BEYOND blue

DORA READINESS FRAMEWORK

CONCEPTUAL VIEW

Prepared by Akanksha Mohan

OVERVIEW

EXECUTIVE SUMMARY

DORA (Digital Operational Resilience) regulations have been introduced with a view of ensuring that the union financial sector becomes more resilient from an operational perspective to ensure the technological safety and good functioning of financial entities.

The proposed regulations aims first at consolidating and upgrading the ICT risk requirements as part of the operational risk requirements addressed so far separately in the different Regulations and Directives.

These proposed requirements are not only based on the elementary concepts of risk management but are also extensive and prescriptive in nature. Therefore it's expected that many financial institutions under the UK regulatory oversight may not see a direct read-across the Operational Resilience principles introduced by FCA, PRA and BoE.

WHAT IS THE DIGITAL OPERATIONAL RESILIENCE?

The operational risk requirements, when developed in Union legal acts, often favoured a traditional quantitative approach to addressing risk (namely setting a capital requirement to cover ICT risks) rather than enshrining targeted qualitative requirements to boost capabilities through requirements aiming at the protection, detection, containment, recovery and repair capabilities against ICT-related incidents or through setting out reporting and digital testing capabilities. DORA aims to consolidate and update rules on ICT risk, wherein all provisions addressing digital risk in finance would be brought together in a consistent manner under a single legislative act for the first time.

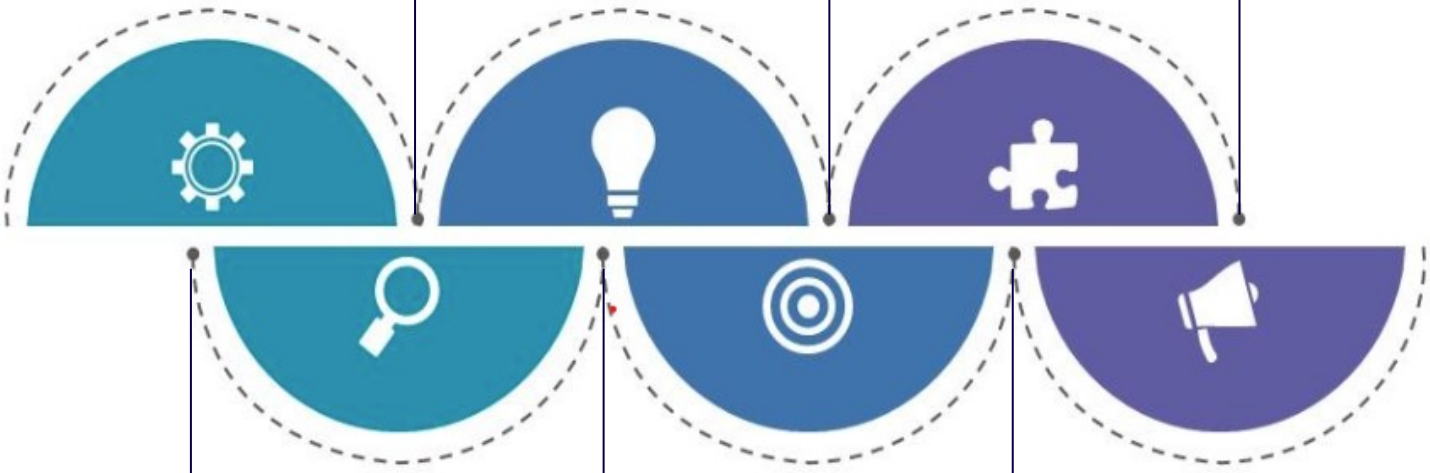
HOW DOES DORA AIM TO ACHIEVE THE OBJECTIVES PROPOSED TO THE EUROPEAN PARLIAMENT?

The proposed regulations aims to achieve the proposed objectives by:

Adopting a coherent approach to ICT risk in finance and recommending to strengthen, in a proportionate way, the digital operational resilience of the financial services industry through a Union sector-specific initiative.

Laying down rules aimed at coordinated testing by financial entities and competent authorities, thus facilitating the mutual recognition of advanced testing for significant financial entities.

Increasing harmonisation on digital resilience components, by introducing stringent requirements on ICT risk management and ICT-related incident reporting as compared to those laid down in the current Union financial services legislation.



Raising the level of harmony relating to ICT-related incident and cyber threats reporting regimes by requiring all financial entities to report to their competent authorities only. In addition, the European Supervisory Authorities (ESAs) would be empowered to further specify ICT-related incident and cyber threats reporting elements such as taxonomy, timeframes, data sets, templates and applicable thresholds.

