IBM Cloud for Financial Services

European Financial Regulatory Guide to relevant policies from the European Supervisory Authorities (EBA, EIOPA and ESMA)

Disclosure

This document is provided for informational purposes only.

IBM is committed to helping our clients and prospects with the knowledge to enable them to make decisions regarding their own client base needs.

The intended audience for this guide is legal and compliance experts seeking to understand the cloud outsourcing and security risk management guidelines published by the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and European Securities and Markets Authorities (ESMA).

Clients are responsible for ensuring their own compliance with various applicable laws and regulations. Clients are solely responsible for obtaining professional legal advice as to identifying and interpreting any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. IBM does not provide legal, accounting or auditing advice. IBM also does not represent or warrant that its services or products will ensure that clients are compliant with any applicable laws or regulations.

Table of Contents

1. Introduction

This European Financial Regulatory Guide (Guide) is intended for financial institutions who want to take advantage of the public cloud through the IBM Cloud® for Financial Services™.

The purpose of this Guide is to highlight key outsourcing, Information and Communications Technology (ICT), and security risk management guidance promulgated by European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authorities (ESMA).

The centerpiece of this Guide is Section 4 “Regulatory Guidance Table,” where key guidance from EBA, EIOPA, and ESMA is listed and is mapped to IBM references that indicate how IBM supports customers in meeting each featured guideline.

The Guide begins with an overview of European Union Financial Supervision (*Section 2*), followed by an overview of IBM Cloud® for Financial Services™ (*Section 3*), which includes a discussion of the IBM Cloud Framework for Financial Services, designed specifically with controls to address the unique risks of the financial services industry. Lastly the Regulatory Guidance Table (*Section 4*), aligns to the IBM Cloud Framework for Financial Services and associated practices, and provides useful IBM reference points for financial institutions doing business in Europe.[1]

[1] For purposes of the guide, “Financial Institutions” (FI) are companies engaged in banking, insurance, or securities markets.

2. European Union financial supervision

In the European Union (EU), the financial industry is divided into banking, securities, and insurance. The supervision of financial institutions is spread among three supervisory authorities, each responsible for a part of the financial sector: the European Banking Authority (EBA) (*banking*), the European Insurance and Occupational Pensions Authority (EIOPA) (*insurance*), and the European Securities and Markets Authorities (ESMA) (*securities*). The system also comprises the European Systemic Risk Board (ESRB) as well as the Joint Committee of the European Supervisory Authorities[2] and the national supervisory authorities. [3]

EBA,[4] EIOPA,[5] ESMA,[6] and other European supervisory agencies have released a series of guidelines for financial institutions that may be applied to cloud transformations, depending on the implementation and the markets in which the financial institution operates.

In particular, the adoption of EBA guidelines by EU member states, as part of the European Single Rulebook, helps to harmonize prudential rules for financial institutions within the EU. However, each country's National Competent Authority has discretion in implementing guidelines so that implementation might vary among the nations.

The guidelines published by EBA, EIOPA, and ESMA — similar to those published by other supervisory bodies in other jurisdictions— are referenced by regulatory bodies, and in many cases increasingly become part of local regulations or legislation. IBM supports the aligned outsourcing guidance issued by these three regulators, which provides greater regulatory clarity for our customers across the EU.

The EBA, EIOPA, and ESMA Guidelines shed light on the control objectives that organizations need for compliance while promoting regulatory convergence for financial institutions in the EU. The EBA Guidelines, in particular, echo the European Central Bank's (ECB) supervisory priorities for 2021[7], ESMA's 2021 Annual Work Programme and EIOPA's 2020_Financial Stability Report[8], including the IT and cyber risks and risks associated with outsourcing.

To stay competitive in a shifting marketplace, outsourcing into the cloud can be an opportunity for financial institutions to innovate, improve efficiencies, enhance competitiveness, and mitigate risk. Moreover, with the EBA, EIOPA, and ESMA Guidelines, it is clear that financial institutions can achieve compliance while leveraging the benefits of the cloud.

[2] To ensure an effective recovery and resolution regime, European Banking Supervision, and the Single Resolution Board (SRB) cooperate closely in implementing the first two pillars of the Banking Union – the Single Supervisory Mechanism (SSM) and the Single Resolution Mechanism (SRM).
https://www.bankingsupervision.europa.eu/press/publications/newsletter/2017/html/ssm.nl171115_4.en.html

[3] *EBA at a Glance*, https://www.eba.europa.eu/about-us/eba-at-a-glance.

[4] "[EBA] is an independent EU Authority which works to ensure effective and consistent prudential regulation and supervision across the European banking sector. Its overall objectives are to maintain financial stability in the EU and to safeguard the integrity, efficiency, and orderly functioning of the banking sector." *Id*.

[5] "EIOPA is an independent advisory body to the European Commission, the European Parliament, and the Council of the European Union. We are one of the EU agencies carrying out specific legal, technical, or scientific tasks and giving evidence-based advice. In this way, we help shape informed policies and laws at EU and national levels." *About EIOPA,* https://www.eiopa.europa.eu/about/mission-and-tasks_en.

[6] "[ESMA] is an independent European Union (EU) Authority that contributes to safeguarding the stability of the EU's financial system by enhancing the protection of investors and promoting stable and orderly financial markets." ESMA in Brief, https://www.esma.europa.eu/about-esma/esma-in-brief
https://www.esma.europa.eu/about-esma/esma-in-brief.

[7] ECB Banking Supervision: SSM Supervisory Priorities for 2021, https://www.bankingsupervision.europa.eu/banking/priorities/html/ssm.supervisory_priorities2021~9b7076bb8b.en.html#toc4.

[8] ECB Banking Supervision: SSM Supervisory Priorities, https://www.bankingsupervision.europa.eu/banking/priorities/html/ssm.supervisory_priorities2021~9b7076bb8b.en.html#toc4.

3. IBM Cloud for Financial Services

IBM Cloud for Financial Services ™ is a first-of-its-kind public cloud developed for and with the industry with the security and controls capabilities to help clients as they work to mitigate risk and accelerate cloud adoption for even their most sensitive workloads.

Our cloud is designed to help clients automate their security and compliance posture and monitor it with security and controls built into the platform — not just offered as add-on tools or do-it-yourself features. It also provides industry-leading security and privacy capabilities[9] and is strengthened by IBM's deep IT operations knowledge, industry expertise and an extensive set of curated ecosystem partners. The result is a secured environment engineered to help clients with lowering the risk and cost of moving sensitive data to the cloud, modernizing workloads and rapidly integrating the capabilities needed to move their business forward. Financial institutions can now take advantage of the benefits of public cloud while also addressing their cybersecurity and regulatory compliance requirements. There's no longer a need to choose between innovation and risk management.

3.1 IBM Cloud Framework for Financial Services

At the core of our offering is a controls framework called IBM Cloud Framework for Financial Services. The framework was developed to help financial institutions automate their security and compliance posture to make it easier for them and their digital supply chain partners to simplify their risk management and demonstrate their regulatory compliance. The controls framework provides a comprehensive security and compliance structure for the ecosystem through a common set of automated, preconfigured controls applied across IBM Cloud® services, third-party applications and financial institution workloads. Created in collaboration with major financial institutions, the controls are designed to align with industry standards and global regulatory bodies. The controls framework is frequently validated with advice from the IBM Financial Services Cloud Council, comprised of top financial institution CIOs, CTOs, CISOs and Compliance and Risk Officers, and guidance from Promontory Financial Group®, an IBM Company and a global leader in regulatory compliance consulting.

The framework evolves, and controls are adapted to emerging industry requirements and regulatory obligations to help financial institutions as they mitigate the cost and complexity of staying compliant in an ever-evolving cybersecurity and regulatory landscape. The extensive control set within the IBM Cloud Framework for Financial Services includes but is not limited to security, data privacy, access management and configuration management.

3.2 A rich catalog of ISV, fintech and SaaS solutions

IBM Cloud for Financial Services is supported by an ecosystem of curated ISVs, fintechs and SaaS providers to help make it easier and faster for financial institutions to onboard third-party applications and services and begin working with them on our cloud.

Through the IBM Cloud® Security and Compliance Center, the security and compliance postures of partner applications and services can be automated and frequently monitored and evidence captured. As a result, manual steps in the compliance-management process for partner applications can be reduced, the potential for human error minimized and consistency, traceability, auditability and scalability can all be enhanced. With automation, organizations are also able to reduce variability between audits, providing valuable, consistent reports and eliminating delays while maintaining consistent compliance.

3.3 IBM Cloud Security and Compliance Center®

The IBM Cloud Security and Compliance Center helps enable clients to monitor and enforce their controls to protect data and assets and manage vulnerabilities across cloud environments. To enable financial institutions to monitor the security and compliance posture of their cloud services, in addition to partner applications and services, IBM provides the security and compliance platform and dashboard as part of an IBM Cloud account. Clients and partners can define compliance profiles, manage controls and maintain an extensive data trail for audit. This can help promote a culture of compliance within the organization that begins with resource configuration and holds through the collection of audit evidence.

[9] Based on IBM Cloud® Hyper Protect Crypto Services, the only public cloud service in the industry built on FIPS 140- 2 Level 4-certified hardware. At this security level, the physical security mechanisms can provide an envelope of protection around the cryptographic module with the intent of detecting and responding to unauthorized attempts at physical access.

The recent integration of Tanium Comply into the IBM Cloud Security and Compliance Center allows customers with regulated workloads to deepen their experience by having the ability to view the compliance evaluation results from Tanium from inside the IBM Cloud Security and Compliance Center. With Tanium Comply, clients can view their compliance data associated with IBM Cloud and Tanium in the same format in a single location. The Tanium integration allows IBM Cloud clients to extend their organization's endpoint management capabilities to include scanning for vulnerabilities and misconfigurations against industry security standards and vulnerability definitions.

3.4 Industry-leading security and data protection controls, with a zero trust approach

IBM Cloud for Financial Services has been designed with the exacting needs of the world's largest and most complex organizations in mind. It draws on all the data protection security capabilities and services built into the IBM public cloud, allowing it to be used for mission-critical workloads and highly sensitive data. IBM offers an enterprise-grade public cloud with extensive service-deployment options — such as VMware and RedHat® OpenShift® as a service —to meet the specific requirements of financial services.

Included within IBM Cloud for Financial Services are core technologies for managing your security risk and regulatory compliance framework, with a data-centric, zero trust approach.

Confidential computing

IBM takes a holistic approach to confidential computing — spanning compute, containers, databases and encryption. Confidential computing helps clients remove the implicit trust that applications place in the underlying software stack and cloud providers, so you can move from operational to technical measures and protect the privacy of your sensitive data at rest, in transit and in use. This can allow clients to move sensitive data and workloads to the cloud, unlocking new ways to collaborate and innovate. Although it's impossible to completely prevent data breaches in today's connected hybrid cloud environment, a data-centric, zero trust approach can help financial institutions modernize operations and embed security controls and is designed to mitigate the impact and cost of a data breach.

End-to-end encryption with extensive control

Our financial services cloud also offers an industry-leading key management approach that technically gives clients exclusive control of their data. Not even IBM can access it.[2] IBM Cloud® Hyper Protect Crypto Services enables cloud data encryption in a dedicated cloud hardware security module (HSM). The service offers technology like Keep Your Own Key (KYOK), a single-tenant key management service, which has key-vaulting provided by dedicated, customer-controlled HSMs and that is designed to support industry encryption standards, such as Public-Key Cryptography Standards (PKCS) #11. It's also the only public cloud service in the industry built on FIPS 140-2 Level 4-certified hardware. At this security level, the physical security mechanisms can provide an envelope of protection around the cryptographic module with the intent of detecting and responding to unauthorized attempts at physical access.

With this type of data protection, the client is the only party that governs and controls access to their private data. These capabilities can be game-changing for the financial services industry that needs to adhere to strict regulatory requirements for data protection.

IBM Cloud for Financial Services draws on additional services built into the IBM public cloud that also allow it to be used for mission-critical workloads and sensitive data.

Workload-centric security by default

Each workload requires various access and security rules. IBM enables organizations to define and enforce such guidelines by way of integrated container security and DevSecOps for cloud-native applications with Red Hat OpenShift as a service.

Multi-Zone Regions (MZRs)

Clients can leverage the underlying capabilities of IBM Cloud for Financial Services to enhance business resiliency and disaster recovery. MZRs comprise multiple high-speed, low-latency, interconnected Availability Zones that are independent from each other to help limit the impact of single-failure events to only a single Availability Zone. They enable financial institutions to locate workloads in specific geographies to fit their needs.

Logging and auditing rules

SaaS and ISV providers are required to log all actions taken through the cloud portal, API or command-line interface to be recorded in detail using IBM Cloud® Activity Tracker. This provides standard logging of activity on systems and services and full-session recording of exactly what actions operators take. This information is centrally stored and analyzed. The logging process is auditable to enable tracing of all steps, including logging both successful and unsuccessful events, and gives role-based protection at all points of intervention. The access logs are stored along with time stamps to assist analysis and forensics.

3.5 Governance and oversight

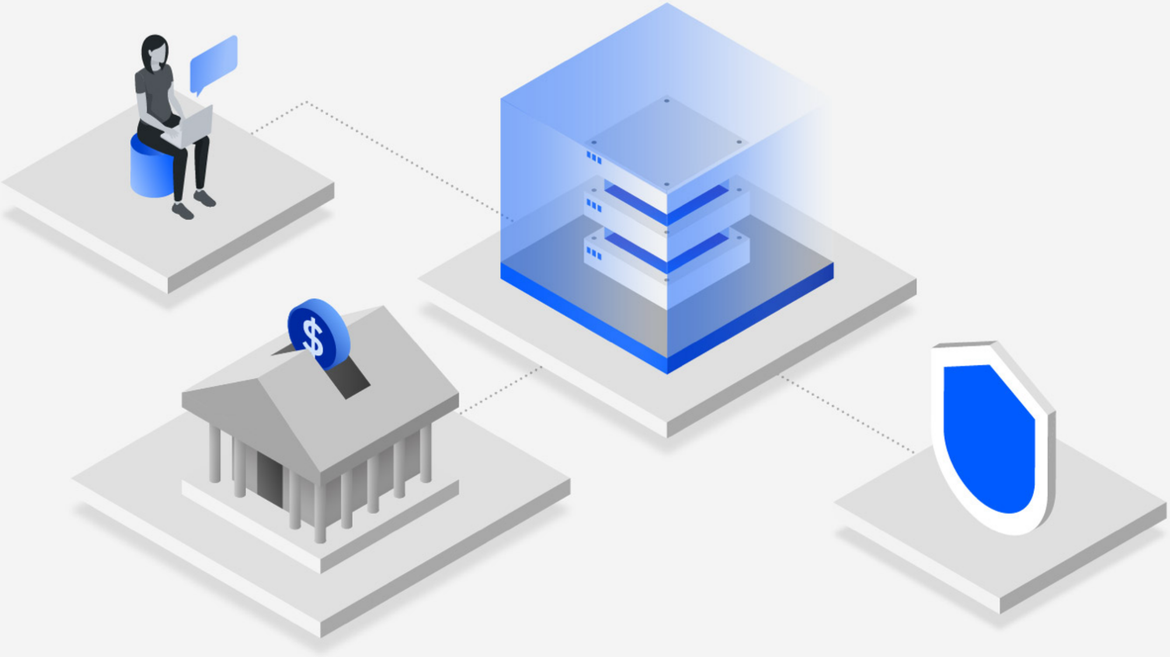
IBM Cloud for Financial Services is designed to deliver the following comprehensive set of capabilities to support governance and oversight.

