Resolver.
A KROLL BUSINESS

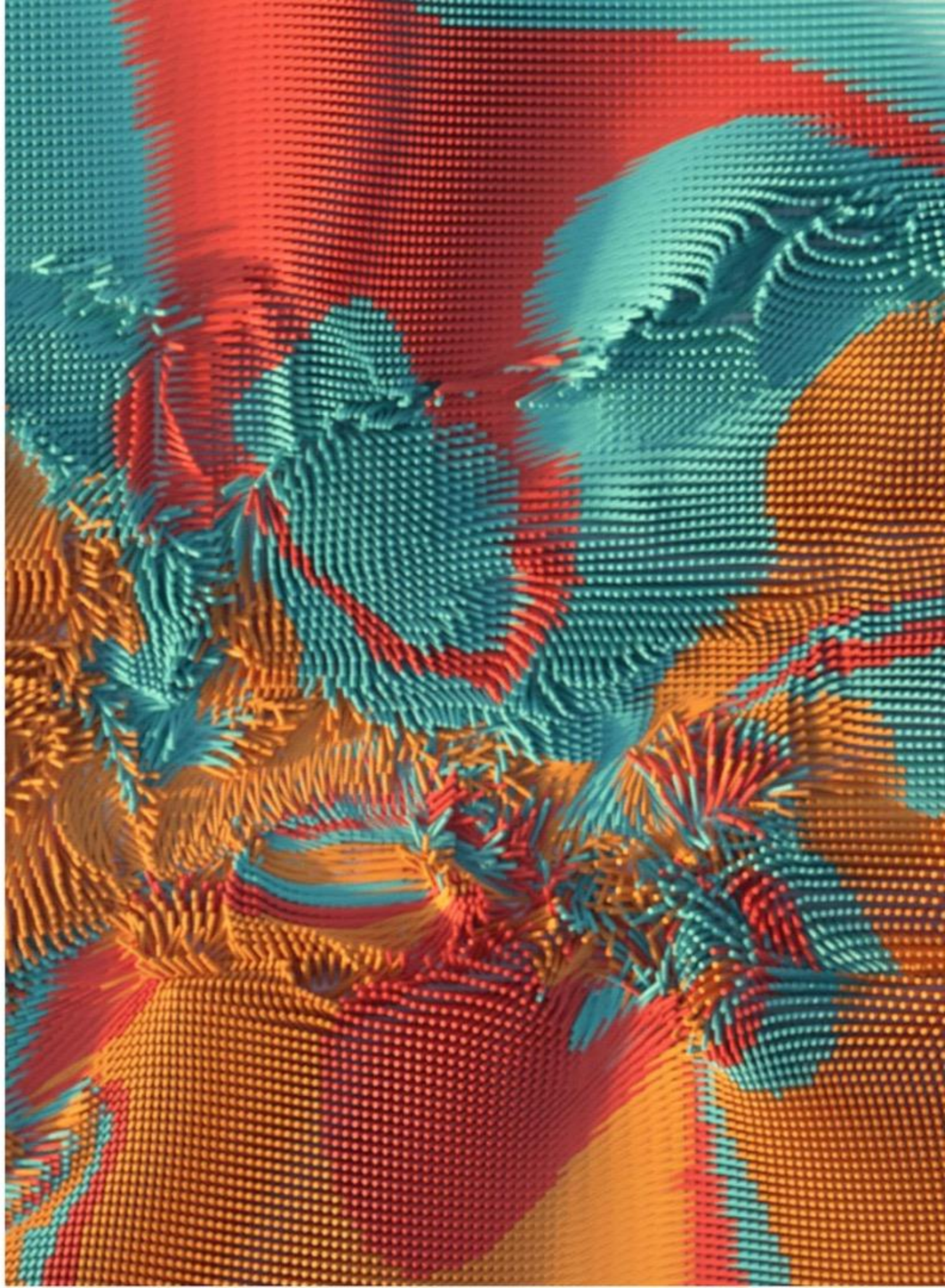
Navigating DORA: Preparing for Europe's New Operational Resilience Regulation

June 6, 2024

Resolver.
A KROLL BUSINESS

Agenda

- Introduction
- Context and Legal Framework
- Risk Management, Resiliency Testing & Incident Reporting
- ICT Third Party Risk Management
- Proportionality
- Key Challenges and How to Navigate Them
- Kroll's DORA Services & Offerings
- Resolver's Operational Resilience Software
- Conclusion



Resolver.
A KROLL BUSINESS

Our Speakers

Hannah Rossiter

Managing Director | Kroll | Dubai

Hannah leads the Financial Services Compliance and Regulation services in France. With over 25 years' experience, Hannah has extensive financial services, regulatory and compliance expertise gained both in London and Paris. She has spent the past 20 years in France working within or advising investment firms and asset managers.

Tiernan Connolly

Managing Director, Cyber Risk | Kroll | Ireland

Tiernan Connolly, a managing director in Kroll's Cyber Risk advisory practice in Dublin, has over 20 years of experience in financial services and consultancy. He specializes in cybersecurity, regulations, threat intelligence, strategy, risk, and governance. At Kroll, he helps clients enhance their cybersecurity programs to ensure regulatory compliance.

Pooja Azhalavan

Senior Manager, Product Marketing | Resolver | Toronto

Pooja leverages her diverse expertise to help customers and internal teams understand the value of our Risk Intelligence platform. Closely works with cross-functional teams to enforce customer needs across - Enterprise Risk, Compliance, Internal Audit, Third-Party Risk & more.