By establishing Union Oversight Framework and addressing broader issue of counteracting systemic risk which may be triggered by the financial sector's exposure to a limited number of critical ICT third-party service providers is barely addressed by Union legislation.

By Setting out certain key principles to guide financial entities management of ICT third-party risk, particularly where financial entities resort to ICT third-party service providers to support their critical or important functions.

COMPARING THE UK & EU RESILIENCE REGULATIONS

Operational Resilience and DORA regulatory concepts have evolved in order to ensure financial institutions (FIs) do more to identify, map, maintain and recover their critical operations to sustain catastrophic events and continue service provisioning including market integrity. In essence both regulations emphasise the need for organisations to adopt an approach of proportionality whilst implementing their strategies surrounding these regulations.

Whilst there are some commonalities in the evolution of these regulations the two sets of regulations are conceptually aimed at managing resilience in their own distinct ways.

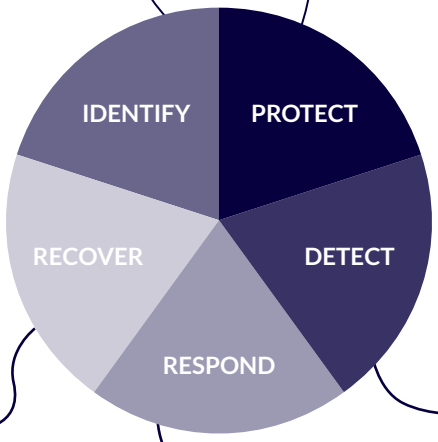
Using an illustration of NIST framework and tethered to its components of IDENTIFY, PROTECT, DETECT, RESPOND and RECOVER, we explore the distinct areas of regulatory focus in these areas from both UK's and EU's lens:

UK REGULATIONS: Aim at focusing on identifying important business services (as opposed to risks) with an external looking view i.e. customer impact being at the heart of defining which services are 'important'.

DORA REGULATIONS: Aim at financial entities identifying critical ICT-related functions in a firm with an internal looking view. ICT risk management & mitigation are the focal domains.

UK REGULATIONS: Have a light touch approach in specifying protect mechanisms for organisations to adhere to. The resilience requirements also pan across all pillars of the operating model (people, process, technology and third-parties).

DORA REGULATIONS: Have a prescriptive approach with specific guidelines in regards to protection and prevention against resilience risks. These resilience considerations only pan across ICT and ICT third-party providers.



UK REGULATIONS: Advocates development and implementation of robust recovery strategies which are adequately tested to ensure a firm's capability to recover from significant disruptions.

DORA REGULATIONS: Factors in the risk management methodologies once again to drive the development of business continuity & disaster recovery plans which are to be tested for their adequacy.

UK REGULATIONS: It assumes that despite robust detect mechanisms a firm could still sustain catastrophic disruptions.

DORA REGULATIONS: Applying the principles of risk management, it takes a risk based approach on deploying detective strategies with a view of avoiding ICT and ICT third-party related risks from materialising.

UK REGULATIONS: Set out principle based approach on how firms respond to disruptive events. The concept of Impact tolerance thresholds has been developed to ensure where possible firms remain within these metrics with a view of lessening the intolerable harm caused to customers.

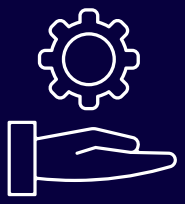
DORA REGULATIONS: Adopts a conventional risk-based approach of firms having well-defined recovery time and point objectives along with applying severity classification criteria for any ICT-related incidents.

DORA PILLAR ALIGNMENT

ICT RISK MANAGEMENT

OVERVIEW: Financial entities are required to have a sound, comprehensive and well-documented Information and Communication Technology (ICT) risk management framework which should include strategies, policies, procedures, ICT protocols and tools that are important to duly and adequately protect all Information and ICT assets. The high-level considerations below are to be applied by financial entities in line with the principles of proportionality i.e., in line with the size and nature of their business; scale & complexity of their services, activities and operations; and their overall risk profile. European Supervisory Authorities (ESA) in conjunction with ENISA will develop draft regulatory technical standards covering the main principles of the Article 3 – 14.