Independent review of IBM Cloud for Financial Services: An independent big four public accounting firm performed an agreed-upon procedures (AUP) engagement over the IBM Cloud for Financial Services environment. Security and risk executives (CISOs and CROs) and the managers of financial institutions using IBM Cloud for Financial Services can gain transparency and efficiency in their risk management practices by using the IBM Cloud for Financial Services AUP Report.

3.6 Managing regulatory change

As part of IBM's regulatory program and watch, IBM monitors changes in global financial regulations to support customers using the IBM Cloud for Financial Services. Regulatory watch is a semi-automated process conducted by Promontory on behalf of the FS Risk Office, during which regulatory domain experts scan trusted information sources for information on regulatory policy updates in jurisdictions where IBM conducts public cloud business. It is the entry-point for triaging regulatory developments that may have an impact on the Cloud Control Framework.

As part of this process, IBM evaluates existing controls within the IBM Cloud Framework for Financial Services and may make appropriate adjustments to align with changing regulatory requirements, at IBM's sole discretion.



4. Regulatory guidance tables

As financial institutions are moving sensitive workloads to the cloud, questions arise on how to navigate the complexity of supervisory obligations in the cloud environment. In order to provide financial institutions with a broad overview of relevant outsourcing, ICT, and security guidelines, selected provisions were chosen from the following supervisory guidelines and reports (*see Section 5 herein*):

- Final Report on EBA Draft Guidelines on Outsourcing Arrangements (Outsourcing Guidelines)[10];
- EIOPA Guidelines on outsourcing to cloud service providers[11];
- Final Report on ESMA Guidelines on outsourcing to cloud service providers[12];
- Joint Advice of the European Supervisory Authorities (ESAs) To the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector.[13]
- Final Report, EBA Guidelines on ICT and Security Risk Management (ICT and Security Guidelines)[14];
- Final Report on EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)[15].

Generally, EBA's Outsourcing Guidelines recognize that financial institutions are increasingly outsourcing functions and services to support their core business to improve efficiencies and gain access to new technologies. The EBA, EIOPA, ESMA guidelines provide financial institutions with guidance when considering outsourcing arrangements and associated supervisory expectations and processes. The ICT and Security Guidelines and the ICT Risk Assessment under the SREP assist financial institutions in managing ICT and security risks.

The guidelines herein are either reproduced verbatim, condensed, or paraphrased for readability. This Guide does not cover all sections or obligations in each of the EBA, EIOPA, and ESMA guidelines covered. This Guide is a snapshot of relevant guidelines that will be helpful to financial institutions migrating sensitive workloads to the cloud. We encourage readers to review the full text of these guidelines and associated regulations in consultation with key stakeholders within their business, including those with risk and compliance responsibilities.[16]

How to read the tables

The tables below map selected EBA, EIOPA, and ESMA provisions to IBM references that assist customers in meeting their regulatory guidance. Each table contains a collection of similarly themed regulatory provisions divided into three sections:

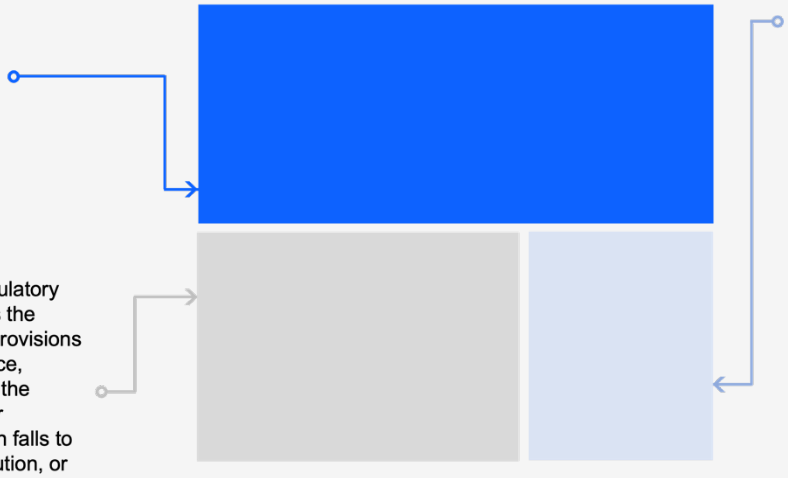


Table Scope

Regulatory provisions and topics covered in the table.

Regulatory Text

The language of the regulatory guidance. Also indicates the industries to which the provisions apply (Banking, Insurance, Securities) and whether the primary responsibility for implementing a provision falls to IBM, the Financial Institution, or both.

IBM Reference

The IBM policies or services that will help customers implement the associated regulatory guidance. This column also shows how IBM's support for each provision maps to the IBM practices and IBM Cloud Framework for Financial Services' seven Focus Areas:

1. Focused Risk Management and Compliance
2. Advanced Data Protection
3. Enhanced Authentication and Access Management
4. Automated Application and Workload Protection
5. Unified Infrastructure Security and Resilience
6. Operational Excellence
7. Active Monitoring and Response

[10] https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements.

[16]https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/guidelines_on_outsourcing_to_cloud_service_providers_en.pdf.

[12] https://www.esma.europa.eu/sites/default/files/library/esma50-157-2403_cloud_guidelines.pdf.

[13]https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf.

[14] https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management.

[15] According to EBA, ". . . these Guidelines drawn up pursuant to Article 107(3) of Directive 2013/36/EU, supplement and further specify criteria for the assessment of ICT risk as part of operational risk put forward in the EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP). https://www.eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-on-ict-risk-assessment-under-the-srep.

[16] This document is provided for informational purposes only. Clients are responsible for ensuring their own compliance with various applicable laws and regulations.

1. Outsourcing and critical or important functions defined

Regulatory Provisions:
EBA Guidelines on Outsourcing Arrangements, February 25, 2019
Title II, Section 3, Outsourcing

EIOPA Guidelines on Outsourcing to Cloud Service Providers, February 6, 2020
Guideline 2, General Principles of Governance for Cloud Outsourcing;
Guideline 5, Documentation Requirements

ESMA Guidelines on Outsourcing to Cloud Service Providers, December 18, 2020
Executive Summary and Annex III

a) Outsourcing defined

Industries: Banking, Insurance, Securities
Primary Responsibility: Financial Institution[22]

Regulatory Text:

EBA defines outsourcing as "an arrangement of any form between an institution, a payment institution or an electronic money institution and a service provider by which that service provider performs a process, a service or an activity that would otherwise be undertaken by the institution, the payment institution or the electronic money institution itself."

EBA, Section 2, Subject Matter, Scope and Definitions, para. 12 (p.19).

Tip: *FIs should consider their intragroup outsourcing and the onward outsourcing from those entities when considering outsourcing, as referenced under requirement in the EBA Guidelines on ICT and Security Risk Management. See EBA Guidelines on ICT and Security Risk Management, 3.2.3 (8) & (9) below.*

By express reference in para. 8 (p.3) of the EIOPA Guidelines, the term 'outsourcing' refers to the one described in the
Directive 2009/138/EC ("Solvency II Directive") Art. 13 'Definitions," para. 28:

"[O]utsourcing means an arrangement of any form between an insurance or reinsurance undertaking and a service provider, whether a supervised entity or not, by which that service provider performs a process, a service or an activity, whether directly or by sub-outsourcing, which would otherwise be performed by the insurance or reinsurance undertaking itself."[23]

ESMA defines **cloud outsourcing arrangement** as an arrangement of any form, including delegation arrangements, between:

(i) a firm and a CSP by which that CSP performs a function that would otherwise be undertaken by the firm itself; or

(ii) a firm and a third-party which is not a CSP, but which relies significantly on a CSP to perform a function that would otherwise be undertaken by the firm itself. In this case, a reference to a 'CSP' in these guidelines should be read as referring to such third-party." [Emphasis added.]

ESMA, Definitions (p. 25).

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

IBM Cloud for Financial Services Supporting Activities & Controls:

IBM remains responsible for the obligations under the Cloud Services Agreement, even if IBM uses a sub-contractor. IBM does not sub-outsource customer data without obtaining prior specific or general written authorization from a customer.[24]

Source: IBM's EBA Cloud Compliance Certificate

[22] Whether a client is solely or jointly responsible is a fact-specific determination for which clients are responsible for obtaining professional legal and business advice.

[23] *Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance* ("Solvency II"), Article 13(28), p. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02009L0138-20140523.

[24] A list of the approved sub-outsourcers is set out and updated from time to time in the respective exhibit to the outsourcing agreement. Provided that the customer subscribes to notifications from a self-service notification portal, IBM will notify the customer in advance of any changes (including addition or replacement) to sub-outsourcers. The customer has the right to object to intended sub-outsourcing, or material changes thereof, within 30 days after IBM's notification of the intended change or addition, on the basis that such addition or change would cause the customer to violate applicable legal requirements; the customer's objection shall be in writing and include the customer's specific reasons for its objection and options to mitigate, if any. If the customer does not object within such period, the respective sub-outsourcer may be commissioned to deliver respective services including the processing of customer data. If the customer legitimately objects to the addition of a sub-outsourcer and IBM cannot reasonably accommodate the customer's objection, IBM will notify the customer. In that case, the customer may terminate the Cloud Service. Upon reasonable advance notice, the customer has the right to terminate the outsourcing agreement in the case of undue sub-outsourcing.

b) Outsourcing important or critical functions

Industries: Banking, Insurance, Securities
Primary Responsibility: Financial Institution

Regulatory Text:

Outsourcing of important or critical functions, in particular when the service provider is located outside the EU, creates specific risks both for institutions and payment institutions and for their competent authorities should be subject to appropriate oversight.

EBA, Background, para. 5 (p. 6).

Tip: *FIs should consider their dependency on outsourced functions to fulfil their client, regulatory and legal obligations, as mentioned in EBA, Title II, Section 4, paras. 29 & 31 below.*

Without prejudice to Article 274(3) of the Delegated Regulation, the undertaking's administrative, management or supervisory body ("AMSB") should ensure that any decision to outsource critical or important operational functions or activities to cloud service providers is based on a thorough risk assessment, including all relevant risks implied by the arrangement such as information and communication technology ("ICT"), business continuity, legal and compliance, concentration, other operational risks, and risks associated to the data migration and/or the implementation phase, where applicable.

EIOPA, Guideline 2, para. 17 (p. 5).

A firm should monitor the performance of activities, the security measures, and the adherence to agreed service levels by its CSPs. This monitoring should be risk-based, with a primary focus on the critical or important functions that have been outsourced.

ESMA, Guideline 1, para. 14, (p. 29).

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

IBM Cloud for Financial Services Supporting Activities & Controls:

FIs must demonstrate continued ownership and management of risk, even when that risk is associated with third and fourth parties storing critical data or performing key processes.

The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access.

c) Functions that are NOT considered outsourcing

Industries: Banking, Insurance, Securities
Primary Responsibility: Financial Institution

Regulatory Text:

Legally required functions performed by a service provider (e.g., statutory audit);

Market information services (e.g., Bloomberg, Moody's, Standard & Poor's);

Global **network infrastructures** (e.g., Visa, MasterCard);

Clearing and settlement arrangements between clearing houses, central counterparties and settlement institutions and their members;

Global **financial messaging infrastructures** subject to oversight by relevant authorities

Correspondent banking services;

Services normally not performed by the financial institution (e.g., architecture advice; a legal opinion and representation in front of a court and administrative bodies; travel services; clerical services; gardening). [Emphasis added.]

EBA, Section 3, Outsourcing, para. 28 (p.26). The ESMA report executive summary, is aligned with the EBA Guidelines (para. 28)[25].

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

IBM Cloud for Financial Services Supporting Activities & Controls:

IBM Cloud has agreements with key third party suppliers with defined expectations and implements relationship management tools where applicable with third-party suppliers. These management mechanisms include frequent validation that the supplier is meeting the expectations as defined in agreements.

IBM Cloud supplier management processes are validated by external auditors as part of compliance with SOC and ISO 27001.

[25] *"ESMA has considered the EBA Guidelines on outsourcing arrangements, which have incorporated the EBA Recommendations on outsourcing to cloud service providers, and the EIOPA Guidelines on outsourcing to cloud service providers, with a view to ensure consistency between the three sets of guidelines."* ESMA, *Executive Summary*, p. 2. https://www.esma.europa.eu/sites/default/files/library/esma50-157-2403_cloud_guidelines.pdf.

In case of outsourcing of non-critical or non-important operational functions or activities, the undertaking should define the information to be recorded on the basis of the nature, scale, and complexity of the risks inherent in the services provided by the cloud service provider.

EIOPA, Guideline 5, Documentation Requirements, para. 25 (p. 7).

d) Critical or important functions

Industries: Banking, Insurance, Securities
Primary Responsibility: Financial Institution

Regulatory Text:

Institutions and payment institutions should always consider a function as critical or important in the following situations:

1. Where a defect or failure in its performance **would materially impair:**
   a. Their continuing compliance with the conditions of their authorisation[26] or its other obligations under Directive 2013/36/EU, Regulation (EU) No 575/2013, Directive 2014/65/EU, Directive 2015/2366, and Directive 2009/110/EC and their regulatory obligations;
   b. Their financial performance; or
   c. The **soundness or continuity** of their banking and payment services and activities;
2. When **operational tasks of internal control functions are outsourced,** unless an assessment concludes a failure to provide the outsourced function or the inappropriate provision of the outsourced function would not have an adverse impact on the effectiveness of the internal control function;
3. When the **outsourced function** would require authorization by a competent authority. [Emphasis added.]

EBA, Section 4, Critical or Important Functions, para. 29 (pp.26-27).

In para. 2 of the EIOPA Guidelines, what is considered critical or important function refers to Guideline 60 of the EIOPA *Guidelines on System of Governance*[27]:

"The undertaking should determine and document whether the outsourced function or activity is a critical or important function or activity on the basis of whether this function or activity is essential to the operation of the undertaking as it would be unable to deliver its services to policyholders without the function or activity."

EIOPA Guidelines on System of Governance (EIOPA-BoS-14/253), Section 11, Guideline 60 – Critical or important operational functions and activities (p. 21).[28]

Critical or important function means any function whose defect or failure in its performance would materially impair:

1. firm's compliance with its obligations under the applicable legislation;
2. a firm's financial performance; or
3. the soundness or the continuity of a firm's main services and activities. [Emphasis added.]

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

IBM Cloud for Financial Services Supporting Activities & Controls:

If IBM's proposed sub-outsourcing could have material adverse effects on the Cloud Services Agreement, or would lead to a material increase of risk, the customer is entitled to exercise its right to object to the sub-outsourcing and may be able to terminate the agreement.[29]

Source: IBM's EBA Cloud Compliance Certificate.

[26] See also, "Authorisations." https://www.bankingsupervision.europa.eu/banking/tasks/authorisation/html/index.en.html.

[27] "Moreover, these Guidelines build also on the guidance provided by EIOPA Guidelines on System of Governance (EIOPA-BoS-14/253)," para. 2, p. 3, https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/guidelines_on_outsourcing_to_cloud_service_providers_en.pdf.

[28] https://www.eiopa.europa.eu/content/guidelines-system-governance_en.