About Kroll | Resolver

- Aligned with our mission to transform Risk Management into **Risk Intelligence**, Resolver was acquired by Kroll in 2022, proving to be strategic and symbiotic for both organizations!

- Kroll brings research insights, **best-in-class consultancy services**, and industry best practices, to further enhance Resolver's **innovative suite of products** and accelerate overall growth.

- The combination of Kroll's deep subject matter expertise and breadth of knowledge, with our technology and software operating experience, will continue to help us meet and exceed our client needs, and **deepen our foothold in the Integrated Risk Management market.**

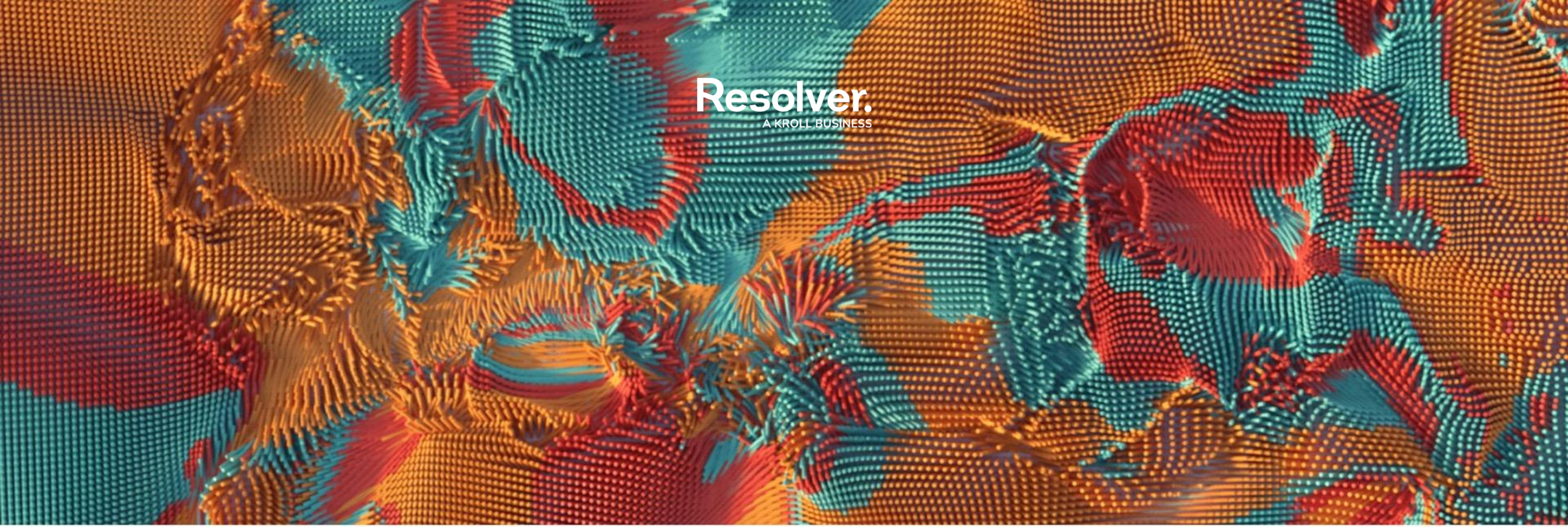
Resolver. A KROLL BUSINESS KROLL

Poll 1: Has your organization conducted a DORA gap assessment?

A) Yes

B) No

C) I'm Not Sure



Context and Legal Framework

DORA Regulatory Framework

- The Digital Operational Resilience Act (DORA) was published in the EU's Official Journal in December 2022 and came into force on January 16, 2023.
- DORA aims to improve cybersecurity and operational resilience in the financial services sector, including both a Regulation and a Directive.
- The requirements of DORA will be applicable from **January 2025**.
- Existing directives such as CRD IV, Solvency 2, MiFID 2, and AIFM are being amended to align with DORA.
- Accompanying DORA are regulatory technical standards (RTS), implementing technical standards (ITS), and guidelines (GL):
  - **First set (published in January 2024)**: ICT risk management framework, ICT-related incident classification, critical functions by ICT third-party service providers, and information register template.
  - **Second set (final reports expected in July 2024)**: incident reporting content, timelines, and templates, cost and loss aggregation for incidents, subcontracting critical functions, and threat-led pen testing.

Main objectives of DORA :

1) Harmonize Information and Communications Technology (ICT) risk management requirements across Europe.

2) Ensure all financial industry participants have safeguards against cyber-attacks and ICT risks.

3) Implement oversight of critical ICT service providers, both through financial institutions' authorization and direct oversight of critical third parties.

Scope & Proportionality

DORA applies to over 22,000 financial entities and ICT service providers within the EU and those supporting them from outside the EU.

- Credit institutions
- Electronic money institutions
- Investment firms
- Insurance and reinsurance undertakings
- Asset management companies
- Data reporting service providers
- Credit rating agencies
- ICT third-party service providers

Proportionality is embedded in DORA and in the draft RTS In two ways:

- Exemptions for **microenterprises** from various requirements of Chapter II of DORA on ICT risk management.
- A **simplified ICT risk management framework** for small and non-interconnected investment firms.

- **Harmonization of rules in the financial sector:**
- DORA requirements apply to EU entities, not non-EU parent entities.
- EU subsidiaries of non-EU parent entities must comply with DORA.
- Financial entities and groups can implement ICT policies leveraging parent-level strategies, considering local specificities.
- Individual financial entities are responsible for complying with DORA and RTS obligations at the individual level.