- To minimise ICT-related risks, organisations should create & maintain resilient ICT systems and tools to ensure a high-level of Confidentiality, Integrity and Availability (CIA) of data.
- Create a risk-based approach covering strong authentication mechanisms and change control
- of ICT assets. For e.g. instances where networks may be turned off in order to proactively isolate Information Assets during sustained cyber attacks.
- Set up and continually monitor risk tolerances, key performance indicators (KPIs), key risk indicators (KRIs) along with analysing the Impact Tolerances following an ICT disruption.
- Establish a management body to define, approve, oversee & be accountable for the implementation of Information and Communication Technology (ICT) risk management framework including third- party service providers.
- Identify & document all ICT functions, Roles and Responsibilities (R&Rs) and Information Assets. This includes ICT-related risks, threats and vulnerabilities across all critical or important functions.
- Build a holistic ICT multi-vendor strategy, at entity level showing key dependencies on
- ICT third-party service providers and explaining the rationale behind the procurement mix of ICT third-party service providers.



MANAGING RISK

BUSINESS CONTINUITY & INCIDENT MANAGEMENT

- Business Continuity, Communication & Crisis Management plans must be both well-defined and robustly tested. This includes quantitative & qualitative assessment of Business Impact Analysis (BIAs) relating to critical processes, functions, third-party dependencies and information assets.
- Firms to adopt a multi-layered detect mechanism which has defined alert thresholds and criterias for incident response.
- Recovery Time and Point Objectives (RTOs & RPOs) to consider the criticality of each business function whilst also considering their impact on overall market stability.
- Develop adequate back-up processes and restoration functionalities to limit the downtime, disruption and loss as a result of an ICT-related risk event. Based on the criticality of data, the key steps would broadly cover the scope of data for backup, frequency of data backup, physical and logical segregation of restoring systems from the source systems such as designated system images or sandbox environments.
- Ensure mechanisms are in place to learn and evolve from incidents including both external & internal ICT-related events.
- Organisations to have clearly defined communication plans to ensure timely and accurate disclosure to counterparties & customers in event of ICT-related events.

Below are the articles that relate to the ICT Risk Management Pillar:

Article 3a – Proportionality;
Article 4 – Governance and Organisation;
Article 5 ICT Risk Management Framework;
Article 6 – ICT Systems, Protocols and tools;
Article 7 – Identification;
Article 8- Protection & Preventions;
Article 9 – Detection;
Article 10 – Response & Recovery;
Article 11 - Backup Policies, Restoration and Recovery Methods;
Article 12 – Learning & Evolving;
Article 13 – Communication;
Article 14 - Further harmonization of ICT Risk Management tools, methods, processes and policies;
Article 14a – Proportionate ICT Risk Management Framework

DORA PILLAR ALIGNMENT

ICT-RELATED INCIDENTS MANAGEMENT, CLASSIFICATION AND REPORTING

OVERVIEW: Financial entities are required to define, establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents and significant cyber threats. In addition to the integrated monitoring and handling of ICT-related incidents, firms will be required to ensure root causes are identified, documented and addressed to prevent the occurrence of such incidents. Below are some additional regulatory considerations for financial entities to embed as part of their ICT-related incident management process.

INCIDENT CLASSIFICATION

- As part of ICT incident management process financial entities would be required to have early warning indicators in place, log and prioritise incidents based on their severity and criticality of services impacted, assign roles and responsibilities to be activated in different ICT-related incident types and scenarios and also set out communication plans for staff, external stakeholders and media.
- Firms will be required to classify ICT-related incidents and cyber threats based on: number of clients/ counterparties affected, reputational impact, service downtime, geographical spread, data loss, criticality of services impacted, economic impact and potential of critical services being impacted as a result of a threat.
- The classification of such incidents and threats is to be based on materiality threshold which will be also be developed by ESA as part of the technical standards.
- The regulations propose the setting up of single EU hub with the aim of enhancing supervisory convergence and exchange of information between public authorities, law enforcement agencies and resolution authorities.

INCIDENT REPORTING

- ESA in conjunction with ENISA & ECB to develop draft regulatory technical standards to establish reporting content of major ICT-related incidents including timeframes for reporting.
- Financial entities are to report all ICT-related incidents to their relevant competent authorities in the respective member states using a common template and a harmonised procedure as established by the respective supervisory authority. Where entities are subject to supervision by more than one competent authority, members state would also be required to designate
- a single competent authority as the main addressee of such reporting.
- ESAs shall report yearly on an anonymised & aggregated basis on the major ICT-related incident
- & significant cyber threat notifications received from competent authorities including their nature, impact on the operations of financial entities or customers, costs and remedial actions taken.
- The ICT-related incident requirements also apply to operational or security payment- related incidents in case it concerns credit institutions, payment institutions, account information service providers & electronic money institutions.