[29] A list of the approved sub-outsourcers is set out and updated from time to time in the respective exhibit to the outsourcing agreement. Provided that the customer subscribes to notifications from a self-service notification portal, IBM will notify the customer in advance of any changes (including addition or replacement) to sub-outsourcers. The customer has the right to object to intended sub-outsourcing, or material changes thereof, within 30 days after IBM's notification of the intended change or addition, on the basis that such addition or change would cause the customer to violate applicable legal requirements; the customer's objection shall be in writing and include the customer's specific reasons for its objection and options to mitigate, if any. If the customer does not object within such period, the respective sub-outsourcer may be commissioned to deliver respective services including the processing of customer data. If the customer legitimately objects to the addition of a sub-outsourcer and IBM cannot reasonably accommodate the customer's objection, IBM will notify the customer. In that case, the customer may terminate the Cloud Service. Upon reasonable advance notice, the customer has the right to terminate the outsourcing agreement in the case of undue sub-outsourcing.

ESMA, Annex III, Definitions, p. 25.

e) Core business lines and critical functions

Industries: Banking, Insurance
Primary Responsibility: Financial Institution

Regulatory Text:

Functions that are **necessary to perform activities of core business lines or critical functions** should be considered as critical or important functions for the purpose of these guidelines, unless the institution's assessment establishes that a failure to provide the outsourced function (or the inappropriate provision of the outsourced function) would not have an adverse impact on the operational continuity of the core business line or critical function. [Emphasis added.]

EBA, Section 4, Critical or Important Functions, para. 30 *(p. 27).*

In para. 2 of the EIOPA Guidelines, what core business lines and critical or important functions refers to Guideline 60 of the EIOPA Guidelines on System of Governance:[30]

> "The undertaking should determine and document whether the outsourced function or activity is a critical or important function or activity on the basis of whether this function or activity is essential to the operation of the undertaking as it would be unable to deliver its services to policyholders without the function or activity."[31]

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

IBM Cloud Framework for Financial Services Supporting Activities & Controls:

If IBM's proposed sub-outsourcing could have material adverse effects on the Cloud Services Agreement, or would lead to a material increase of risk, the customer is entitled to exercise its right to object to the sub-outsourcing and may be able to terminate the agreement.[32]

Source: IBM's EBA Cloud Compliance Certificate.

2. Determining whether the outsourced function or service is important or critical

Regulatory Provisions:
EBA Guidelines on Outsourcing Arrangements, February 25, 2019
Title II, Section 4, Critical or Important Functions

EIOPA Guidelines on Outsourcing to Cloud Service Providers, February 6, 2020
Guideline 7, Assessment of critical or important operational functions and activities

ESMA Guidelines on Outsourcing to Cloud Service Providers, December 18, 2020
Annex III, Section 1, Definitions

a) Factors to consider when assessing if an outsourced function is critical or important

Industries: Banking, Insurance, Securities
Primary Responsibility: Financial Institution

Regulatory Text:

a. Whether the outsourcing arrangement is directly connected to the provision of banking activities or payment services for which they are authorized;

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 on their:

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

IBM Cloud for Financial Services Supporting Activities & Controls:

IBM maintains written corporate directives that establish a framework for business continuity standards, including roles and responsibilities for oversight of compliance with such standards. Each business unit assigns an executive business continuity management sponsor who is responsible for providing corporate

[30] "Moreover, these Guidelines build also on the guidance provided by EIOPA Guidelines on System of Governance (EIOPA-BoS-14/253)," para. 2, p. 3, https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/guidelines_on_outsourcing_to_cloud_service_providers_en.pdf.

[31] EIOPA Guidelines on System of Governance (EIOPA-BoS-14/253), Section 11, Guideline 60 – Critical or important operational functions and activities, p. 21, https://www.eiopa.europa.eu/content/guidelines-system-governance_en.

[32] A list of the approved sub-outsourcers is set out and updated from time to time in the respective exhibit to the outsourcing agreement. Provided that the customer subscribes to notifications from a self-service notification portal, IBM will notify the customer in advance of any changes (including addition or replacement) to sub-outsourcers. The customer has the right to object to intended sub-outsourcing, or material changes thereof, within 30 days after IBM's notification of the intended change or addition, on the basis that such addition or change would cause the customer to violate applicable legal requirements; the customer's objection shall be in writing and include the customer's specific reasons for its objection and options to mitigate, if any. If the customer does not object within such period, the respective sub-outsourcer may be commissioned to deliver respective services including the processing of customer data. If the customer legitimately objects to the addition of a sub-outsourcer and IBM cannot reasonably accommodate the customer's objection, IBM will notify the customer. In that case, the customer may terminate the Cloud Service. Upon reasonable advance notice, the customer has the right to terminate the outsourcing agreement in the case of undue sub-outsourcing.

a. Short- and long-term financial resilience and viability;

b. Business continuity and operational resilience;

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

d. Reputational risks;

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

c. Potential impact of the outsourcing arrangement on their ability to:

a. Identify, monitor, and manage all risks;

b. Comply with all legal and regulatory requirements;

c. Conduct appropriate audits regarding the outsourced function;

d. The potential impact on the services provided to its clients;

e. All outsourcing arrangements, the financial institution'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 area affected;

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

The ability to transfer the proposed outsourcing arrangement to another service provider

The ability to reintegrate the outsourced function into the institution or payment institution, if necessary or desirable;

The protection of data and the potential impact of a confidentiality breach or failure to ensure data availability and integrity on the institution or payment institution and its clients, including but not limited to compliance with Regulation (EU) 2016/679 (General Data Protection Regulation). [*Emphasis added*].

EBA, Section 4, Critical or Important Functions, para. 31 (pp. 27-29).

Prior to entering into any outsourcing arrangement with cloud service providers, the undertaking should assess if the cloud outsourcing arrangement relates to an operational function or activity that is critical or important. In performing such an assessment, where relevant, the undertaking should consider whether the arrangement has the potential to become critical or important in the future. The undertaking should also reassess the criticality or importance of the operational function or activity previously outsourced to cloud service providers, if the nature, scale, and complexity of the risks inherent in the agreement materially changes.

In the assessment, the undertaking should take into account, together with the outcome of the risk assessment, at least, the following factors:

a. the potential impact of any material disruption to the outsourced operational function or activity or failure of the cloud service provider to provide the services at the agreed service levels on the undertaking's:
   i. continuous compliance with its regulatory obligations;
   ii. short and long-term financial and solvency resilience and viability;
   iii. business continuity and operational resilience;
   iv. operational risk, including conduct, ICT, and legal risks;
   v. reputational risks.

b. the potential impact of the cloud outsourcing arrangement on the ability of the undertaking to:
   i. identify, monitor, and manage all relevant risks;
   ii. comply with all legal and regulatory requirements;
   iii. conduct appropriate audits regarding the operational function or activity outsourced.

guidance to the business unit, and for overseeing the business unit's enactment of and compliance with IBM's business continuity directives, policies, and implementation guidelines.

IBM relies on third-party auditors to validate our compliance with many global, industry and regional standards including, but not limited to ISO 27001, SOC, PCI.[33]

Security and privacy terms for IBM services are provided in the base contractual agreement, including Data Security and Privacy Principles for IBM Cloud Services, the Data Processing Addendum for personal data subject to the EU General Data Protection Regulation (GDPR), the Brazilian General Data Protection Law (Lei Geral de Proteção de Dados Pessoais or LGPD), and other applicable regulations/legislation, and relevant Transaction Documents, such as the GDPR/LGPD Data Exhibits, Service Description, order document, and associated attachments.

Customers are responsible for determining whether a standard IBM service is suitable for their use and are required to review and agree with the terms of the relevant IBM service, including its stated security and privacy measures, prior to use.

[33] https://www.ibm.com/cloud/compliance.

c. the undertaking's (and/or group's where applicable) aggregated exposure to the same cloud service provider and the potential cumulative impact of outsourcing arrangements in the same business area;
d. the size and complexity of any undertaking's business areas affected by the cloud outsourcing arrangement;
e. the ability, if necessary or desirable, to transfer the proposed cloud outsourcing arrangement to another cloud service provider or reintegrate the services ("substitutability");
f. the protection of personal and non-personal data and the potential impact on the undertaking, policyholders or other relevant subjects of a confidentiality breach or failure to ensure data availability and integrity based on inter alia Regulation (EU) 2016/6797. The undertaking should particularly take into consideration data that is business secret and/or sensitive (for example, policyholders' health data).

EIOPA Guideline 7, paras. 28-29 (pp. 8-9).

Critical or important function means any function whose defect or failure in its performance would materially impair:

1. firm's compliance with its obligations under the applicable legislation;
2. a firm's financial performance; or
3. the soundness or the continuity of a firm's main services and activities;

ESMA, Annex III, Definitions (pp. 25-27).

3. FIs remain responsible when outsourcing function or services

Regulatory Provisions:
EBA Guidelines on Outsourcing Arrangements (EBA) (February 25, 2019)
EBA: Title III, Section 6, Sound Governance Arrangements and Outsourcing

EIOPA Guidelines on Outsourcing to Cloud Service Providers (EIOPA) (February 6, 2020)
EIOPA: Guideline 2, General principles of governance for cloud outsourcing;
Guideline 14, Monitoring and oversight of cloud outsourcing arrangements

ESMA Guidelines on Outsourcing to Cloud Service Providers (ESMA) (December 18, 2020)
ESMA: Guideline 1, Governance, Oversight and Documentation

a) FIs remain responsible

Industries: Banking, Insurance, Securities
Primary Responsibility: Financial Institution / IBM

Regulatory Text:

Institutions and payment institutions remain fully responsible and accountable for complying with all of their regulatory obligations, including the ability to oversee the outsourcing of critical or important functions.

EBA, Section 6, Sound Governance Arrangements and Outsourcing, para. 35 (p.30).

The undertaking should monitor, on a regular basis, the performance of activities, the security measures, and the adherence to agreed service level by their cloud service providers on a risk-based approach. The main focus should be on the cloud outsourcing of critical and important operational functions.
In order to do so, the undertaking should set up monitoring and oversight mechanisms, which should take into account, where feasible and appropriate, the presence of sub-outsourcing of critical or important operational functions or a part thereof.

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

IBM Cloud for Financial Services Supporting Activities & Controls:

IBM's shared responsibility model is designed to support customers in meeting this and related requirements around the need for clearly defined responsibilities and accountability.[34]

[34] https://cloud.ibm.com/docs/overview?topic=overview-shared-responsibilities.

EIOPA, Guideline 14, paras. 51-52 A firm should establish a cloud outsourcing oversight function or designate senior staff members who are directly accountable to the management body and responsible for managing and overseeing the risks of cloud outsourcing arrangements. *ESMA Guideline 1, para. 13(c) (p.28).*	IBM remains responsible for the obligations under the applicable agreement, even if IBM uses a sub-contractor. IBM does not sub-outsource customer data without obtaining prior specific or general written authorization from a customer.[35] Further details are addressed in IBM's EBA Cloud Compliance Certificate.
b) FI Management responsibilities **Industries:** Banking, Insurance, Securities **Primary Responsibility:** Financial Institution **Regulatory Text:** The management body is at all times fully responsible and accountable for at least: a. Ensuring that the institution or payment institution meets on an ongoing basis the conditions with which it must comply to remain authorized, including any conditions imposed by the competent authority; b. The internal organization of the institution or the payment institution; c. The identification, assessment, and management of conflicts of interest; d. The setting of the institution's or payment institution's strategies and policies (e.g., the business model, the risk appetite, the risk management framework); e. Overseeing the day-to-day management of the institution or payment institution, 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. *EBA, Section 6, Sound Governance Arrangements and Outsourcing,* para. 36 (p.30). Without prejudice to Article 274(3) of the Delegated Regulation, the undertaking's administrative, management or supervisory body ("AMSB") should ensure that any decision to outsource critical or important operational functions or activities to cloud service providers is based on a thorough risk assessment, including all relevant risks implied by the arrangement such as information and communication technology ("ICT"), business continuity, legal and compliance, concentration, other operational risks, and risks associated to the data migration and/or the implementation phase, where applicable. *EIOPA, Guideline 2, para. 17 (p. 5).* When complying with this guideline, firms should take into account the nature, scale, and complexity of their business, including in terms of risk for the financial system, and the risks inherent to the outsourced functions and make sure that their management body has the relevant technical skills to understand the risks involved in cloud outsourcing arrangements. Small and less complex firms should at least ensure a clear division of tasks and responsibilities for the management and oversight of cloud outsourcing arrangements. *ESMA, Guideline 1, para. 13(c)* (p.28). A firm should monitor the performance of activities, the security measures, and the adherence to agreed service levels by its CSPs. This monitoring should be risk-based, with a primary focus on the critical or important functions that have been outsourced. *ESMA, Guideline 1, para. 14* (p. 29).	**IBM Cloud Framework for Financial Services Focus Area(s):** **Focused Risk Management and Compliance** **Advanced Data Protection** **Unified Infrastructure Security & Resiliency** **Enhanced Authentication and Access Management** **IBM Cloud for Financial Services Supporting Activities & Controls:** IBM has made significant investments in cloud data centers around the world to give customers the flexibility to decide where to store and process their data. These decisions generally should be driven by customer choice rather than government mandate. [36] IBM follows industry standard best practices and complies with all contractual obligations to document APIs and clearly communicates them with customers. Service Level Agreements (SLAs) and capacity expectations capture offering expectations, policies, and procedures. IBM Cloud maintains capacity and resource planning in alignment with ISO27001 and these efforts are validated by external auditors to confirm IBM Cloud is ISO 27001 compliant. Capacity management is also ensured for IBM Cloud Disaster Recovery. IBM Cloud Console provides usage reports for all services and resource the Customer consumes. All IBM Cloud services actively manage vulnerabilities by regularly scanning all public/private endpoints using best in class commercial vulnerability scanners, to the timeframes defined in applicable policy. These scans include both network, application, and system layer scans. Services remediate any vulnerabilities found according to timescales in applicable policy. All IBM Cloud services comply with a set of security requirements across the development lifecycle including, but not limited to, static code scanning,

[35] A list of the approved sub-outsourcers is set out and updated from time to time in the respective exhibit to the outsourcing agreement. Provided that the customer subscribes to notifications from a self-service notification portal, IBM will notify the customer in advance of any changes (including addition or replacement) to sub-outsourcers. The customer has the right to object to intended sub-outsourcing, or material changes thereof, within 30 days after IBM's notification of the intended change or addition, on the basis that such addition or change would cause the customer to violate applicable legal requirements; the customer's objection shall be in writing and include the customer's specific reasons for its objection and options to mitigate, if any. If the customer does not object within such period, the respective sub-outsourcer may be commissioned to deliver respective services including the processing of customer data. If the customer legitimately objects to the addition of a sub-outsourcer and IBM cannot reasonably accommodate the customer's objection, IBM will notify the customer. In that case, the customer may terminate the Cloud Service. Upon reasonable advance notice, the customer has the right to terminate the outsourcing agreement in the case of undue sub-outsourcing.

[36] *Location, Location, Location: The Importance of Security and Privacy of Your Data in the Cloud.* https://www.ibm.com/downloads/cas/6YZRYLAJ.

dynamic scanning of APIs and UIs, build dependency checking and enrollment with IBM PSIRT to receive notification on all relevant vulnerabilities.

Teams must either have an automated process to block code deployment in case of security test failures such as static scans or have a traceable process for signing off security tests such as dynamic scans.

Anti-malware detection and prevention services are maintained by the corporate CISO office; endpoints are internally managed and are required to comply with corporate security requirements; diagnostic tools check for core endpoint security features, which automatically correct issues, or notifies workstation users of noncompliance.

These checks include: hard drive security (password protection or full disk encryption); screen saver; antivirus; firewall; database encryption, if required based on data sensitivity; endpoint user account passwords; operating system pack level and security patch currency; as well as checks to verify certain features are not enabled such as file sharing capabilities. When non-compliance issues are identified, email notifications are sent.