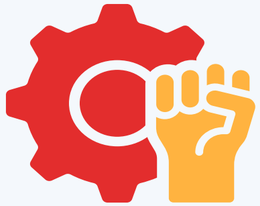
ICT Risk Management
Embed a comprehensive risk management framework for ICT systems.

ICT Related Incident Reporting
Standardize reporting of ICT related incidents. Incident management processes and templates for reporting of incidents.

Digital Operational Resilience Testing
Testing & assurance of technology resiliency through different techniques & harmonization of data collected by financial organizations.

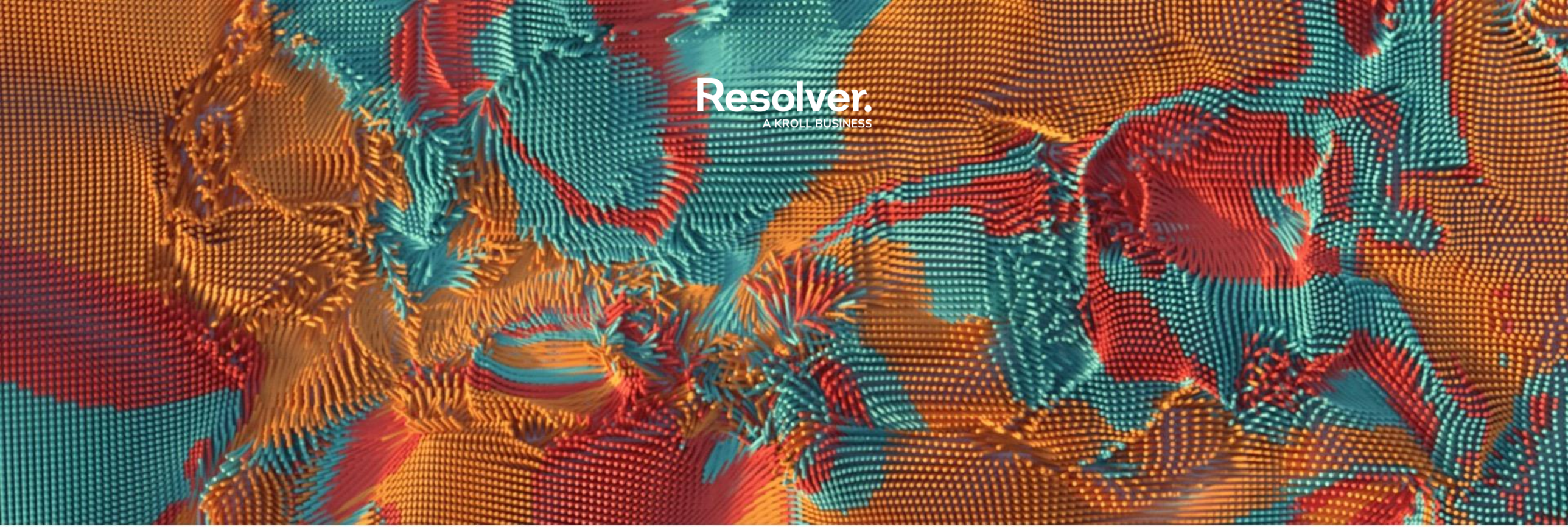
ICT Third - Party Risk
Stricter controls and processes for third-party risk management and oversight.

Information Sharing
Mechanisms for sharing information on threat actor activity.



Business Resilience

Resolver.
A KROLL BUSINESS



ICT Risk Management, Resiliency Testing & Incident Reporting

ICT Risk Management

Governance, frameworks, policies and procedures

Governance and Organisation

- ✓ Responsibility of the management body for implementing and overseeing the operational resilience strategy
- ✓ Definition of roles and responsibilities for overseeing arrangements concluded with ICT third-party providers
- ✓ Determination and allocation of budgets
- ✓ Independence of IT risk management functions from internal control and audit functions
- ✓ Assigning the responsibility to a member of senior management for monitoring critical ICT third party service providers
- ✓ Annual / Change-Driven reviews of the ICT risk management framework

ICT Security Policies and Procedures

- ✓ ICT asset management policy and procedure
- ✓ Data and system security procedure
- ✓ ICT operations policy and procedure
- ✓ ICT project management policy
- ✓ ICT change management procedure
- ✓ ICT-related **incident management policy**
- ✓ ICT **business continuity policy**
- ✓ Encryption and cryptographic controls policy
- ✓ Acquisition, development and maintenance of ICT systems
- ✓ Physical and environmental security policy
- ✓ Human resources policy
- ✓ Identity management policy and procedure
- ✓ Access control policy
- ✓ Capacity and performance management procedure
- ✓ Vulnerability and patch management procedure
- ✓ Logging procedure

ICT Risk Management

ICT Systems, Protocols and Tools

Protection

- ✓ Implementation of sound network and infrastructure management
- ✓ Implementation of appropriate mechanisms and tools for preventive security of assets
- ✓ Administration and control of access rights
- ✓ Implementation of strong authentication mechanisms
- ✓ Implementation of controls for managing changes to assets and information systems

Detection & Reporting

- ✓ Classification of ICT supported business functions, assets and third-party service providers, with an emphasis on Critical and Important Functions (CIF)
- ✓ ICT risk assessments (cyber threats and ICT vulnerabilities)
- ✓ Implementation of several levels of control, definition of alert thresholds and criteria for triggering IT incident detection and response processes
- ✓ Regular pen-testing

