key controls identified by the Licence Holder and the compliance with relevant regulatory requirements;

c) Thoroughly assess the content of the certifications or audit reports on an ongoing basis and verify that the reports or certifications are not obsolete;

d) Ensure that key systems and controls are covered in future versions of the certification or audit reports;

e) Are satisfied with the aptitude of the certifying or auditing party (e.g. with regard to rotation of the certifying or auditing company, qualifications, expertise, re-performance/verification of the evidence in the underlying audit file);

f) Are satisfied that the certifications are issued, and the audits are performed against widely recognised relevant professional standards and include a test of the operational effectiveness of the key controls in place;

g) Have the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls; the number and frequency of such requests for scope modifications should be reasonable and legitimate from a risk management perspective; and

h) Retain the contractual right to perform individual on-site audits at their discretion with regard to the outsourcing of critical or important functions; such rights should be exercised in case of specific needs not manageable through other types of interactions with the service provider.

5.11.21 The outsourcing contract should have provisions for adequate notice to be given to the service provider before a planned on-site visit by the Licence Holder, the Authority, and auditors or third parties acting on behalf of the Licence Holder or the Authority, without prejudice to the right of the Licence Holders, the Authority, and auditors or third parties acting on their behalf, for immediate access owing to an emergency or crisis situation, or to cater for situations where advance notice regarding an audit would render the audit objectives ineffective.

5.11.22 When performing audits in the operating environment of the service provider, particularly in the case of multi-client environments, care should be taken to ensure that risks to the service provider's or service provider's clients' operating environment (e.g. impact on service levels, availability of data, confidentiality aspects), are avoided or mitigated, for example by agreeing with the service provider on alternative ways to provide a similar level of assurance to the Licence Holder.

5.11.23 Where the outsourcing arrangement carries a high level of technical complexity, for instance in the case of cloud outsourcing, the Licence Holder should verify that whoever is performing the audit - whether it is its internal auditors, the pool of auditors or external auditors acting on its behalf – has appropriate and relevant skills and knowledge to perform relevant audits and/or assessments effectively. The same applies to any staff of the Licence Holders reviewing third-party certifications or audits carried by service providers.

5.11.24 *Termination rights*

The outsourcing arrangements should expressly allow the possibility for the Licence Holder to terminate the arrangement, in accordance with applicable law, including in the following situations:

a) Where the provider of the outsourced functions is in a breach of applicable law, regulations or contractual provisions;

b) Where impediments capable of altering the performance of the outsourced function are identified;

c) Where there are material changes affecting the outsourcing arrangement or the service provider (e.g. sub-outsourcing or changes of sub-contractors);

d) Where there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information; and

e) Where instructions are given by the Authority e.g. in the case that the Authority is no longer in a position to effectively supervise the Licence Holder because of the outsourcing arrangement.

5.11.25

The outsourcing arrangement should facilitate the transfer of the outsourced function and sub-outsourced elements to another service provider or its re-incorporation into the Licence Holder. To this end, the written outsourcing arrangement should:

a) Clearly set out the obligations of the existing service provider, in the case of a transfer of the outsourced function to another service provider or back to the Licence Holder, including treatment of data;

b) Set an appropriate transition period, during which the service provider, after the termination of the outsourcing arrangement, would continue to provide the outsourced function to reduce the risk of disruptions; and

c) Include an obligation of the service provider to support the Licence Holder in the orderly transfer of the function in the event of the termination of the outsourcing agreement;

d) Clearly specify that after the transfer to another provider or the Licence Holder, any remaining Licence Holder data will be completely and irrevocably deleted by the service provider.

Section 12 Outsourcing process – monitoring and oversight of outsourcing arrangements

5.12.1

Licence Holders should monitor, on an ongoing basis, the performance of the service providers with regard to all outsourcing arrangements on a risk-based approach, taking into account the principle of proportionality, and with the main focus being on the outsourcing and sub-outsourcing of critical or important functions, including that the availability, integrity and security of data and information is ensured. In order to do so, Licence Holders should set up monitoring and oversight mechanisms which include, but are not limited to the management of:

a) Service provider incidents having an impact on the Licence Holder's activities, in accordance with Section 8, 4.8.10 under Title 4;

b) Roles and responsibilities between the service provider and the Licence Holder in relation to all the IT (including cybersecurity) and non-IT processes affected by the outsourcing arrangement, which should be clearly delineated;

c) Ongoing and independent verifications of the Service Level Agreements, as agreed with the service provider.