At least annually, policies and procedures are reviewed and updated to ensure that the most current policy is available to company employees via dissemination by management for viewing and commitment. In addition to these annual reviews and updates, policies are updated ad hoc with administrative and content changes.

Internally IBM Cloud key management controls are maintained through frequent internal audits and are validated by external auditors through assessments including but not limited to FedRAMP, ISO 27001, SOC, PCI, and HIPAA.

IBM Cloud engages third party groups on at least an annual basis to conduct penetration testing on each service as prescribed by industry best practices.

Continuing assessments of IBM’s controls and control enhancements are conducted to maintain a high degree of confidentiality, integrity, and availability. These assessments include audits conducted by external audit groups, internal control testing conducted, and various security monitoring processes in place.

Reports from both the annual assessments and quarterly internal control testing are provided to leadership

For customers that need a more involved monitoring service, IBM Cloud Monitoring[37] is a managed enterprise grade monitoring service that provides operational visibility into the performance and health of applications, services, and infrastructure. It offers administrators, DevOps teams and developers full stack telemetry with advanced features to monitor and troubleshoot, define alerts, and design custom dashboards.

[37] https://www.ibm.com/cloud/cloud-monitoring.

	IBM secure engineering and privacy by design standards and guidelines dictate multiple scanning techniques be used before the promotion of code into production. These include static and dynamic scans, penetration tests, threat modeling, manual code reviews, and other techniques. The change request process provides a high level of control for all software development activities.[38] The IBM services Information Security Management System (ISMS) and Privacy Information Management System (PIMS) control framework captures the legal, regulatory, and contractual obligations of the IBM services. The ISMS/PIMS team works with an industry and regulatory compliance group that helps define applicable requirements to the offerings that are incorporated into the ISMS/PIMS. This would include any requirements specific to data handling. IBM offers the following business continuity and resiliency services. IBM Cloud Backup is a full-featured, automated, agent-based backup and recovery system managed through the IBM Cloud Backup WebCC browser utility. Using multivault technologies, you can more securely back up your data between IBM Cloud servers in one or more IBM Cloud data centers, worldwide.[39] IBM Cloud Disaster Recovery Solutions provide comprehensive disaster recovery services, including health monitoring as well as continuous replication of applications, infrastructure, data, and cloud systems.[40] IBM's Cyber Resilience Services help protect platform configurations and applications data by using air-gapped protection, immutable storage, and anomaly detection while orchestrating rapid and reliable recovery at the disaster recover (DR) site.[41] IBM Cloud Resiliency Orchestration provides disaster recovery monitoring, reporting, testing, and workflow automation capabilities of complex hybrid environments in a scalable, easier-to-use solution built on industry standards.[42] This service combines automation and analytics for faster, more cost-effective disaster recovery (DR) that helps keep daily business operations running and proactively avoids disruptions that lead to lost revenue, brand damage and dissatisfied customers.[43]

[38] IBM Security and Privacy by Design, https://www.ibm.com/security/secure-engineering/.

[39] https://www.ibm.com/cloud/backup

[40] https://www.ibm.com/cloud/disaster-recovery

[41] https://www.ibm.com/services/business-continuity/cyber-resilience

[42] https://www.ibm.com/products/disaster-recovery-orchestration

[43] https://www.ibm.com/cloud/disaster-recovery

4. FI responsibilities when outsourcing functions or services

Regulatory Provisions:

EBA Guidelines on Outsourcing Arrangements, February 25, 2019
Title III, Section 6, Sound Governance Arrangements and Outsourcing

EIOPA Guidelines on Outsourcing to Cloud Service Providers, February 6, 2020
Guideline 14, Monitoring and oversight of cloud outsourcing arrangements

ESMA Guidelines on Outsourcing to Cloud Service Providers, December 18, 2020
Guideline 1, Governance, Oversight and Documentation;
Guideline 2, Pre-outsourcing Analysis and Due Diligence

a) FI oversight responsibilities

Industries: Banking, Insurance, Securities
Primary Responsibility: Financial Institution

Regulatory Text:

When outsourcing, institutions and payment institutions should at least ensure that:

1. They can take and implement decisions related to their business activities and critical or important functions, including with regard to those that have been outsourced;
2. They maintain the orderliness of the conduct of their business and the banking and payment services they provide;
3. The risks related to current and planned outsourcing arrangements are adequately identified, assessed, managed, and mitigated, including risks related to ICT a technology (fintech);
4. Appropriate confidentiality arrangements are in place regarding data and other information;
5. An appropriate flow of relevant information with service providers is maintained;
6. With regard to the outsourcing of critical or important functions, they are able to undertake at least one of the following actions, within an appropriate time frame:
    a. transfer the function to alternative service providers;
    b. reintegrate the function; or
    c. discontinue the business activities that are depending on the function.
7. 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 the GDPR.
   [Emphasis added.]

EBA, Section 6, Sound Governance Arrangements and Outsourcing, para. 40 (p. 32).

In order to ensure the adequate monitoring and oversight of their cloud outsourcing arrangements, undertakings should employ enough resources with adequate skills and knowledge to monitor the services outsourced to the cloud. The undertaking's personnel in charge of these activities should have both ICT and business knowledge as deemed necessary.

EIOPA Guideline 14, para. 54 (p. 14).

A firm should allocate sufficient resources to ensure compliance with these guidelines and all of the legal requirements applicable to its cloud outsourcing arrangements.

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

IBM Cloud for Financial Services Supporting Activities & Controls:

IBM Cloud engages third party groups on at least an annual basis to conduct penetration testing on each service as prescribed by industry best practices.

IBM Cloud has agreements with key third party suppliers with defined expectations and implements relationship management tools where applicable with third-party suppliers. These management mechanisms include frequent validation that the supplier is meeting the expectations as defined in agreements.

IBM Cloud supplier management processes are validated by external auditors as part of compliance with SOC and ISO27001.

All IBM Cloud services actively manage vulnerabilities by scanning all public endpoints using best in class commercial vulnerability scanners, to the timeframes defined in applicable policy. These activities include both the virtualization technologies and all virtual machines and containers deployed on those virtualization technologies.

All IBM Security & Privacy by Design processes such as threat assessments and penetration tests also apply to the virtualization technologies.

IBM maintains corporate policies and standards which support data and system security, privacy, confidentiality, integrity, and availability.

Each IBM service implements standard controls and processes in compliance with IBM's corporate policies, and is subject to accredited third-party validation against standards, such as ISO 27001, ISO 27017, ISO 27018, SSAE SOC 2, FedRAMP, HIPAA, and PCI-DSS, to the extent stated in the relevant service description.

Compliance with legal, regulatory, and contractual obligations is mandatory for all IBM services and checks for adherence to such obligations are performed regularly. Revisions to the associated policies, controls, and terms are incorporated as required and appropriate.

ESMA Guideline 1, para. 13(b) (p. 28)

When assessing the suitability of the CSP, a firm should ensure that the CSP has the business reputation, the skills, the resources (including human, IT and financial), the organizational structure and, if applicable, the relevant authorization(s) or registration(s) to perform the critical or important function in a reliable and professional manner and to meet its obligations over the duration of the cloud outsourcing arrangement.

ESMA Guideline 2, para. 22 (p. 31).

IBM's Security and Compliance Center provides a single dashboard to help monitor security and compliance postures.[44]

IBM's OpenShift Container Platform delivers portability and compatibility across multiple cloud providers, including private on-premises cloud, the IBM Cloud, and other cloud service providers.

IBM's cloud data centers around the globe give customers the flexibility to decide where to store and process their data.[45] The determination of where data are stored and processed should be driven by the customer.

IBM's information security controls and supplier management processes are validated by external auditors as part of its compliance with SOC and ISO 27001.[46]

A third-party assessor performs periodic, rigorous assessments of the IBM Cloud for Financial Services against the IBM Cloud Framework for Financial Services. These assessments are more extensive than typical system and organization controls SOC 2 audits or SOC 3 executive summaries of SOC 2 reports. They benefit customers by offering more visibility and transparency into the control effectiveness.[47]

5. FIs should approve, regularly review, and update a written outsourcing policy, and ensure its implementation

Regulatory Provisions:
EBA Guidelines on Outsourcing Arrangements, February 25, 2019
Title III, Section 7, Outsourcing Policy;
Section 11, Documentation Requirements

EIOPA Guidelines on Outsourcing to Cloud Service Providers, February 6, 2020
Guideline 3, Update of the Outsourcing Written Policy

ESMA Guidelines on Outsourcing to Cloud Service Providers, December 18, 2020
Guideline 4, Information security

a) Outsourcing policy coverage

Industries: Banking, Insurance, Securities
Primary Responsibility: Financial Institution

Regulatory Text:

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

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

IBM Cloud for Financial Services Supporting Activities & Controls:

The ISMS/PIMS supplier management controls, coupled with IBM's standard global procurement process, helps maintain that all vendors, contractors, and suppliers of services are vetted, sign binding

[44] https://www.ibm.com/cloud/security-and-compliance-center.
[45] https://www.ibm.com/blogs/think/fi-fi/2020/10/20/cloud-portability-and-interoperability/.
[46] https://www.ibm.com/cloud/compliance.
[47] IBM Cloud Framework for Financial Services, https://www.ibm.com/downloads/cas/JYB6MQRB.

a. The responsibilities of the management body, including its involvement, as appropriate, in the decision-making on outsourcing of critical or important functions;

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

c. The planning of outsourcing arrangements, including:

    a. The definition of business requirements regarding outsourcing arrangements;
    b. The criteria, including those referred to in Section 4, and processes for identifying critical or important functions;
    c. Risk identification, assessment, and management in accordance with Section 12.2;
    d. Due diligence checks on prospective service providers, including the measures required under Section 12.3;
    e. Procedures for the identification, assessment, management, and mitigation of potential conflicts of interest, in accordance with Section 8;
    f. Business continuity planning in accordance with Section 9;
    g. The approval process of new outsourcing arrangements.

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

    a. The ongoing assessment of the service provider's performance in line with Section 14;
    b. The procedures for being notified and responding to changes to an outsourcing arrangement or service provider (e.g., to its financial position, organizational or ownership structures, sub-outsourcing);
    c. The independent review and audit of compliance with legal and regulatory requirements and policies;
    d. The renewal processes;

e. The documentation and record-keeping, taking into account the requirements in Section 11;

f. The exit strategies and termination processes, including a requirement for a documented exit plan for each critical or important function to be outsourced where such an exit is considered possible taking into account possible service interruptions or the unexpected termination of an outsourcing agreement.

EBA, Section 7, Outsourcing Policy, para. 42 (pp.33-34).

As part of their risk management framework, institutions and payment institutions should maintain an updated register of information on all outsourcing arrangements at the institution and, where applicable, at sub-consolidated and consolidated levels, as set out in Section 2, 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 law, institutions should maintain the documentation of ended outsourcing arrangements within the register and the supporting documentation for an appropriate period.

EBA, Section 11, Documentation Requirements, para. 52

In case of outsourcing to cloud service providers, the undertaking should update the written outsourcing policy (for example, by reviewing it, adding a separate appendix, or developing new dedicated policies) and the other relevant internal policies (for

non-disclosure agreements and require adherence to all technical and organizational measures (TOMs), and security requirements.

IBM's legal teams review and approve all contractual documents, including:

- Supplier and Customer Contracts;
- Service Descriptions (SD);
- Offering Data Sheets (DS);
- Service Level Agreements (SLA);
- Cloud Services Agreement;
- Data Security & Privacy Principles;
- Data Processing Addendum (w/ EU Standard Contractual Clauses).

IBM maintains a rigorous program of internal audits, quarterly KPI control testing, and semi-annual external audits. The audit program is part of the executive management approval and review process.

Offerings are certified annually to ISO 27001 or SAE SOC 2 or both, or as stated in the relevant Transaction Document and Service Description. IBM provides certifications, attestations, audit reports, and other supporting materials to its customers, which verify and demonstrate IBM's adherence to its legal and contractual obligations.

All third-party requirements are implemented to align with ISO 27001, which are reviewed by external auditors to confirm compliance.

IBM's own security controls form part of its compliance audits for its SOC 2 and ISO 27001 assessments.

IBM's clear documentation on the technical and organizational measures used in the IBM Cloud around data security and privacy helps financial institutions perform their risk assessment when deploying to the cloud. [48]

Customers are able to monitor their applications, containers, hosts, networks, and metrics for insights into complex environments using IBM Cloud Monitoring with Sysdig.[49]

IBM employees must complete a screening process, including but not limited to, background checks, Non-Disclosure Agreement acknowledgement, and Business Conduct Guidelines acknowledgement.

SOC 1 and SOC 2 audit reports are available by contacting an IBM representative.[50] The IBM SOC 3[51] report, is a public version of the SOC 2 Type 2.

[48] *IBM Cloud's European Banking Authority (EBA) Compliance Brief.* https://www.ibm.com/downloads/cas/KRGNBGBD.
[49] https://www.ibm.com/us-en/marketplace/sysdig-monitor.
[50] https://www.ibm.com/account/reg/us-en/signup?formid=MAIL-wcp.
[51] https://www.ibm.com/cloud/compliance/global.

example, information security), taking into account cloud outsourcing specificities at least in the following areas:

a. the roles and responsibilities of the undertaking's functions involved, in particular AMSB, and the functions responsible for ICT, information security, compliance, risk management and internal audit;

b. the processes and reporting procedures required for the approval, implementation, monitoring, management, and renewal, where applicable, of cloud outsourcing arrangements related to critical or important operational functions or activities;

c. the oversight of the cloud services proportionate to the nature, scale, and complexity of risks inherent in the services provided, including (i) risk assessment of cloud outsourcing arrangements and due diligence on cloud service providers, including the frequency of the risk assessment; (ii) monitoring and management controls (for example, verification of the service level agreement); (iii) security standards and controls;

d. with regard to cloud outsourcing of critical or important operational functions or activities, a reference should be made to the contractual requirements as described in Guideline 10;

e. documentation requirements and written notification to the supervisory authority regarding cloud outsourcing of critical or important operational functions or activities;

f. with regard to each cloud outsourcing arrangement that covers critical or important operational functions or activities, a requirement for a documented and, where appropriate, sufficiently tested 'exit strategy' that is proportionate to the nature, scale, and complexity of the risks inherent in services provided. The exit strategy may involve a range of termination processes, including but not necessarily limited to, discontinuing, reintegrating, or transferring the services included in the cloud outsourcing arrangement.

EIOPA Guideline 3, para. 20(a-f) (pp. 5-6).

A firm should set information security requirements in its internal policies and procedures and within the cloud outsourcing written agreement and monitor compliance with these requirements on an ongoing basis, including to protect confidential, personal, or otherwise sensitive data. These requirements should be proportionate to the nature, scale, and complexity of the function that the firm outsources to the CSP and the risks inherent to this function.

ESMA, Guideline 4, para. 29 (p. 31).

6. The rights and obligation of the FI and its service provider should clearly be allocated in a written agreement

Regulatory Provisions:
EBA Guidelines on Outsourcing Arrangements, February 25, 2019
Title IV, Section 13, Contractual Phase

EIOPA Guidelines on Outsourcing to Cloud Service Providers, February 6, 2020
Guideline 3, Update of the outsourcing written policy;
Guideline 10, Contractual Requirements

ESMA Guidelines on Outsourcing to Cloud Service Providers, December 18, 2020
Guideline 3, Key Contractual Elements

a) Rights and obligations

Industries: Banking, Insurance, Securities
Primary Responsibility: Financial Institution / IBM

Regulatory Text:

The rights and obligations of the institution, the payment institution and the service provider should be clearly allocated in a written agreement.