Response & Recovery

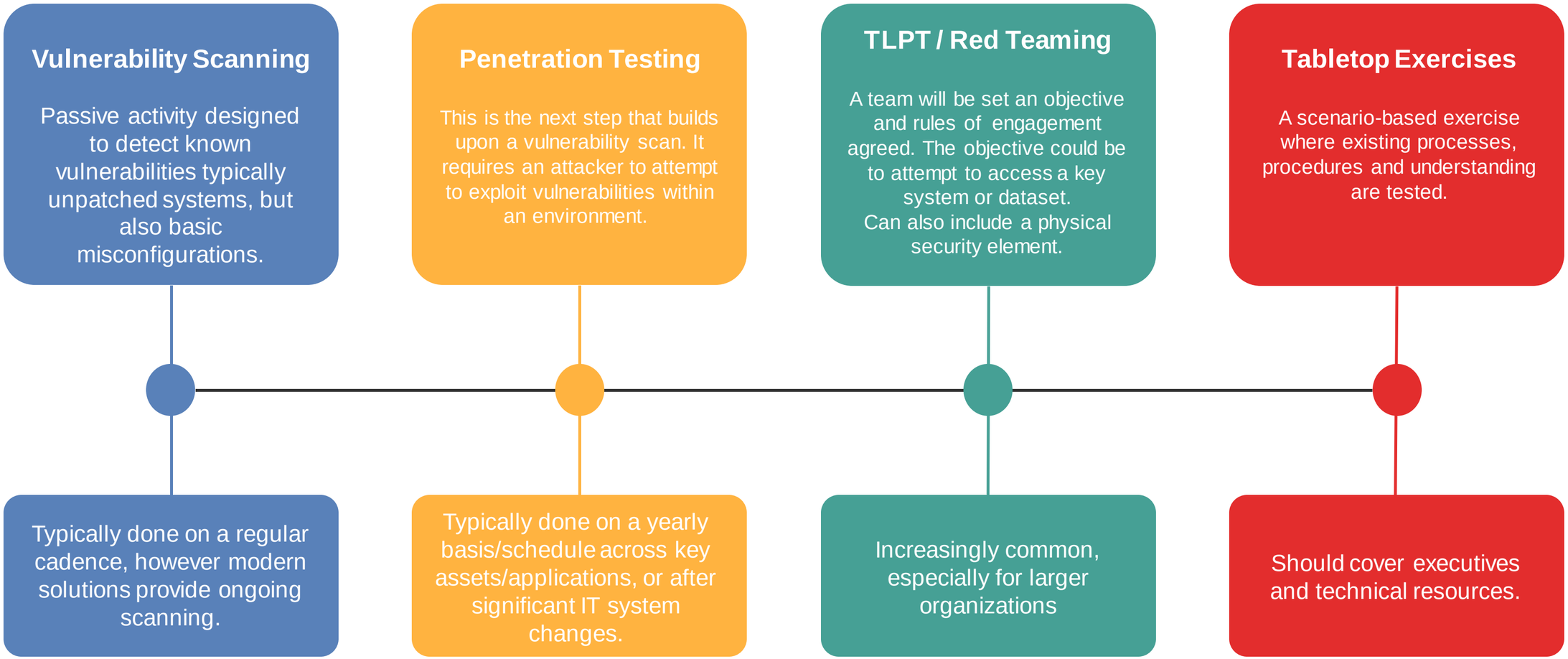
- ✓ Incident management process
- ✓ Business continuity plan
- ✓ Escalation and analysis
- ✓ Implementing ICT-incident log
- ✓ Incident analysis and impact assessment
- ✓ Classification of ICT-related incidents
- ✓ Reporting of critical incidents to national authorities

Communication & Learning

- ✓ Post-incident IT reviews to identify improvements to IT operations
- ✓ Escalation of findings to the management body
- ✓ Development of IT security awareness programs for staff members
- ✓ Monitoring technological developments
- ✓ Implementation of communication plans to all stakeholders internal and external

Types of Cyber Resiliency Testing

Multiple types of testing techniques are outlined in DORA to ensure the effectiveness of controls.



Resolver.
A KROLL BUSINESS

ICT Incident Reporting

Updated And Consolidated Reporting Requirements

- Mandatory reporting of major ICT-related incidents and voluntary notification of significant cyber threats

- Classification of incidents according to key pre-defined criteria and materiality thresholds for determining major ICT- related incidents;
  - Estimation of the aggregated costs/losses, along with other criteria, caused by major ICT related incidents

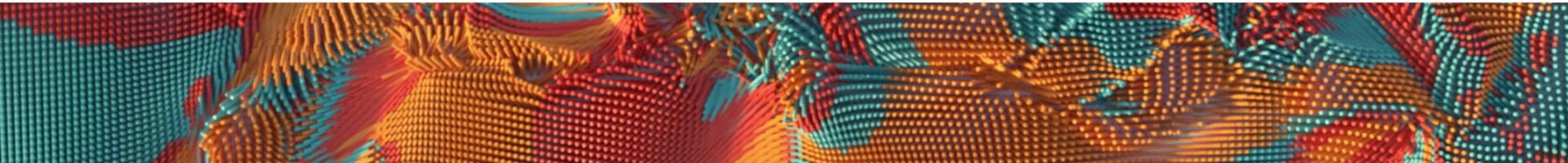
- Timelines for incident reporting:
  - Initial notification: **4 hours** from determining the incident is major but in any event within **24 hours** of detecting the incident;
  - Intermediate notification within **72 hours** of classifying the incident as major; and
  - Final report no later than **1 month** from classifying the incident as major.