Where the risk, nature or scale of an outsourced function has materially changed, Licence Holders should reassess the criticality or importance of that function in line with 5.3.5 and 5.3.6.

5.12.2 Licence Holders should apply due skill, care and diligence when monitoring and managing outsourcing arrangements. In order to ensure the adequate monitoring and oversight of the outsourcing arrangements, Licence Holders should employ enough resources with adequate skills and knowledge to monitor the outsourced services. The Licence Holder's personnel in charge of these activities should have both IT and business knowledge as deemed necessary.

5.12.3 Licence Holders should regularly update their risk assessment, that is by carrying out a periodic risk assessment as written in the outsourcing policy, in accordance with 5.10.4 to 5.10.8, and in any case, before renewal of the agreement if it concerns content and scope. Moreover, if the Licence Holder becomes aware of significant deficiencies and significant changes of the services provided or the situation of the outsourcer, the risk assessment should be promptly reviewed or re-performed. The Management Body should be informed about the risks identified in respect of the outsourcing of critical or important functions.

5.12.4 Licence Holders should monitor and manage their internal concentration risks caused by outsourcing arrangements, taking into account 5.10.4 to 5.10.8 of these guidelines, and the Management Body should be regularly updated accordingly.

5.12.5 Further to 5.12.1, Licence Holders should ensure, on an ongoing basis, that outsourcing arrangements, with the main focus being on outsourced critical or important functions, meet appropriate performance and quality standards in line with their policies by:

a) Ensuring that they receive appropriate reports from service providers;

b) Evaluating the performance of service providers using tools such as key performance indicators, key control indicators, service delivery reports, self-certification and independent reviews; and

c) Reviewing all other relevant information received from the service provider, including reports on business continuity measures and testing.

5.12.6 Licence Holders should take appropriate measures if they identify shortcomings in the provision of the outsourced function. In particular, authorised firms should follow up on any indications that service providers may not be carrying out the outsourced critical or important function effectively or in compliance with applicable law and regulatory requirements. If shortcomings are identified, Licence Holders should take appropriate corrective or remedial actions. Such actions may include terminating the outsourcing agreement, with immediate effect, if necessary.

Section 13 Outsourcing process – exit strategies

5.13.1 Licence Holders should have a documented exit strategy when outsourcing critical or important functions that is in line with their outsourcing policy and business continuity plans, taking into account at least the possibility of:

a) The termination of outsourcing arrangements;

b) The failure of the service provider;

c) The deterioration of the quality of the function provided and actual or potential business disruptions caused by the inappropriate or failed provision of the function;

d) Material risks arising for the appropriate and continuous application of the function.

5.13.2 Licence Holders should ensure that they are able to exit outsourcing arrangements without undue disruption to their business activities, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of its provision of services to clients. To achieve this, they should:

a) Develop and implement exit plans that are comprehensive, service based, documented and, where appropriate, sufficiently tested (e.g. by carrying out an analysis of the potential costs, impacts, resources and timing implications of transferring an outsourced service to an alternative provider); and

b) Identify alternative solutions and develop transition plans to enable the Licence Holder to remove outsourced functions and data from the service provider and transfer them to alternative providers or back to the Licence Holder or to take other measures that ensure the continuous provision of the critical or important function or business activity in a controlled and sufficiently tested manner, taking into account the challenges that may arise because of the location of data and taking the necessary measures to ensure business continuity during the transition phase.

5.13.3 When developing exit strategies, Licence Holders should:

a) Define the objectives of the exit strategy;

b) Perform a business impact analysis that is commensurate with the risk of the outsourced process, services or activities, with the aim of identifying what human and financial resources would be required to implement the exit plan and how much time it would take;

c) Assign roles, responsibilities and sufficient resources to manage exit plans and the transition of activities;

d) Define success criteria for the transition of outsourced functions and data; and

e) Define the indicators to be used for the monitoring of the outsourcing arrangements (as outlined in 5.12.4 to 5.12.6), including indicators based on unacceptable service levels that should trigger an exit.

Malta Financial Services Authority

Triq L-Imdina, Zone 1
Central Business District, Birkirkara, CBD 1010, Malta
communications@mfsa.mt
www.mfsa.mt