EBA, Section 13, Contractual Phase, para. 74 (p.44).

The respective rights and obligations of the undertaking and of the cloud service provider should be clearly allocated and set out in a written agreement.

EIOPA, Guideline 10, para. 36 (p. 10).

The respective rights and obligations of a firm and its CSP should be clearly set out in a written agreement.

ESMA, Guideline 3, para. 26 (p. 32).

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

IBM Cloud for Financial Services Supporting Activities & Controls:

IBM has implemented standardized clauses that align with EBA requirements.

To assist our FI customers in complying with the EBA Guidelines, IBM developed an “IBM EBA Cloud Compliance Certificate”[52] to address the EBA Guidelines’ contractual requirements in its Outsourcing Guidelines. Structured to provide full transparency into how IBM Cloud services and contracts align, the IBM EBA Cloud Compliance Certificate makes it easier for customers to contract with IBM.[53]

The security and privacy of data in our cloud is paramount, which is why our Data Security and Privacy Principles for IBM Cloud Services[54] apply to generally available cloud services.

[52] https://www.ibm.com/downloads/cas/KRGNBGBD.
[53] *Note, IBM’s EBA Cloud Compliance Certificate was created by IBM to assist its customers in understanding how IBM Cloud services and contracts align with the EBA Outsourcing Guidelines and is not affiliated with the EBA in anyway.*
[54] https://www-03.ibm.com/software/sla/sladb.nsf/pdf/7745WW2/$file/Z126-7745-WW-2_05-2017_en_US.pdf.

b) Outsourcing agreement coverage for critical or important functions

Industries: Banking, Insurance, Securities
Primary Responsibility: Financial Institution / IBM

Regulatory Text:

The outsourcing agreement for critical or important functions should set out at least:

a. A clear description of the outsourced function to be provided;
b. The start date and end date, where applicable, of the agreement and the notice periods for the service provider and the institution or payment institution;
c. The governing law of the agreement;
d. The parties' financial obligations;
e. **Whether the sub-outsourcing of a critical or important function, or material parts** thereof, is permitted and, if so, the conditions specified in Section 13.1 that the sub- outsourcing is subject to;
f. 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 institution or payment institution if the service provider proposes to change the location(s);
g. Where relevant, provisions regarding the accessibility, availability, integrity, privacy, and safety of relevant data, as specified in Section 13.2;
h. The right of the institution or payment institution to monitor the service provider's performance on an ongoing basis;
i. The **agreed service levels, which should include precise quantitative and qualitative performance targets** for the outsourced function to allow for timely monitoring so that appropriate corrective action can be taken without undue delay if the agreed service levels are not met;
j. The **reporting obligations of the service provider** to the financial institution or payment institution, 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;
k. Whether the service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;
l. The requirements to implement and **test business contingency plans**;
m. Provisions that ensure that the data that are owned by the financial institution or payment institution can be accessed in the case of the insolvency, resolution, or discontinuation of business operations of the service provider;
n. The obligation of the **service provider to cooperate with the competent authorities** and resolution authorities of the institution or payment institution, including other persons appointed by them;
o. For institutions, **a clear reference to the national resolution authority's powers**, especially to Articles 68 and 71 of Directive 2014/59/EU (BRRD), and in particular a description of the 'substantive obligations' of the contract in the sense of Article 68 of that Directive;
p. The unrestricted **right** of financial institutions, payment institutions and competent authorities **to inspect and audit the service provider** with regard to, in particular, the critical or important outsourced function, as specified in Section 13.3;
q. **Termination rights**, as specified in Section 13.4. [*Emphasis added.*]

EBA, Section 13, Contractual Phase, para. 75 (pp. 44-45).

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

IBM Cloud for Financial Services Supporting Activities & Controls:

FIs must demonstrate continued ownership and management of risk, even when that risk is associated with third and fourth parties storing critical data or performing key processes.

IBM identifies which part of the Cloud Services is being sub-outsourced (see applicable DPA Exhibit). IBM is responsible for the obligations under the applicable agreement, even if IBM uses a sub-contractor, and will have appropriate agreements in place to enable IBM to meet its obligations for a Cloud Service.

IBM agrees not to sub-outsource customer data without obtaining prior specific or general written authorization from the customer. A list of the approved sub-outsourcers is set out and updated from time to time in the respective exhibit to the outsourcing agreement. Provided that the customer subscribes to notifications from a self-service notification portal, IBM will notify the customer in advance of any changes (including addition or replacement) to sub-outsourcers.[55]

If IBM's proposed sub-outsourcing could have material adverse effects on the applicable agreement, or would lead to a material increase of risk, the customer is entitled to exercise its right to object to the sub-outsourcing and may be able to terminate the agreement.

Source: IBM's EBA Cloud Compliance Certificate.

Upon termination or expiration of the Agreement IBM will either delete or return Client Personal Data in its possession as set out in the respective DPA Exhibit, unless otherwise required by applicable law.

IBM will not disclose Client Personal Data to any third party, unless authorized by the client or required by law.

If a government or Supervisory Authority demands access to Client Personal Data, IBM will notify client prior to disclosure, unless such notification is prohibited by law.

IBM will notify a client without undue delay upon confirmation of a security incident that is known or reasonably suspected by IBM to affect client. IBM will provide the client with reasonably requested

[55] The customer has the right to object to intended sub-outsourcing, or material changes thereof, within 30 days after IBM's notification of the intended change or addition, on the basis that such addition or change would cause the customer to violate applicable legal requirements; the customer's objection shall be in writing and include the customer's specific reasons for its objection and options to mitigate, if any. If the customer does not object within such period, the respective sub-outsourcer may be commissioned to deliver respective services including the processing of customer data. If the customer legitimately objects to the addition of a sub-outsourcer and IBM cannot reasonably accommodate the customer's objection, IBM will notify the customer. In that case, the customer may terminate the Cloud Service. Upon reasonable advance notice, the customer has the right to terminate the outsourcing agreement in the case of undue sub-outsourcing.

With regard to each cloud outsourcing arrangement that covers critical or important operational functions or activities, a requirement for a documented and, where appropriate, sufficiently tested ‘exit strategy’ that is proportionate to the nature, scale, and complexity of the risks inherent in services provided. The exit strategy may involve a range of termination processes, including but not necessarily limited to, discontinuing, reintegrating, or transferring the services included in the cloud outsourcing arrangement.

EIOPA, Guideline 3, para. 20(f) (p. 6).
Without prejudice to the requirements defined in Article 274 of the Delegated Regulation, in case of outsourcing of critical or important operational functions or activities to a cloud service provider, the written agreement between the undertaking and the cloud service provider should set out:

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

b. the start date and end date, where applicable, of the agreement and the notice periods for the cloud service provider and for the undertaking; the court jurisdiction and the governing law of the agreement;

c. the parties’ financial obligations;

d. whether the sub-outsourcing of a critical or important operational function or activity (or material parts thereof) is permitted, and, if so, the conditions to which the significant sub-outsourcing is subject to (see Guideline 13);

e. the location(s) (i.e., regions or countries) where relevant data will be stored and processed (location of data centers), and the conditions to be met, including a requirement to notify the undertaking if the service provider proposes to change the location(s);

f. provisions regarding the accessibility, availability, integrity, confidentiality, privacy, and safety of relevant data, taking into account the specifications of Guideline 12;

g. the right for the undertaking to monitor the cloud service provider’s performance on a regular basis;

h. the agreed service levels which should include precise quantitative and qualitative performance targets in order to allow for timely monitoring so that appropriate corrective actions can be taken without undue delay if agreed service levels are not met;

i. the reporting obligations of the cloud service provider to the undertaking, including, as appropriate, the obligations to submit reports relevant for the undertaking’s security function and key functions, such as reports of the internal audit function of the cloud service provider;

j. whether the cloud service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;

k. the requirements to implement and test business contingency plans;

l. the requirement for the cloud service provider to grant the undertaking, its supervisory authorities and any other person appointed by the undertaking or the supervisory authorities, the following:

    i. full access to all relevant business premises (head offices and operation centers), 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 cloud service provider’s external auditors (“access rights”);

    ii. unrestricted rights of inspection and auditing related to the cloud outsourcing arrangement (“audit rights”), to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements;

m. provisions to ensure that the data owned by the undertaking can be promptly recovered by the undertaking in case of the insolvency, resolution, or discontinuation of business operations of the cloud service provider.

EIOPA, Guideline 10, para. 37 (p. 10).

information about the security incident and the status of any IBM remediation and restoration activities. [56]

For cloud data encryption Hyper Protect Crypto Services is a dedicated key management services and hardware security module (HSM) - using FIPS 140-2 Level 4 certified hardware. The same state of the art cryptographic technology relied upon by banks and financial services.[57]

Notably, the U.S. Federal Financial Institutions Examination Council (FFIEC), an interagency composed of five U.S. banking regulators, directly regulates certain aspects of IBM’s business relating to the financial industry (e.g., business continuity and resilience services, security services).

[56] *Data Security and Privacy Principles for IBM Cloud Services.* https://www-03.ibm.com/software/sla/sladb.nsf/pdf/7745WW2/$file/Z126-7745-WW-2_05-2017_en_US.pdf.

[57] https://www.ibm.com/cloud/hyper-protect-crypto.

In case of outsourcing of critical or important functions, the written agreement should include at least:

a. a clear description of the outsourced function;

b. the start date and end date, where applicable, of the agreement and the notice periods for the CSP and for the firm;

c. the governing law of the agreement and, if any, the choice of jurisdiction;

d. the firm's and the CSP's financial obligations;

e. whether sub-outsourcing is permitted, and, if so, under which conditions, having regard to Guideline 7;

f. the location(s) (namely regions or countries) where the outsourced function will be provided and where data will be processed and stored, and the conditions to be met, including a requirement to notify the firm if the CSP proposes to change the location(s);

g. provisions regarding information security and protection of personal data, having regard to Guideline 4;

h. the right for the firm to monitor the CSP's performance under the cloud outsourcing arrangement on a regular basis, having regard to Guideline 6;

i. the agreed service levels, which should include, quantitative and qualitative performance targets in order to allow for timely monitoring so that appropriate corrective actions can be taken without undue delay if agreed service levels are not met;

j. the reporting obligations of the CSP to the firm and, as appropriate, the obligations to submit reports relevant for the firm's security function and key functions, such as reports prepared by the internal audit function of the CSP;

k. provisions regarding the management of incidents by the CSP, including the obligation for the CSP to report to the firm without undue delay incidents that have affected the operation of the firm's contracted service;

l. whether the CSP should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;

m. the requirements for the CSP to implement and test business continuity and disaster recovery plans;

n. the requirement for the CSP to grant the firm, its competent authorities and any other person appointed by the firm or the competent authorities the right to access ('access rights') and to inspect ('audit rights') the relevant information, premises, systems, and devices of the CSP to the extent necessary to monitor the CSP's performance under the cloud outsourcing arrangement and its compliance with the applicable regulatory and contractual requirements, having regard to Guideline 6;

o. provisions to ensure that the data that the CSP processes or stores on behalf of the firm can be accessed, recovered, and returned to the firm as needed, having regard to Guideline 5.

ESMA, Guideline 3, para. 28 (pp. 32-33).

7. The outsourcing agreement should specify whether or not sub-outsourcing of critical or important functions (or material parts) is permitted

Regulatory Provisions:
EBA Guidelines on Outsourcing Arrangements, February 25, 2019
Title III, Section 13.1, Sub-Outsourcing of Critical or Important Functions

EIOPA Guidelines on Outsourcing to Cloud Service Providers, February 6, 2020
Guideline 10, Contractual Requirements;
Guideline 13, Sub-outsourcing of critical or important operational functions or activities

ESMA Guidelines on Outsourcing to Cloud Service Providers, December 18, 2020
Guideline 2, Pre-outsourcing analysis and due diligence;
Guideline 3, Key Contractual Elements; Guideline 7, Sub-Outsourcing

a) Outsourcing agreement – FI/IBM

Industries: Banking, Insurance, Securities
Primary Responsibility: Financial Institution / IBM

Regulatory Text:

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

EBA, Section 13.1, Sub-Outsourcing of Critical or Important Functions, para. 76 (p.45).

The respective rights and obligations of the undertaking and of the cloud service provider should be clearly allocated and set out in a written agreement.

EIOPA, Guideline 10, para. 36 (p. 10).

In case of outsourcing of critical or important functions, the written agreement should include at least whether sub-outsourcing is permitted, and, if so, under which conditions.

ESMA Guideline 3, para. 28(e) (p. 32).

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

IBM Cloud for Financial Services Supporting Activities & Controls:

IBM remains responsible for the obligations under the Cloud Services Agreement, even if IBM uses a sub-contractor. IBM does not sub-outsource client data without obtaining prior specific or general written authorization from a client. However, IBM may use personnel and resources in locations worldwide, including contractors, to support the delivery of IBM Cloud Services.

Sub-outsourcing of critical or important functions, or material parts is permitted, subject to the IBM EBA Cloud Compliance Certificate and IBM's agreement with the customer.[58]

Source: IBM's EBA Cloud Compliance Certificate

b) Sub-outsourcing critical or important functions

Industries: Banking, Insurance, Securities
Primary Responsibility: Financial Institution

Regulatory Text:

If sub-outsourcing of critical or important functions is permitted, institutions and payment institutions 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.

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

IBM Cloud for Financial Services Supporting Activities & Controls:

The sub-outsourcing of critical or important functions, or material parts is permitted, subject to the terms of the EBA Certificate and to any terms agreed to between the parties within the Agreement.[59]

Source: IBM's EBA Cloud Compliance Certificate

[58] A list of the approved sub-outsourcers is set out and updated from time to time in the respective exhibit to the outsourcing agreement. Provided that the customer subscribes to notifications from a self-service notification portal, IBM will notify the customer in advance of any changes (including addition or replacement) to sub-outsourcers. The customer has the right to object to intended sub-outsourcing, or material changes thereof, within 30 days after IBM's notification of the intended change or addition, on the basis that such addition or change would cause the customer to violate applicable legal requirements; the customer's objection shall be in writing and include the customer's specific reasons for its objection and options to mitigate, if any. If the customer does not object within such period, the respective sub-outsourcer may be commissioned to deliver respective services including the processing of customer data. If the customer legitimately objects to the addition of a sub-outsourcer and IBM cannot reasonably accommodate the customer's objection, IBM will notify the customer. In that case, the customer may terminate the Cloud Service. Upon reasonable advance notice, the customer has the right to terminate the outsourcing agreement in the case of undue sub-outsourcing.

[59] A list of the approved sub-outsourcers is set out and updated from time to time in the respective exhibit to the outsourcing agreement. Provided that the customer subscribes to notifications from a self-service notification portal, IBM will notify the customer in advance of any changes (including addition or replacement) to sub-outsourcers. The customer has the right to object to intended sub-outsourcing, or material changes thereof, within 30 days after IBM's notification of the intended change or addition, on the basis that such addition or change would cause the customer to violate applicable legal requirements; the customer's objection shall be in writing and include the customer's specific reasons for its objection and options to mitigate, if any. If the customer does not object within such period, the respective sub-outsourcer may be commissioned to deliver respective services including the processing of customer data. If the customer legitimately objects to the addition of a sub-outsourcer and IBM cannot reasonably accommodate the customer's objection, IBM will notify the customer. In that case, the customer may terminate the Cloud Service. Upon reasonable advance notice, the customer has the right to terminate the outsourcing agreement in the case of undue sub-outsourcing.