- Harmonization of reporting content and templates

Resolver.
A KROLL BUSINESS

Resolver.
A KROLL BUSINESS

ICT Third-Party Risk Management



ICT Third Party Risk Management

Oversight For Critical Third-party Service Providers

- **Greater emphasis on governance, oversight and documentation**
- **Pre-outsourcing analysis and due diligence**
- **Specific contractual provisions required**
- **Minimum standards for information security requirements**
- **Exit strategies**
- **Access and Audit Rights**

INTRAGROUP SERVICES

- Financial group entities providing ICT services to their parent, subsidiaries, or branches are considered ICT third-party service providers under DORA.
- Financial entities providing ICT services to other financial entities are also considered ICT third-party service providers under DORA.
- Intra-group ICT services have specific risks and benefits but should not be considered less risky than external providers.
- Intra-group ICT services should adhere to the same regulatory framework as external providers.
- The principle of proportionality applies, with no differentiated requirements between intra-group and external providers.

Financial entities may make use of the services of **critical** ICT third-party service providers established in a third country only if the latter had **established a subsidiary in the EU within 12 months following the designation.**

Resolver.
A KROLL BUSINESS

Contractual provisions

Minimum requirements based on existing frameworks for critical third-party contracts

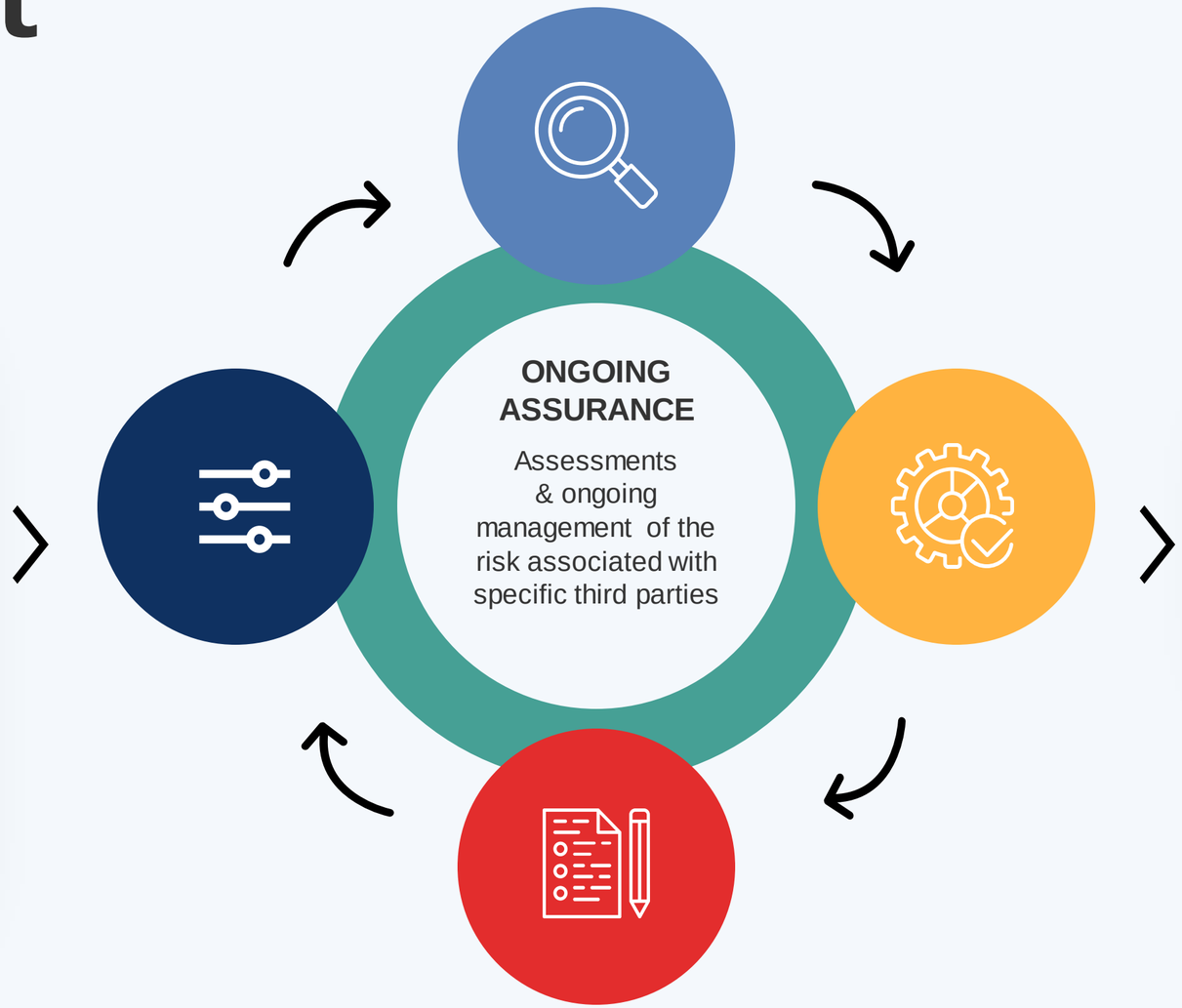
- Respective rights & obligations
- Termination provisions
- Description of the outsourced function
- Dates and notice periods
- Governing law and jurisdiction(s)
- Sub-outsourcing or delegation conditions
- Location(s) including where data processed/stored
- Information security and personal data provisions
- Performance monitoring on a regular basis
- Agreed service levels and performance targets
- Reporting obligations (& sharing of audit reports)
- Incident management and notification without undue delay
- Insurance requirements (certain risks and level of cover)
- BCP/DR requirements including testing
- Access & inspection rights (information, premises, systems & devices)
- Data accessed, recovered and returned to the firm as needed