Below are the articles that relate to the ICT-related Incidents Management, Classification and Reporting Pillar:

Article 14b – Management, Classification and Reporting;
Article 15 – ICT-related Incident Management Processes;
Article 16 - Classification of ICT-related incidents (and cyber threats);
Article 17 – Reporting of Major ICT-related incident (and significant cyber threats);
Article 18 – Harmonisation of reporting contents and templates;
Article 19 - Centralisation of reporting of major ICT-related incidents;
Article 20 – Supervisory Feedback;

DORA PILLAR ALIGNMENT

DIGITAL OPERATIONAL RESILIENCE TESTING

OVERVIEW: The regulations require that financial entities should establish, maintain and review, a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk management framework. This is with a view to ensure that firms are assessing their preparedness for handling such incidents and are also identifying gaps or deficiencies with prompt implementation of corrective measures to counteract such deficiencies.

- When implementing the DORA testing programme, firms are required to follow a risk-based approach to duly consider the evolving landscape of ICT risks, any existing exposure to specific risks and the criticality of information assets and of services provided.
- The testing programme must be embedded based on the principle of proportionality considering size of the business and risk profiles.
- Through the lifecycle of ICT-related testing and in practice, firms must classify and prioritise the issues or vulnerabilities identified through these tests. These should be promptly mitigated via counteractive measures in line with their severity classification.
- Wide-lens approach to types of ICT testing must be adopted which includes vulnerability assessments, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires & scanning software solutions, source code reviews, scenario- based tests, compatibility testing, performance testing, end-to-end testing and/ or penetration testing.
- Financial entities are required to conduct testing of their critical ICT assets and applications at least annually. Although the regulations have not categorically defined the meaning of 'critical ICT assets', these could be software or hardware assets in the network and information systems used by financial firms. It would also include electronic communications network, device or group of devices performing automated processing of digital data and any devices storing, processing, retrieving or transmitting the digital data for operational purposes.

TESTING PROGRAMME

THREAT LED PENETRATION TESTING

- Advanced testing such as Threat Led Penetration Testing (TLTP), also known as a Red / Purple Team Assessment must be carried out by external testers to address higher levels of risk exposure for several or all critical functions of the firm.
- Firms would also need to identify all underlying ICT processes, systems, technologies and ICT third-party services providers relating to such critical functions in advance of conducting TLTP. Where ICT third-party providers have been identified as providing services to a critical function, firms must take necessary steps to ensure their participation in such exercises.
- Organisation must also consider pooled threat led penetration testing involving several financial entities to which a common third-party provides ICT services to.

Below are the articles that relate to the Digital Operational Resilience Testing Pillar:

Article 21 – General requirements for the performance of Digital Operational Resilience Testing;
Article 22 – Testing of ICT Tools and Systems;
Article 23 – Advanced testing of ICT tools, systems and processes based on threat led penetration testing;
Article 24 – Requirements for External Testers;

DORA PILLAR ALIGNMENT

MANAGING OF ICT THIRD-PARTY RISK

OVERVIEW: The regulations looks to address the lack of homogeneity and consistency in the monitoring and management of ICT third party risks, ICT third-party dependencies and concentration risks . This regulation covers a wide range of ICT third-party providers across cloud computing services, software and data analytics services, provisioning of data centres services, participants in payments provision services (except central banks), financial entities providing ICT services within the same financial group to the parent or subsidiaries of the group as well as where such entities provide ICT services to other financial entities.

- In instances where a third-party service(s) is critical to the stability and integrity of Union financial system, then such service providers are to be recognised as 'critical ICT third-party service providers'. Additionally, to drive adequate oversight, where such providers are domiciled and established in third countries, they would be required to establish a subsidiary in the Union within 12 months of being designated as 'critical' by the Lead Overseer.
- Risk-based approach must be adopted to carry out inspection & audit of the ICT third-party service provider.
- Financial entities must assess potential concentration risks across both contracted and/ or subcontracted service provisioning domains. They must also ensure ICT third-party providers' adhere to highest information security standards whilst also robustly implementing and testing their contingency plans.
- To proactively identify & monitor risks emanating from the reliance on ICT third-party providers, firms are expected to conduct thorough pre and post-contracting analysis of such arrangements against a range of criteria's that could impact their critical functions or services.
- Businesses must ensure ICT third-party providers contracts contain all the necessary monitoring & accessibility details such as a full service level description, locations where data is being processed, etc.
- Organisations will be required to adopt the draft technical standards template (developed by ESAs) to capture contractual arrangement of services provided by the ICT third-party service providers. This further enables the financial entities to enhance their understanding around contractually binding obligations on part of their third-party service providers.
- Well defined & proportional exit plans must be developed in event of significant service deterioration, failure or business disruptions by the third-party service provider.