EBA, Section 13.1, Sub-Outsourcing of Critical or Important Functions, para. 77 (p.45).

Without prejudice to the requirements defined in Article 274 of the Delegated Regulation, in case of outsourcing of critical or important operational functions or activities to a cloud service provider, the written agreement between the undertaking and the cloud service provider should set out whether the sub-outsourcing of a critical or important operational function or activity (or material parts thereof) is permitted, and, if so, the conditions to which the significant sub-outsourcing is subject to (see Guideline 13).

EIOPA, Guideline 10, Contractual Requirements, para. 37(e) (p. 10).

. . . [I]n case of sub-outsourcing, the additional risks that may arise if the sub-outsourcer is located in a third country or a different country from the CSP and, in case of a sub-outsourcing chain, any additional risk which may arise, including in relation to the absence of a direct contract between the firm and the sub-outsourcer performing the outsourced function.

ESMA, Guideline 2, Pre-Outsourcing Analysis and Due Diligence, para. 21(a)(vi) (p. 31).

c) Agreement coverage if sub-outsourcing is permitted

Industries: Banking, Insurance, Securities
Primary Responsibility: Financial Institution / IBM

Regulatory Text:

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 institution or payment institution are continuously met
d. require the service provider to obtain prior specific or general written authorization from the institution or payment institution before sub-outsourcing data;
e. include an obligation of the service provider to inform the financial institution or payment institution 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 institution or payment institution 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 institution or payment institution has the right to object to intended sub-outsourcing, or material changes thereof, or that explicit approval is required;
g. ensure that the institution or payment institution 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 institution or payment institution or where the service provider sub-outsources without notifying the institution or payment institution.

EBA, Section 13.1, Sub-Outsourcing of Critical or Important Functions, para. 78 (pp. 45-46).

If sub-outsourcing of critical or important operational functions (or a part thereof) is permitted, the cloud outsourcing agreement between the undertaking and the cloud service provider should:

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

IBM Cloud for Financial Services Supporting Activities & Controls:

IBM remains responsible for the obligations under the Cloud Services Agreement, even if IBM uses a sub-contractor. IBM agrees not to sub-outsource customer data without obtaining prior specific or general written authorization from the customer.

Upon reasonable advance notice, a customer has the right to terminate the Cloud Agreement.

A list of the approved sub-outsourcers is set out and updated from time to time in the respective exhibit to the outsourcing agreement. Provided that the customer subscribes to notifications from a self-service notification portal available at mycloudservices.ibm.com, IBM will notify the customer in advance of any changes (including addition or replacement) to sub-outsourcers.

Source: IBM's EBA Cloud Compliance Certificate.

a. specify any types of activities that are excluded from potential sub-outsourcing;
b. indicate the conditions to be complied with in case of sub-outsourcing (for example, that the sub-outsourcer will also fully comply with the relevant obligations of the cloud service provider). These obligations include the audit and access rights and the security of data and systems;
c. indicate that the cloud service provider retains full accountability and oversight for the services sub-outsourced;
d. include an obligation for the cloud service provider to inform the undertaking of any planned significant changes to the sub-contractors or the sub-outsourced services that might affect the ability of the service provider to meet its obligations under the cloud outsourcing agreement. The notification period for those changes should allow the undertaking, at least, to carry out a risk assessment of the effects of the proposed changes before the actual change in the sub-outsourcers or the sub-outsourced services comes into effect;
e. ensure, in cases where a cloud service provider plan changes to a sub-outsourcer or sub-outsourced services that would have an adverse effect on the risk assessment of the agreed services, that the undertaking has the right to object to such changes and/or the right to terminate and exit the contract.

EIOPA, Guideline 13, para. 50 (p. 13).

If sub-outsourcing of critical or important functions (or material parts thereof) is permitted, the cloud outsourcing written agreement between the firm and the CSP should:

a. specify any part or aspect of the outsourced function that are excluded from potential sub-outsourcing;
b. indicate the conditions to be complied with in case of sub-outsourcing;
c. specify that the CSP remains accountable and is obliged to oversee those services that it has sub-outsourced to ensure that all contractual obligations between the CSP and the firm are continuously met;
d. include an obligation for the CSP to notify the firm of any intended sub-outsourcing, or material changes thereof, in particular where that might affect the ability of the CSP to meet its obligations under the cloud outsourcing arrangement with the firm. The notification period set in the written agreement should allow the firm sufficient time at least to carry out a risk assessment of the proposed sub-outsourcing or material changes thereof and to object to or explicitly approve them, as indicated in point (e) below;
e. ensure that the firm has the right to object to the intended sub-outsourcing, or material changes thereof, or that explicit approval is required before the proposed sub-outsourcing or material changes come into effect;
f. ensure that the firm has the contractual right to terminate the cloud outsourcing arrangement with the CSP in case it objects to the proposed sub-outsourcing or material changes thereof and in case of undue sub-outsourcing (for example, where the CSP proceeds with the sub-outsourcing without notifying the firm or it seriously infringes the conditions of the sub-outsourcing specified in the outsourcing agreement).

ESMA, Guideline 7, Sub-Outsourcing, para. 42 (p. 37).

d) Sub-contractor requirements

Industries: Banking, Insurance, Securities
Primary Responsibility: Financial Institution / IBM

Regulatory Text:

Institutions and payment institutions should agree to sub-outsourcing only if the sub-contractor undertakes to:

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

IBM Cloud for Financial Services Supporting Activities & Controls:

IBM requires that sub-contractors delivering sub-outsourcing services to IBM comply with all applicable laws, regulatory requirements and obligations as

a. Comply with all applicable laws, regulatory requirements, and contractual obligations; and b. Grant the institution, payment institution and competent authority the same contractual rights of access and audit as those granted by the service provider. *EBA, Section 13.1, Sub-Outsourcing of Critical or Important Functions,* para. 79 (p. 46). If sub-outsourcing of critical or important operational functions (or a part thereof) is permitted, the cloud outsourcing agreement between the undertaking and the cloud service provider should: indicate that the cloud service provider retains full accountability and oversight for the services sub-outsourced. *EIOPA, Guideline 13, para. 50 (p. 14).* The firm should ensure that the CSP appropriately oversees the sub-outsourcer. *ESMA, Guideline 7, Sub-Outsourcing, para. 43* (p. 37).	contractually agreed between the sub-outsourcer and IBM.[60] In accordance with IBM's Data Processing Addendum,[61] IBM will allow for, and contribute to, audits, including inspections, conducted by the customer or another auditor mandated by the customer.

[60] *IBM's EBA Compliance Brief*. https://www.ibm.com/downloads/cas/KRGNBGBD.

[61] https://www.ibm.com/support/customer/csol/terms/.

8. FIs must ensure that the service provider appropriately oversees the sub-service providers

Regulatory Provisions:
EBA Guidelines on Outsourcing Arrangements, February 25, 2019
Title III, Section 13.1, Sub-Outsourcing of Critical or Important Functions

EIOPA Guidelines on Outsourcing to Cloud Service Providers, February 6, 2020
Guideline 14, Monitoring and Oversight of Cloud Outsourcing Arrangements

ESMA Guidelines on Outsourcing to Cloud Service Providers, December 18, 2020
Guideline 7, Sub-Outsourcing

a) Appropriate oversight by service provider

Industries: Banking, Insurance, Securities
Primary Responsibility: Financial Institution / IBM

Regulatory Text:

Institution and payment institutions should ensure that the service provider **appropriately oversees the sub-service providers**, in line with the policy defined by the [institution]. 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 ... the institution or payment institution **should exercise its right to object to the sub-outsourcing**, if such a right was agreed, and/or terminate the contract. [Emphasis added.]

EBA, Section 13.1, Sub-Outsourcing of Critical or Important Functions, para. 80 (p.46).

In order to do so, the undertaking should set up monitoring and oversight mechanisms, which should take into account, where feasible and appropriate, the presence of sub-outsourcing of critical or important operational functions or a part thereof.

EIOPA, Guideline 14, Monitoring and Oversight of Cloud Outsourcing Arrangements, para. 52 (p. 14).

The firm should ensure that the CSP appropriately oversees the sub-outsourcer.

ESMA, Guideline 7, Sub-Outsourcing, para. 43 (p. 37).

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

IBM Cloud for Financial Services Supporting Activities & Controls:

IBM agrees not to sub-outsource customer data without obtaining prior specific or general written authorization from the customer. A list of the approved sub-outsourcers is set out and updated from time to time in the respective exhibit to the outsourcing agreement. Provided that the customer subscribes to notifications from a self-service notification portal, IBM will notify the customer in advance of any changes (including addition or replacement) to sub-outsourcers.[62]

The sub-outsourcing of critical or important functions, or material parts thereof, is permitted, subject to the terms of this EBA Certificate and subject to any terms agreed between the parties within the Cloud Agreement.

IBM will appropriately oversee the sub-service providers. If the sub-outsourcing proposed could have material adverse effects on the Cloud Agreement or would lead to a material increase of risk, a customer is entitled to exercise its right to object to the sub-outsourcing and/or terminate the Cloud Agreement in accordance with the Agreement as referenced in IBM's EBA Cloud Compliance Certificate.

[62] The customer has the right to object to intended sub-outsourcing, or material changes thereof, within 30 days after IBM's notification of the intended change or addition, on the basis that such addition or change would cause the customer to violate applicable legal requirements; the customer's objection shall be in writing and include the customer's specific reasons for its objection and options to mitigate, if any. If the customer does not object within such period, the respective sub-outsourcer may be commissioned to deliver respective services including the processing of customer data. If the customer legitimately objects to the addition of a sub-outsourcer and IBM cannot reasonably accommodate the customer's objection, IBM will notify the customer. In that case, the customer may terminate the Cloud Service. Upon reasonable advance notice, the customer has the right to terminate the outsourcing agreement in the case of undue sub-outsourcing.

9. Joint Advice on ICT risk management requirement in the EU financial sector

Regulatory Provisions:
EBA Guidelines on ICT and Security Risk Management (EBA ICT)
November 29, 2019

EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (EBA SREP)
November 9, 2017

Joint Advice of the European Supervisory Authorities (ESAs) to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector
April 10, 2019

In the Joint Advice on ICT risk management requirements in the EU financial sector, the ESAs state:

> "Centered their analysis of current legislation on overall operational resilience, including ICT and cyber governance and security. While operational risk requirements are generally in place in the sectoral legislation, there is typically a lack of explicit references to ICT and cybersecurity risk. As such the ESAs believe that, across their respective sectors, it should be articulated clearly that every relevant entity should be subject to general requirements on governance of ICT, including cybersecurity, to ensure safe provision of regulated services. Such consistency will help set appropriate supervisory expectations, aid good governance and in turn promote greater ICT security and cybersecurity."[63]

In view of the aforementioned imbalance in the specificity of these requirements between the EBA, EIOPA and ESMA, it has been decided to only include the most comprehensive and specific guidance in deeper detail in the tables below: the EBA Guidelines on ICT and Security Risk Management.

10. FIs should ensure there is adequate internal governance and an internal control framework for their ICT and security risks

Regulatory Provisions:
EBA Guidelines on ICT and Security Risk Management (EBA ICT), November 29, 2019
Section 3.2, Governance and Strategy

EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (EBA SREP), November 9, 2017
Title 2, Assessment of Institutions' Governance and Strategy on ICT;
Title 3, Assessment of Institutions' ICT Risks Exposures and Controls

a) Internal governance and control framework

Industries: Banking
Primary Responsibility: Financial Institution

Regulatory Text:

The management body should ensure that financial institutions have adequate internal governance and internal control framework in place for their ICT and security risks. The management body should set clear roles and responsibilities for ICT functions, information security risk management, and business continuity, including those for the management body and its committees.

EBA ICT, Section 3.2.1(2), Governance, (p.14).

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

IBM Cloud for Financial Services Supporting Activities & Controls:

The IBM Cloud Framework for Financial Services includes IBM's infrastructure and platform information security and privacy policies and risk assessment processes, which are aligned with ISO 27001 and ISO 31000.[64]

IBM Cloud for Financial Services[65] aligns framework obligations globally with NIST 800-53, "Security and

[63] Joint Advice of the European Supervisory Authorities (EIOPA, EBA, ESMA) to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector, p. 4 (April 10, 2019). https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf.
[64] https://www.ibm.com/cloud/compliance/global.
[65] https://www.promontory.com/our-expertise/article/5f99a1355d477f0f98b6d4c3.

Competent authorities should assess whether the institution's general governance and internal control framework duly cover the ICT systems and related risks and if the management body adequately addresses and manages these aspects, as ICT is integral to the proper functioning of an institution. *EBA SREP, Title 2, Section 2.1, General Principles, para. 20* (p. 8).	Privacy Controls for Information Systems and Organizations." IBM Cloud also provides third-party audit reports, certifications,[66] and responsibility matrixes to customers. These documents are comprised of information pertaining to IBM Cloud's core controls, processes, and procedures.
b) ICT strategy **Industries:** Banking **Primary Responsibility:** Financial Institution **Regulatory Text:** The management body has overall accountability for setting, approving, and overseeing the implementation of their 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. *EBA ICT, Section 3.2.1(4), Governance,* (p. 14). Under this section competent authorities should assess whether the institution has an ICT strategy in place: that is subject to adequate oversight from the institution's management body; that is consistent with the business strategy, particularly for keeping its ICT up-to-date and planning or implementing important and complex ICT changes; and that supports the institution's business model. *EBA SREP, Section 2.2, ICT Strategy, para. 25* (pp. 8-9).	**IBM Cloud Framework for Financial Services Focus Area(s):** **Focused Risk Management and Compliance** **IBM Cloud for Financial Services Supporting Activities & Controls:** Data quality and integrity are assessed and validated using multiple third-party auditing firms to conduct audits including, but not limited to SOC, ISO 27001, ISO 27017, ISO 27018, and PCI.[67]
c) What should your ICT strategy do? **Industries:** Banking **Primary Responsibility:** Financial Institution **Regulatory Text:** The ICT strategy should be aligned with financial institutions' overall business strategy and define: a. How financial institutions' ICT should evolve to effectively support and participate in their business strategy, including the evolution of the organizational structure, ICT system changes and key dependencies with third parties; b. The planned strategy and evolution of the architecture of ICT, including third-party dependencies; and c. Clear information security objectives, focusing on the ICT systems, services, staff, and processes. EBA ICT, Section 3.2.2(5), Strategy, (pp. 14-15). Competent authorities should assess whether the institution has a framework in place, proportionate to the nature, scale, and complexity of its ICT activities, for the preparation and development of the institution's ICT strategy. In conducting this assessment competent authorities should take into account whether: a. The senior management of the business line(s) is adequately involved in the definition of the institution's strategic ICT priorities and that, in turn,	**IBM Cloud Framework for Financial Services Focus Area(s):** **Focused Risk Management and Compliance** **IBM Cloud for Financial Services Supporting Activities & Controls:** IBM works with customers to implement a programmatic approach to security by helping them: • Manage continuous security and compliance monitoring and threat protection; • Advise on security and compliance obligations; • Build applications based on secure software development lifecycle processes and practices; and • Migrate and modernize infrastructure and applications based on secure environment and security best practices.