ICT Third Party Risk Management

Vendor Management Cycle

SELECTION & ONBOARDING

- Classify vendors using a risk-based approach (supplier criticality)
- Due diligence on the selected third parties before contracting
- Establishing necessary appropriate controls



OFFBOARDING

Secure termination and offboarding of third party and company data

Resolver.
A KROLL BUSINESS

ICT Third Party Risk Management

Registers of information

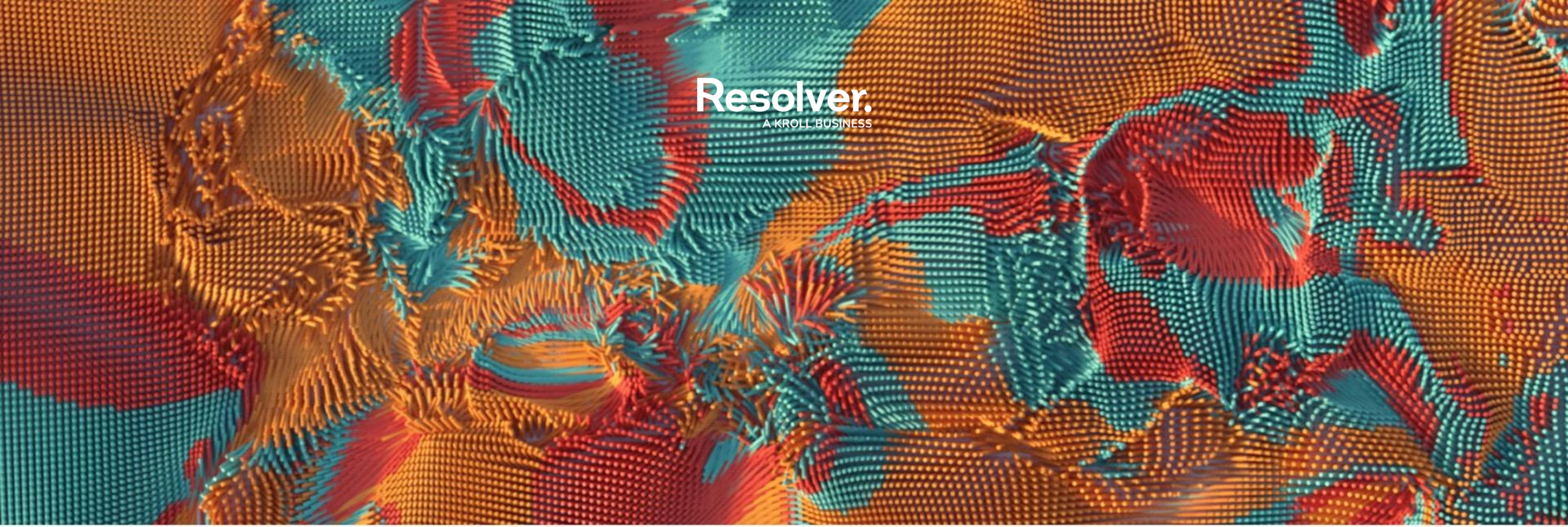
The Regulation establishes standard templates for the information register, essential for internal ICT risk management, effective supervision by authorities, and oversight of critical ICT third-party providers.

1. Vendor details e.g. name and brand, country of registration, corporation number, registered address, governing law etc.
2. Start date, next contract renewal date as well as the end date and/or notice periods
3. Description of the service or function and types of data involved
4. Nature of the service or function and its criticality assessment
5. Whether the service or function supports business operations that are time-critical
6. Type of services and deployment models, nature of data to be held and storage locations (regions or countries)
7. Date of the most recent assessment of criticality of the service or function and the next assessment date
8. Date of the most recent risk assessment/audit with a brief summary of results, and the next risk assessment date
9. The individual or decision-making body in the firm that approved the third party
10. Vendor details for any other parties to which there is material sub-outsourcing or delegation
11. Estimated annual budget cost associated with the service or function

Non-critical third-party management

We expect that firms will have flexibility to define the information to be included in the register based on the nature, scale and complexity of the risks inherent to the outsourced function or service being provided.

Resolver.
A KROLL BUSINESS



Proportionality

Microenterprise

Proportionality is a key concept in DORA, with one example being less stringent requirements for “micro-enterprises”

MICROENTERPRISE	REQUIREMENT	FULL SCOPE FIRMS
✗	Governance requirements relating to establishing a specific role and designating a senior manager to be responsible for overseeing risk	✓
✗	Assigning ICT risk to a control function, ensuring segregation and independent audits	✓
✗	Annual ICT risk assessment on legacy systems, risk assessment on each major change in network and information system infrastructure or procedures affecting ICT supported business functions, information assets or ICT assets	✓
✗	Crisis management function and procedures for internal and external crisis communications	✓
✗	Maintain redundant ICT capacities equipped with resources, capabilities and functions that are adequate to ensure business needs although they must assess the need to maintain such redundant ICT capacities based on risk profile	✓
✗	Monitor relevant technological developments on a continuous basis, also with a view to understanding the possible impact of the deployment of new technologies on ICT security requirements and digital operational resilience and keep up-to-date with the latest ICT risk management processes	✓

Poll 2: Have you established whether your organization is a microenterprise or a full scope firm, or is this still to be done?