RISK BASED APPROACH

SUPERVISION & COORDINATION

- All financial entities must maintain a Register of Information with all contractual arrangements of ICT services provided by ICT third-party providers.
- A consistent & confluent supervisory approach on ICT third-party risks will be followed by subjecting the service providers to a Union Oversight Framework which is to be established by this regulation.
- As part of the Union Oversight Framework, an Oversight Forum will be established to promote coordination and to increase the digital operational resilience whilst fostering best practices on addressing ICT concentration risks & exploring mitigants for cross-sector risk transfers.
- Lead Overseer (any of the three European Supervisory Authorities may be designated as a Lead Overseer) will ensure viability, continuity, scalability & quality of services provided by ICT third-party service providers. This includes assessment of their testing framework, on-site inspections, physical security measures, ICT- related governance & risk management processes.
- To promote international convergence and development of best practices on ICT third- party service providers digital risk management, regulations enable ESAs to conclude cooperation arrangements with third-country regulatory and supervisory authorities to ensure cross border support.

Below are the articles that relate to the Digital Operational Resilience Testing Pillar:

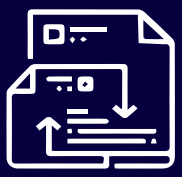
Article 25 – General Principles ;
Article 26 – Preliminary assessment of ICT related risk and further subcontracting arrangements with regards to concentration risk;
Article 27 - Key Contractual Provisions;
Article 28 – Designation of critical ICT third-party service providers;
Article 29 – Structure of the Oversight Framework;
Article 30 - Tasks of Lead Overseer;
Article 31 – Powers of the Lead Overseer;
Article 32 – Request for Information;
Article 33 - General Investigations;
Article 34 – On-site Inspections;
Article 35 – Ongoing Oversight;
Article 36 - Harmonisation of conditions enabling the conduct of the Oversight;
Article 37 – Follow-up by competent authorities;
Article 38 - Oversight Fees;
Article 39 - International Cooperation;

DORA PILLAR ALIGNMENT

INFORMATION SHARING ARRANGEMENT

OVERVIEW: The regulation proposes a Union level voluntary information sharing mechanism which would help the financial community in collectively preventing and responding to threats thereby limiting the spread of ICT risks and potential contagion.

- Through information-sharing arrangements & whilst protecting potentially sensitive nature of the information, financial entities may exchange cyber threat intelligence, including indicators of compromise, tactics, techniques & procedures, cyber security alerts & configuration tools.
- Information sharing arrangements are aimed at enhancing digital operational resilience of financial entities through raising awareness in relations to cyber threats, supporting defensive capabilities and threat detection techniques.



COLLABORATION

Below article relates to the Information Sharing Arrangement Pillar:

Article 41 – Information-sharing arrangements on cyber threat information and intelligence;

COMPETENT AUTHORITIES

Overview: EBA, ESMA or EIOPA and the ECB shall cooperate closely with each other and exchange information to carry out their duties

AUTHORITIES

- Competent authorities & the Lead Overseer must mutually exchange all relevant information concerning critical ICT third-party service providers in relation to identified risks, approaches & measures.
- Competent authorities, EBA, ESMA or EIOPA and the ECB may develop crisis-management exercises involving cyber-attack scenarios to develop communication channels & enable an effective EU- level coordinated response in the event of a major cross-border ICT-related incident.
- Competent authorities will have all supervisory, investigatory & sanctioning powers.
- Criminal/ administrative penalties & remedial measures must be imposed by member states for breaches of this Regulation. Imposing such penalties for breaches is to be decided at the discretion of the member states.
- Competent authorities must publish on their official websites, without undue delay, any decisions imposing an administrative penalty including information on the type & nature of the breach, the identity of the persons responsible & the penalties imposed.