[66] https://www.ibm.com/cloud/compliance.
[67] https://www.ibm.com/cloud/compliance/global.

senior management of the ICT function is aware of the development, design and initiation of major business strategies and initiatives to ensure the continued alignment between ICT systems, ICT services and the ICT function (i.e. those responsible for the management and deployment of these systems and services), and the institution's business strategy, and that ICT are effectively up-dated; b. The ICT strategy is documented and supported by concrete implementation plans, in particular regarding the important milestones and resource planning (including financial and human resources) to ensure that they are realistic and enable the delivery of the ICT strategy; c. The institution periodically updates its ICT strategy, in particular when changing the business strategy, to ensure continued alignment between the ICT and business medium-term to long-term objectives, plans and activities; and g. the institution's management body approves the ICT strategy, implementation plans and monitors its implementation. EBA SREP, Section 2.2.1, ICT Strategy Development and Adequacy, para. 26 (p. 9).	
d) ICT contract terms **Industries:** Banking **Primary Responsibility:** Financial Institution / IBM **Regulatory Text:** To ensure continuity of ICT services and ICT systems, financial institutions should ensure that contracts and service level agreements with providers (outsourcing providers, group entities, or third-party providers) include the following. a. Appropriate and proportionate information security-related objectives and measures (e.g., minimum cybersecurity requirements; data life cycle specifications; requirements for data encryption, network security and security monitoring processes, and the location of data centers); b. Operational and security incident handling procedures including escalation and reporting. *EBA ICT, Section 3.2.3(8), Use of Third-Party Providers*, (p. 15).	**IBM Cloud Framework for Financial Services Focus Area(s):** **Focused Risk Management and Compliance** **Active Monitoring and Response** **IBM Cloud for Financial Services Supporting Activities & Controls:** In accordance IBM Data Security and Privacy Principles for IBM Cloud Services the measures[68] implemented and maintained by IBM within each IBM Cloud Service will be subject to annual certification of compliance with ISO 27001 or SSAE SOC 2, or both, unless stated otherwise in an IBM Services Document. IBM's Cloud Compliance Programs[69] provides programs, and certifications on a global, government, industry, and regional basis. IBM maintains and follows documented incident response policies consistent with NIST guidelines, or equivalent industry standards, for computer security incident handling and will comply with the data breach notification terms of the applicable written contract between IBM and the customer. IBM Security offers the industry's first mobile Security Operations Center,[70] capable of traveling onsite for cybersecurity training, preparedness and response.
e) Monitor compliance of third-party providers **Industries:** Banking **Primary Responsibility:** Financial Institution / IBM	**IBM Cloud Framework for Financial Services Focus Area(s):** **Focused Risk Management and Compliance** **Active Monitoring and Response**

[68] https://www.ibm.com/support/customer/csol/terms/.

[69] https://www.ibm.com/cloud/compliance.

[70] https://www.ibm.com/security/services/managed-security-services/command-center-mobile.

Regulatory Text:

Financial institutions should monitor and seek assurance on the level of compliance of these providers with the security objectives, measures, and performance targets of the financial institution.

EBA ICT, Section 3.2.3(9), Use of Third-Party Providers, (p.15).

...[C]ompetent authorities should assess whether the institution has an effective framework in place for identifying, understanding, and measuring ICT outsourcing risk, and in particular, controls and a control environment in place for mitigating risks related to material outsourced ICT services that are commensurate with the size, activities and the ICT risk profile of the institution and include:

a. an assessment of the impact of the ICT outsourcing on the risk management of the institution related to the use of service providers (e.g., cloud service providers) and their services during the procurement process that is documented and is taken into account by senior management or the management body for the decision to outsource the services or not. The institution should review the ICT risk management policies and the ICT controls and control environment of the service provider to ensure that they meet the institution's internal risk management objectives and risk appetite. This review should be periodically updated during the contractual outsourcing period, taking into account the characteristics of the outsourced services;

b. a monitoring of the ICT risks of the outsourced services during the contractual outsourcing period as part of the institution's risk management, that feeds into the institution's ICT risk management reporting (e.g., business continuity reporting, security reporting);

c. a monitoring and comparison of the received service levels with the contractually agreed upon service levels which should form part of the outsourcing contract or service level agreement (SLA); and

d. adequate staff, resources, and competences to monitor and manage the ICT risks from the outsourced services.

EBA SREP, Section 3.3.4 €, Controls for Managing Material ICT Outsourcing Risks, para. 60 (p. 22).

IBM Cloud for Financial Services Supporting Activities & Controls:

To aid in preventing compliance drift, automation using IBM Cloud Security and Compliance Center[71] and associated reporting provides banks with the level of insights that they need to meet their compliance requirements much faster and more efficiently.

IBM Cloud Monitoring[72] is a managed enterprise grade monitoring service that provides operational visibility into the performance and health of applications, services, and infrastructure. It offers administrators, DevOps teams and developers full stack telemetry with advanced features to monitor and troubleshoot, define alerts, and design custom dashboards.

f) Criticality of business functions – FI

Industries: Banking
Primary Responsibility: Financial Institution / IBM

Regulatory Text:
Financial institutions should classify the identified business functions, supporting processes and information assets referred to in paragraphs 15 and 16 in terms of criticality.

To define the criticality of these identified business functions, supporting processes and information assets, financial institutions should, at a minimum, consider the confidentiality, integrity, and availability requirements. There should be clearly assigned accountability and responsibility for the information assets.

EBA ICT, Section 3.3.3(17) & (18), Classification and Risk Assessment, (p.17).

If the institution's ICT strategy requires the implementation of important and complex ICT changes, or changes with material implications for the institution's business model, competent authorities should assess whether the institution has a control framework in place, appropriate to its size, its ICT activities as well as the level of change activities, to support the effective implementation of the institution's ICT strategy.

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

Advanced Data Protection

Enhanced Authentication & Access Management

Automated Application & Workload Protection

Active Monitoring & Response

IBM Cloud for Financial Services Supporting Activities & Controls:

In order to help FIs classify outsourced functions to determine the appropriate level of governance, IBM provides a comprehensive set of suggested secure-design patterns.[73]

[71] https://www.ibm.com/cloud/blog/announcements/new-in-the-security-and-compliance-center-control-where-your-data-is-stored-and-processed.
[72] https://www.ibm.com/cloud/cloud-monitoring.
[73] IBM Cloud's EBA Compliance Brief at 5. https://www.ibm.com/downloads/cas/KRGNBGBD.

EBA SREP, Section 2.2.2, ICT Strategy Implementation, para. 27 (p. 9).

These design patterns contain robust capabilities to safeguard a FI’s data and systems to host demanding workloads, and include:

- identity and access management;
- data security;
- application security;
- secure DevOps;
- network security;
- security monitoring and intelligence; and
- physical security.[74]

IBM supports financial institutions in tailoring their own security assessments to best serve their business objectives.

g) Risk assessment and classification of risk

Industries: Banking
Primary Responsibility: Financial Institution / IBM

Regulatory Text:

This risk assessment should be carried out and documented annually or at shorte intervals if required. Such risk assessments should also be performed on any major changes in infrastructure, processes or procedures affecting the business functions, supporting processes or information assets, and consequently the current risk assessment of financial institutions should be updated.

EBA ICT, Section 3.3.3(20), Classification and Risk Assessment, (p. 17).

Competent authorities should assess whether the institution has properly identified, assessed, and mitigated its ICT risks. This process should be part of the operational risk management framework and congruent to the approach applying to operational risk.

EBA SREP, Section 3.1, General Consideration, para. 35 (p. 12).

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

IBM Cloud for Financial Services Supporting Activities & Controls:

As stated in IBM’s Data Security and Privacy Principles,[75] IBM performs security and privacy risk assessment at least annually. IBM also performs security testing and vulnerability assessments at least annually.

h) Audit for ICT and security risks

Industries: Banking
Primary Responsibility: Financial Institution / IBM

Regulatory Text:

A financial institution’s governance, systems and processes for its ICT and security risks should be audited on a periodic basis by auditors with sufficient knowledge, skills and expertise in ICT and security risks and in payments (for PSPs) to provide independent assurance of their effectiveness to the management body.

The auditors should be independent within or from the financial institution. The frequency and focus of such audits should be commensurate with the relevant ICT and security risks.

EBA ICT, Section 3.3.6, Audit, para. 25 (pp. 17-18).

IBM Cloud Framework for Financial Services (Focus Areas):

Focused Risk Management and Compliance

IBM Cloud for Financial Services Supporting Activities & Controls:

The IBM Cloud Framework for Financial Services maintains adherence to global, industry and regional standards (e.g., ISO, SOC, PCI), as evidenced through third-party certifications and attestations. Further details can be found at IBM Cloud Compliance Programs.[76]

A periodic audit is conducted by an independent third-party assessor on the IBM Cloud for Financial Services against the IBM Cloud Framework for Financial Services.

[74] *IBM Cloud’s European Banking Authority (EBA) Compliance Brief. https://www.ibm.com/downloads/cas/KRGNBGBD.*
[75] https://www.ibm.com/support/customer/csol/terms/.
[76] https://www.ibm.com/cloud/compliance/global.

Competent authorities should consider whether the Internal Audit Function is effective with regards to auditing the applicable ICT risk control framework, by reviewing whether:

a. the ICT risk control frameworks audited with the required quality, depth, and frequency and commensurate with the size, activities, and the ICT risk profile of the institution
b. the audit plan includes audits on the critical ICT risks identified by the institution;
c. the important ICT audit findings, including agreed actions, are reported to the management body; and
d. ICT audit findings, including agreed actions, are followed up and progress reports periodically reviewed by the senior management and/or the audit committee.

EBA SREP, Section 3.3.3, Internal Audit Coverage and Findings, para. 51 (pp. 16-17).

i) Approval of audit plan

Industries: Banking
Primary Responsibility: Financial Institution

Regulatory Text:

A financial institution's management body should approve the audit plan, including any ICT audits and any material modifications thereto. The audit plan and its execution, including the audit frequency, should reflect and be proportionate to the inherent ICT and security risks in the financial institution and should be updated regularly.

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

EBA ICT, Section 3.3.6, Audit, paras. 26 & 27 (p.18).

Competent authorities should consider whether the Internal Audit Function is effective with regards to auditing the applicable ICT risk control framework, by reviewing whether:

the audit plan includes audits on the critical ICT risks identified by the institution.

EBA SREP, Section 3.3.3, Internal Audit Coverage and Findings, para. 51(b) (p. 16)

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

IBM Cloud for Financial Services Supporting Activities & Controls:

IBM Cloud works with independent auditors and third-party organizations globally to meet the industry's most stringent guidelines, and to provide customers certain reports and certificates that they can leverage in their compliance efforts. These are available by contacting an IBM representative.[77] For further details visit IBM Cloud Compliance Programs.[78]

11. FIs should develop and document an information security policy that protects the confidentiality, integrity, and availability of their own and their customers' data and information

Regulatory Provisions:
EBA Guidelines on ICT and Security Risk Management (EBA ICT), November 29, 2019
Section 3.4, Information Security

a) Information Security Policy

Industries: Banking
Primary Responsibility: Financial Institution / IBM

Regulatory Text:

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

[77] https://www.ibm.com/cloud/compliance/global.
[78] https://www.ibm.com/cloud/compliance.

Financial institutions should develop and document an information security policy that should define the high-level principles and rules to protect the confidentiality, integrity and availability of financial institutions and their customers' data and information. . .The information security policy should be in line with the financial institution's information security objectives and based on the relevant results of the risk assessment process. The policy should be approved by the management body.

The policy should include a **description of the main roles and responsibilities of information security management**, and it should set out the requirements for staff and contractors, processes, and technology in relation to information security, recognizing that staff and contractors at all levels have responsibilities in ensuring financial institutions' information security.

The policy **should ensure the confidentiality, integrity, and availability** of a financial institution'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 to all staff and contractors of the financial institution. [Emphasis added.]

EBA ICT, Section 3.4.1, Information Security Policy, paras. 28 & 29, (p. 18).

IBM Cloud for Financial Services Supporting Activities & Controls:

As detailed in IBM's Data Security and Privacy Principles,[79] IBM reviews its IT security policies at least annually and amends such policies to maintain protection of IBM Services and content.

b) Mitigating ICT and security risks

Industries: Banking
Primary Responsibility: Financial Institution / IBM

Regulatory Text:

Based on the information security policy, FIs should establish and implement security measures to mitigate the ICT and security risks that they are exposed to. These measures should include:

a. Organization and governance
b. Logical security;
c. Physical security;
d. ICT operations security;
e. Security monitoring;
f. Information security reviews, assessment, and testing;
g. Information security training and awareness.

EBA ICT, Section 3.4.1, *Information Security Policy,* para. 30, (p. 18).

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

Enhanced Authentication & Access Management

IBM Cloud for Financial Services Supporting Activities & Controls:

Risk mitigation in the IBM Cloud includes, but is not limited to the following controls:

- Physical security is reviewed by periodic internal audits as well as by third-party audits such as FedRAMP, PCI, SOC, ISO 27001[80]
- Internally, IBM Cloud key management controls, maintained through frequent internal audits and validated by external auditors ISO27001, SOC, PCI, and HIPAA; and
- IBM Cloud identifies and maintains all requirements for access within the Logical Access Management Policy, which is based on least privilege and best practices.

IBM Supplier Security Risk Management ensures all third parties or suppliers have a risk assessment and have a set of security policies covering required security controls including segregation of duties, role-based access controls based on least privilege principles.

IBM also performs security and privacy risk assessments and penetration testing of the IBM Services at least annually.[81]

All IBM data centers have multiple layers of physical security, starting with access controls at the facility perimeter working inward to the data center building, the building lobby, the building interior, and controlled rooms within the data center building. These controlled rooms include the raised floor server rooms, network closets,

[79] https://www.ibm.com/support/customer/csol/terms/.
[80] https://www.ibm.com/cloud/compliance.
[81] *Data Security and Privacy Principles for IBM Cloud Services.*https://www-03.ibm.com/software/sla/sladb.nsf/pdf/7745WW2/$file/Z126-7745-WW-2_05-2017_en_US.pdf.

	electrical equipment and utility rooms, and the IBM Cloud staging areas.[82]
c) ICT operations security **Industries:** Banking **Primary Responsibility:** Financial Institution / IBM **Regulatory Text:** Financial institutions should implement procedures to prevent the occurrence of security issues in ICT systems and ICT services and should minimize their impact on ICT service delivery. These procedures should include the following measures: a. Identification of potential vulnerabilities, which should be evaluated and remediated by ensuring that software and firmware are up to date. b. Implementation of secure configuration baselines of all network components; c. Implementation of network segmentation, data loss prevention systems and the encryption of network traffic (in accordance with the data classification); d. Implementation of protection of endpoints including servers, workstations, and mobile devices; financial institutions should evaluate whether endpoints meet the security standards defined by them before they are granted access to the corporate network. e. Ensuring that mechanisms are in place to verify the integrity of software, firmware, and data; f. Encryption of data at rest and in transit (in accordance with the data classification). *EBA ICT, Section 3.4.4, ICT Operations Security, para. 36, (p. 20).*	**IBM Cloud Framework for Financial Services Focus Area(s):** **Focused Risk Management and Compliance** **Advanced Data Protection** **IBM Cloud for Financial Services Supporting Activities & Controls:** IBM Cloud does not access, modify, delete, or retain customer data outside the terms of the customer service agreement. IBM Cloud services allow Customers to manage their own encryption keys for data protection and cryptographic erase in order to meet their specific compliance initiatives” Hyper Protect Crypto Services is a dedicated key management services and hardware security module (HSM) - using FIPS 140-2 Level 4 certified hardware. The same state of the art cryptographic technology relied upon by banks and financial services.[83] IBM’s Zero Trust technologies[84] help customers discover and classify all assets in the cloud to establish the right protections and access controls.[85] IBM’s Cloud Security and Compliance Center[86] allows customers to implement controls that continuously assess security and compliance posture, apply rules to enforce configuration standardization across accounts, and gain insight into suspicious activity. IBM assists FI customers in establishing security policies and procedures to protect their sensitive workloads.
d) Information security reviews, assessment, and testing **Industries:** Banking **Primary Responsibility:** Financial Institution / IBM **Regulatory Text:** Financial institutions should perform a variety of information security reviews, assessments, and testing to ensure the effective identification of vulnerabilities in their ICT systems and ICT services. For instance, financial institutions may perform gap analysis against information security standards, compliance reviews, internal and external audits of the information systems, or physical security reviews. Financial institutions should also consider good practices, such as source code reviews, vulnerability assessments, penetration tests and red team exercises.	**IBM Cloud Framework for Financial Services Focus Area(s):** **Focused Risk Management and Compliance** **Unified Infrastructure Security & Resiliency** **IBM Cloud for Financial Services Supporting Activities & Controls:** All IBM Cloud services actively manage vulnerabilities by regularly scanning all public/private endpoints using best in class commercial vulnerability scanners, to the timeframes defined in applicable policy. These scans include both network, application, and system layer scans.