A) Yes

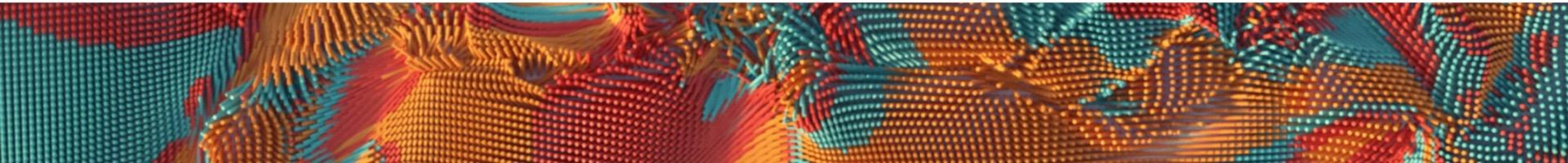
B) No

C) Not yet started

D) Finding it difficult to understand the rules

Resolver.
A KROLL BUSINESS

Key Challenges & How to Navigate Them



Potential Pitfalls & Recommendations

STAKEHOLDER AWARENESS/BUY-IN

- Communicate, educate, and garner support from senior stakeholders for DORA implementation.

DORA REQUIREMENTS (RTS)

- Conduct gap analysis and document interpretation of each requirement for regulatory and internal audits.

PROPORTIONALITY CONCEPT

- Use ”proportionality” to flexibly adhere to DORA requirements in a risk-based, business-aligned manner.

DORA ICT 3RD PARTY REGISTERS

- Assign clear ownership and accountability for these registers within your organization.
- Automate register population and maintenance as much as possible.

IMPROVING SECURITY POSTURE

- Ensure controls and processes are effective and repeatable beyond compliance.
- Establish appropriate governance and reporting metrics up to the board.

Poll 3: What is your organization's biggest challenge in achieving DORA compliance?

A) Understanding DORA requirements

B) Budget constraints for necessary technologies

C) Integrating new solutions with existing systems

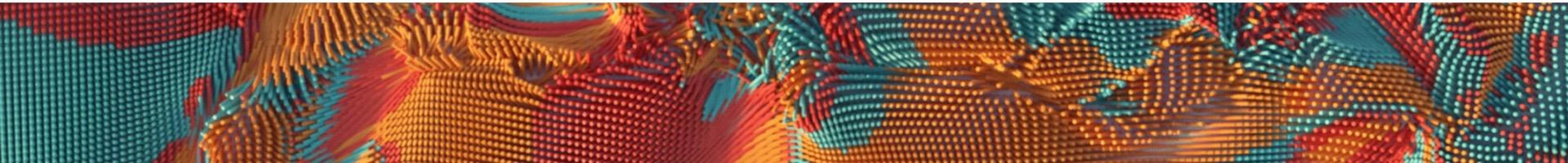
D) Lack of skilled personnel

E) Managing different aspects of operational resilience

F) None of the above

Resolver.
A KROLL BUSINESS

Kroll's DORA Services & Offerings



KROLL

Our Methodology

Delivery over four phases

Preliminary Phase

Determine the ICT risk management framework that is applicable to the Firm or the Group under DORA (full scope, simplified framework or microenterprise regime)

Phase 01

Perform an operational resilience gap assessment against the provisions of DORA and draft RTS

Phase 02

Develop a roadmap for achieving DORA compliance and strengthening the digital operational resilience framework