Below are the articles that relate to the Competent Authorities Pillar:

Article 41 – Competent Authorities ;
Article 42 – Cooperation with structures and authorities established by Directive (EU) 2016/1148;
Article 42a - Cooperation between authorities;
Article 43 – Financial cross-sector exercises, communication and cooperation;
Article 44 – Administrative penalties and remedial measures;
Article 45 - Exercise of the power to impose administrative penalties and remedial measures;
Article 46 – Criminal Penalties ;
Article 47 – Notification Duties;
Article 48 - Publication of administrative penalties;
Article 49 – Professional Secrecy;
Article 49a – Data Protection;

TRANSITIONAL AND OTHER FINAL PROVISIONS

The European commission shall consult with EBA, ESMA or EIOPA and the ECB to carry out a review and submit a report to European Parliament and Council covering the criteria for designation of critical third-party service providers, the voluntary nature of notification of significant cyber threats and the powers of Lead Overseer to ensure the effectiveness of the oversight framework that these regulations propose.

The DORA regulations have also introduced some updates to Regulation (EC) No 1060/2009, whereby credit reference agencies are required to have effective procedures for risk assessment, internal control mechanisms to effectively mitigate any risks against their critical ICT systems.

Amendments to Regulation (EU) No 648/2012 require Central Counterparties to ensure continuity and orderly functioning of its services and preservation of it's critical functions by implementing adequate business continuity and disaster recovery plans . These should also include ICT business continuity and response and recovery plans.

Regarding Regulation (EU) No 909/2014, Central Security Depositories are required to consider appropriate ICT tools, processes and policies to manage the ICT risks. Similar to the requirements placed on Central Counterparties, Central Security Depositories are also required to implement and maintain robust continuity and recovery plans in order to ensure preservation of operations and critical functions. They are also required to monitor and manage any risks to the market infrastructure, service and utility providers and any other key participants in securities settlement systems process.

GLOSSARY

- **Business Impact Analysis (BIAs)**
  A systemic process to determine and evaluate the potential effects of disaster or disruption to critical or important functions
- **Critical or Important Function**
  Any function where it's disruption would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or where it's discontinuation would materially impair financial entity's compliance with conditions and obligations of its authorisation
- **European Supervisory Authorities (ESAs)**
  Comprises of: the European Supervisory Authority (European Banking Authority) ('EBA'), the European Supervisory Authority (European Securities and Markets Authority) ('ESMA'), and the European Supervisory Authority (European Investment and Occupational Pensions Authority) ('EIOPA')
- **Oversight Framework**
  The framework to be established by this regulation
- **Recovery Time Objective (RTO)**
  The maximum duration of downtime that a business can tolerate without incurring a significant financial loss or causing a detrimental impact to its customers.
- **Recovery Point Objective (RPO)**
  The maximum amount of data that can be lost during a disruption before significant harm occurs. These objectives drive the development of effective backup strategies.
- **Information and Communication Technology (ICT)**
  A diverse set of technological tools and resources used to transmit, store, create, share or exchange information. These could include technologies relating to computers, networks, internet and telephony.
- **ICT Services**
  The regulations defines this broadly as digital and data services provided through ICT systems to one or more external users on an ongoing basis including the so called 'over the top' services such as electronic communications services.
- **ICT-related Risks**
  Any circumstance or event which if materialized may compromise the network and information systems and may also adversely impact the provision of services by financial entities
- **ICT-related Incidents**
  Any unexpected single event o series of linked events that compromises the network and information systems and adversely impacts the services provided by financial entities. Such events could also have the propensity to adversely impact the availability, authenticity, integrity or confidentiality of data that underpin the provisioning of services.
- **ICT Third-party provider**
  Any undertaking external to a financial entity that provides ICT services
- **ICT Concentration Risks**
  It arises where there is an exposure to individual or multiple related critical ICT third-party service providers thereby creating a degree of dependency on their services. The unavailability or failure of the provision of such ICT services by these providers could potentially adversely impact the ability of financial entity to deliver its critical or important functions.
- **Threats**
  Any event with the potential to adversely impact organizational operations, assets, individuals through unauthorized access, destruction, modification of information or denial of service.
- **Threat Led Penetration Testing**
  A methodology that mimics the tactics and techniques of real-life threat actors perceived to be posing as genuine cyber threat. It delivers a controlled, bespoke, intelligence-led test of firm's critical live production systems.
- **Vulnerabilities**
  A weakness in an information system that could be exploited by cyber criminals to gain unauthorized access to computer systems, networks and applications. Vulnerabilities weaken the security systems of a firm's critical assets and infrastructure and open the door to malicious attacks.