[82] https://www.ibm.com/cloud/architecture/.
[83] https://www.ibm.com/cloud/hyper-protect-crypto.
[84] https://www.ibm.com/topics/zero-trust.
[85] https://www.ibm.com/security/zero-trust/cloud.
[86] https://www.ibm.com/cloud/security-and-compliance-center.

Financial institutions should establish and implement an information security testing framework that validates the robustness and effectiveness of their information security measures and ensure that this framework considers threats and vulnerabilities, identified through threat monitoring and ICT and security risk assessment process.

The information security testing framework should ensure that tests:

a. Are carried out by independent testers with sufficient knowledge, skills, and expertise in testing information security measures and who are not involved in the development of the information security measures;

b. Include vulnerability scans and penetration tests (including threat-led penetration testing where necessary and appropriate) commensurate to the level of risk identified with the business processes and systems.

EBA ICT, Section 3.4.6, paras. 41 – 43, Information Security Reviews, Assessment and Testing (p. 21).

IBM Cloud employs logical segmentation in all networks and the hypervisors enforce compute isolation in Virtual Machines. These controls are tested regularly by penetration tests.

Trusted third-party organizations also conduct penetration testing, as prescribed by industry best practices on at least an annual basis.

As referenced in Data Security and Privacy Principles for IBM Cloud Services,[87] IBM maintains measures designed to assess, test, and apply security advisory patches to the IBM Services and associated systems, networks, applications, and underlying components within the scope of the IBM Services.

Zero Trust technologies[88] used to build in privacy and security at the beginning helps ensure anyone accessing customer data is validated with strong authentication. This continuous verification relies on context so that every user, every device, every connection must prove a legitimate need.

12. FIs should have documented and implemented processes and procedures approved by management, maintain an inventory of ICT assets, and establish and implement an incident and problem management process

Regulatory Provisions:
EBA Guidelines on ICT and Security Risk Management (EBA ICT), November 29, 2019
Section 3.5, ICT Operations Management

EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP), November 9, 2017
Title 2, Assessment of Institutions' Governance and Strategy on ICT

a) ICT documented and implemented processes and procedures

Industries: Banking
Primary Responsibility: Financial Institution / IBM

Regulatory Text:

Financial institutions should manage their ICT operations based on documented and implemented processes and procedures. . . that are approved by management. This set of documents should define how financial institutions operate, monitor, and control their ICT systems and services, including the documenting of critical ICT operations and should enable financial institutions to maintain up-to-date ICT asset inventory.

EBA 3.5, ICT Operations Management, para.50, (p. 22).

Competent authorities should assess whether the institution has a framework in place, proportionate to the nature, scale, and complexity of its ICT activities, for the preparation and development of the institution's ICT strategy. In conducting this assessment competent authorities should take into account whether:

IBM Cloud Framework for Financial Services Focus Area(s):

Enhanced Authentication & Access Management

IBM Cloud Framework for Financial Services Supporting Activities & Controls:

Logical access to systems is protected by authentication requirements and restricted to the least access necessary. Enforcement auditing is conducted by IBM's Security Operations Center.

IBM's Zero Trust technologies[89] help customers discover and classify all assets in the cloud to establish the right protections and access controls. By centralizing visibility and policy management, customers can maximize compliance while improving monitoring and reporting.

[87] https://www-03.ibm.com/software/sla/sladb.nsf/pdf/7745WW2/$file/Z126-7745-WW-2_05-2017_en_US.pdf.
[88] https://www.ibm.com/topics/zero-trust.
[89] https://www.ibm.com/topics/zero-trust.

> the ICT strategy is documented and supported by concrete implementation plans, in particular regarding the important milestones and resource planning (including financial and human resources) to ensure that they are realistic and enable the delivery of the ICT strategy…

EBA SREP, Section 2.2.1, *ICT Strategy Development and Adequacy, para. 26(b)* (p. 9).

b) Inventory ICT assets

Industries: Banking
Primary Responsibility: Financial Institution / IBM

Regulatory Text:

Financial institutions should maintain an up-to-date inventory of their ICT assets (including ICT systems, network devices, databases, etc.). The ICT asset inventory should store the configuration of the ICT assets and the links and interdependencies between the different ICT assets, to enable a proper configuration and change management process.

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

EBA ICT, Section 3.5, ICT Operations Management, paras.53 & 54 (p. 22-23).

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

Active Monitoring & Response

IBM Cloud for Financial Services Supporting Activities & Controls:

IBM Cloud’s incident response policy covers threat events, threat sources, and scenarios that may affect the security and availability of the company’s information assets. The Network Reliability Engineering (NRE) and Security Operations Center (SOC) are responsible for monitoring the IBM Cloud environment and manage the identification, response, and resolution of incidents.

Through the NRE and SOC, IBM Cloud provides 24/7 monitoring of data centers. IBM Cloud utilizes a variety of tools, in combination, to monitor, mitigate, and resolve potential issues. Each data center also has its own local Data Center Control Room (DCR), which is used to monitor and resolve potential issues locally.

IBM Cloud maintains an inventory of all assets including identified owners. All processes have a designated owner responsible for maintaining the process.

c) Establish and implement incident and problem management process

Industries: Banking
Primary Responsibility: Financial Institution / IBM

Regulatory Text:

Financial institutions should establish and implement an incident and problem management process to monitor and log operational and security ICT incidents and to enable financial institutions to continue or resume, in a timely manner, critical business functions and processes when disruptions occur.

Financial institutions should determine appropriate criteria and thresholds for classifying events as operational or security incidents, as set out in the ‘Definitions’ section of these guidelines, as well as early warning indicators that should serve as alerts to enable early detection of these incidents.

…The **incident and problem management process** should establish:

a. Procedures to identify, track, log, categorize and classify incidents according to a priority, based on business criticality;

b. Roles and responsibilities for different incident scenarios (e.g., errors, malfunctioning, cyber-attacks);

IBM Cloud Framework for Financial Services Focus Area(s):

Focused Risk Management and Compliance

Active Monitoring and Response

Unified Infrastructure Security and Resilience

IBM Cloud for Financial Services Supporting Activities & Controls:

IBM Cloud’s incident response plan was developed on the foundation of NIST 800-53 with special consideration of other relevant standards, such as ISO 27001. IBM Cloud’s Trust and Assurance maintains all core controls through internal Key Control Objective audits and validates these controls using multiple third-party auditing firms to conduct audits including, but not limited to SOC, ISO 27001, ISO 27017, ISO 27018, PCI assessments.[90]

Testing of Incident Response Plan is conducted internally as well as tested by external auditors on a regular basis.

[90] https://www.ibm.com/cloud/compliance.

c. Problem management procedures to identify, analyze and solve the root cause behind one or more incidents — a financial institution should analyze operational or security incidents likely to affect the financial institution that have been identified or have occurred within and/or outside the organization;

d. Effective internal communication plans, including incident notification and escalation procedures — also covering security-related customer complaints to ensure that

  i. incidents with a potentially high adverse impact on critical ICT systems and services are reported to the relevant senior management and ICT senior management;

  ii. the management body is informed on an ad hoc basis in the event of significant incidents and, at least, informed of the impact, the response, and the additional controls to be defined as a result of the incidents.

e. Incident response procedures to mitigate the impacts related to the incidents and to ensure that the service becomes operational and secure in a timely manner;

f. Specific external communication plans for critical business functions and processes in order to:

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

  ii. provide timely information to external parties (e.g., customers, other market participants, the supervisory authority) as appropriate and in line with an applicable regulation. [Emphasis added.]

EBA ICT, Section 3.5.1, ICT Incident and Problem Management, paras. 59 & 60 (pp. 23-24).

IBM Cloud has a security incident response plan, which aligns with the corporate wide IBM Cybersecurity Incident Response process (CSIRT). The CSIRT team is engaged wherever there is a confirmed security incident involving any IBM Cloud Customer system or Customer data and includes a process to communicate with the Customer should they be impacted.

The IBM Cloud platform status page[91] is used for all customer notifications including "general" security related notifications. Security notifications point to IBM security bulletins published per the IBM Product Security Incident Response Team (PSIRT) process.

IBM will investigate Security Incidents of which IBM becomes aware, and, within the scope of the IBM Services, IBM will define and execute an appropriate response plan. A customer may notify IBM of a suspected vulnerability or incident by submitting a request through the incident reporting process specific to the IBM Service or, in the absence of such process, by submitting a technical support request. [92]

13. FIs should conduct business impact analysis (BIA) and develop response and recovery plans

Regulatory Provisions:
EBA Guidelines on ICT and Security Risk Management (EBA ICT), November 29, 2019
Section 3.7, Business Continuity Management

a) Business Impact Analysis (BIA)

Industries: Banking
Primary Responsibility: Financial Institution / IBM

Regulatory Text:

As part of sound business continuity management, financial institutions should conduct business impact analysis (BIA) by analyzing 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.

IBM Cloud Framework for Financial Services Focus Area(s):

Unified Infrastructure Security and Resilience

IBM Cloud Framework for Financial Services Supporting Activities & Controls:

Each IBM Service is separately assessed for business continuity and disaster recovery requirements through business impact analysis and risk assessments intended to identify and prioritize critical business functions.[93]

IBM Cloud business continuity processes are validated frequently by external auditors through assessments including but not limited to FedRAMP, ISO27001, SOC, PCI, and HIPAA.

[91] https://cloud.ibm.com/status.
[92] Data Security and Privacy Principles for IBM Cloud Services. https://www.ibm.com/trust/security-psirt.
[93] *Id.*

The BIA should also consider the criticality of the identified and classified business functions, supporting processes, third parties and information assets, and their interdependencies, in accordance with Section 3.3.3. *EBA ICT, Section 3.7.1, Business Impact Analysis, para. 78* (p. 26).	IBM Cloud’s backup and redundancy mechanisms are tested at a frequency that aligns with NIST 800-53 and ISO 27001 standards. Policies are established to help maintain the continuity and availability of operations and support personnel, including redundant links, replication, and automatic failover, to ensure hardware maintenance activities are transparent to IBM service subscribers and end users.
b) Response and recovery plans **Industries:** Banking **Primary Responsibility:** Financial Institution / IBM **Regulatory Text:** Based on the BIAs (paragraph 78) and plausible scenarios (paragraph 82), financial institutions should develop response and recovery plans. These plans should specify what conditions may prompt activation of the plans and what actions should be taker to ensure the availability, continuity, and recovery of, at least, financial institutions’ critical ICT systems and ICT services. The response and recovery plans should aim to meet the recovery objectives of financial institutions’ operations. The response and recovery plans should consider both short-term and long-term recovery options. The plans should: a. Focus on the recovery of the operations of critical business functions, supporting processes, information assets and their interdependencies to avoid adverse effects on the functioning of financial institutions and on the financial system, including on payment systems and on payment service users, and to ensure execution of pending payment transactions; b. Be documented and made available to the business and support units and readily accessible in the event of an emergency; c. Be updated in line with lessons learned from incidents, tests, new risks identified and threats, and changed recovery objectives and priorities. *EBA ICT, Section 3.7.3, Response and Recovery Plans, paras. 83 & 84* (p. 27).	**IBM Cloud Framework for Financial Services Focus Area(s):** **Unified Infrastructure Security and Resilience** **IBM Cloud for Financial Services Supporting Activities & Controls:** As part of the implementation and operation of its Business Continuity Plan, IBM has identified four impact scenarios that might occur due to natural, physical, or man-made disruptive threats (e.g., earthquake, fire, social/political unrest, health threat, pandemic). (BPBC127 Guideline – Business Process Business Continuity).

5. References and Resources

a. EBA, EIOPA, and ESMA

- Final Report on EBA Draft Guidelines on Outsourcing Arrangements[94]
- Final Report, EBA Guidelines on ICT and Security Risk Management[95]
- Final Report on EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)[96]
- EIOPA Guidelines on outsourcing to cloud service providers[97]
- Final Report on ESMA Guidelines on outsourcing to cloud service providers[98]
- Joint Advice of the European Supervisory Authorities (ESAs)To the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector[99]

b. IBM

- IBM European Banking Authority Compliance Brief[100]
- IBM Cloud Compliance Programs[101]
- IBM Cloud PCI Guidance[102]
- IBM GDPR Framework[103]
- IBM Cloud Terms and Conditions[104]: Documents related to data security & privacy for IBM Cloud Services offerings, including:
  - Business Associate Addendum (BAA)
  - Cloud services terms (Service Descriptions)
  - Data security and privacy principles for Cloud Services
  - IBM standard terms (including Cloud Services Agreement)
  - IBM Data Processing Addendum
  - Data processing and protection data sheets for Cloud Services
- IBM Cloud Services CSA STAR Self-Assessment[105]
- IBM Cloud Infrastructure CSA STAR Self-Assessment[106]
- IBM Cloud Platform CSA START Self-Assessment[107]

[94] https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements.
[95] https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management.
[96] https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1954038/0d11223d-d682-4bd9-bb82-72b81ba6282e/Guidelines%20on%20ICT%20Risk%20Assessment%20under%20SREP%20%28EBA-GL-2017-05%29_EN.pdf?retry=1.
[97] https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/guidelines_on_outsourcing_to_cloud_service_providers_en.pdf.
[98] https://www.esma.europa.eu/sites/default/files/library/esma50-157-2403_cloud_guidelines.pdf.
[99] https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf.
[100] https://www.ibm.com/downloads/cas/KRGNBGBD.
[101] https://www.ibm.com/cloud/compliance.
[102] https://www.ibm.com/downloads/cas/OPLDK4Q2.
[103] https://www.ibm.com/data-responsibility/gdpr/.
[104] https://www.ibm.com/support/customer/csol/terms/.
[105] https://cloudsecurityalliance.org/star/registry/services/ibm-cloud-services.
[106] https://cloudsecurityalliance.org/star/registry/services/ibm-cloud-infrastructure.
[107] https://cloudsecurityalliance.org/star/registry/services/ibm-cloud-platform.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
May 2022

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANT-ABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM will not be liable for any direct or indirect damages, including without limitation, lost profits, lost savings, or any incidental, special, or other economic consequential damages, even if it has been advised of the possibility of such damages based on the information in this document. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Clients are responsible for ensuring their own compliance with various applicable laws and regulations. Clients are solely responsible for obtaining professional legal advice as to the identification and interpretation of any relevant laws and regulations that may affect the clients’ business and any actions the clients may need to take to comply with such laws and regulations. IBM does not provide legal, accounting or auditing advice. IBM also does not represent or warrant that its services or products will ensure that clients are compliant with any applicable laws or regulations.