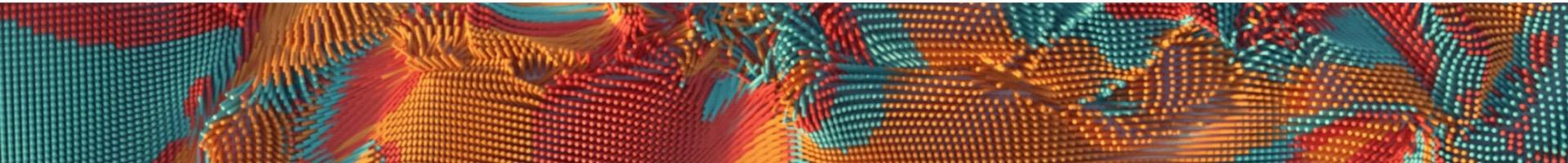
Phase 03

Assistance in implementing remedial measures

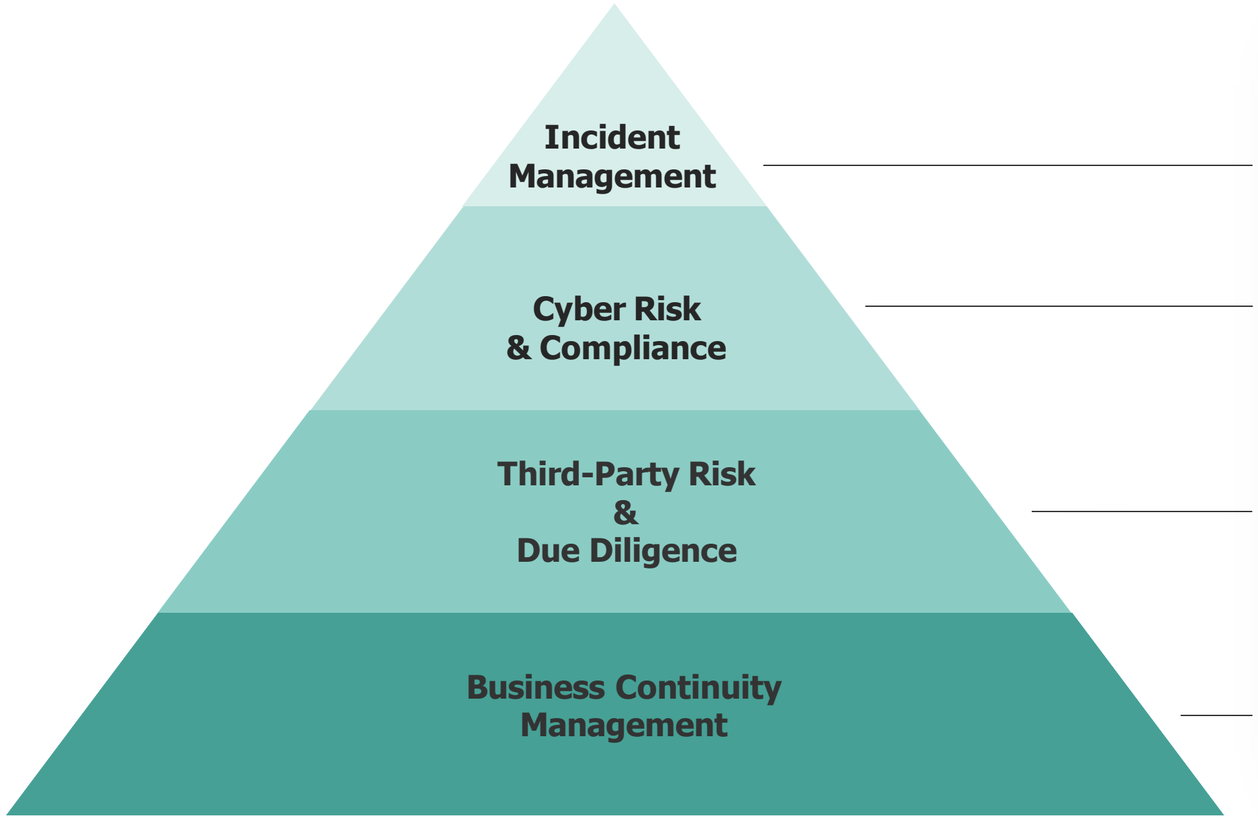
Resolver.
A KROLL BUSINESS

Resolver.
A KROLL BUSINESS

Building Operational Resilience with Resolver



Managing DORA Compliance with Integrated GRC Technology

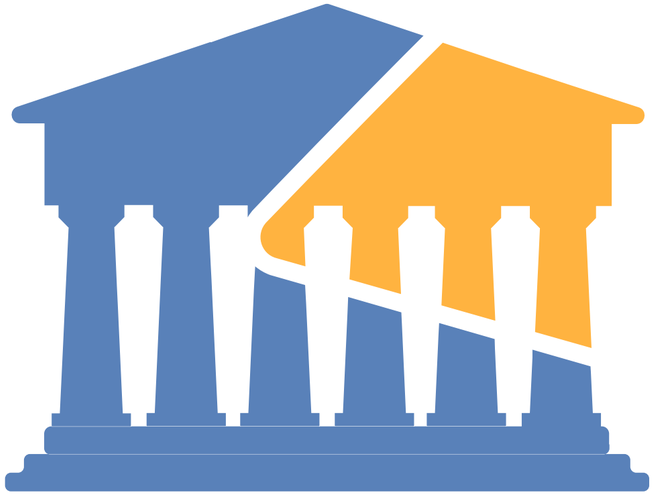


Purpose-built for financial organizations, the tool empowers teams to prepare and achieve DORA compliance with ease.

By improving visibility into all Information and Communications Technology (ICT) related incidents, cyber risks, threats, vulnerabilities, and critical third-parties, get a holistic view into your obligations, all in **one platform.**

Resolver.
A KROLL BUSINESS

The Challenge with Manual Compliance



- ✓ Delayed incident detection and reporting.
- ✓ Prone to errors, which can lead to inaccurate assessment of third-party risks.
- ✓ Incomplete or inaccurate compliance records.
- ✓ Extensive manpower required for manual risk tracking.
- ✓ Increasingly difficult to scale.

Resolver.
A KROLL BUSINESS

Integrated GRC

- **Regulatory Library**
- **Automated Regulatory Updates**
- **Risk-Based**
- **Risk Assessments**
- **Alerts**
- **Board & Regulator Reports**

Regulatory Compliance Management

AI-powered RegTech Solution uses algorithms to analyze regulations and build an **inventory of regulatory requirements**

Reconcile regulatory obligations with ease against an **integrated controls library**

Monitoring of regulatory change through alerts and notifications

Effective issue management by assigning clear accountability and aligning on remediation

Communicate real-time metrics of compliance coverage, assessment completion, risk exposure, and driving continuous improvement.

Resolver.
A KROLL BUSINESS

Regulatory Change Automation

Resolver.
A KROLL BUSINESS

Incident Management

- **Incident Detection and Reporting**

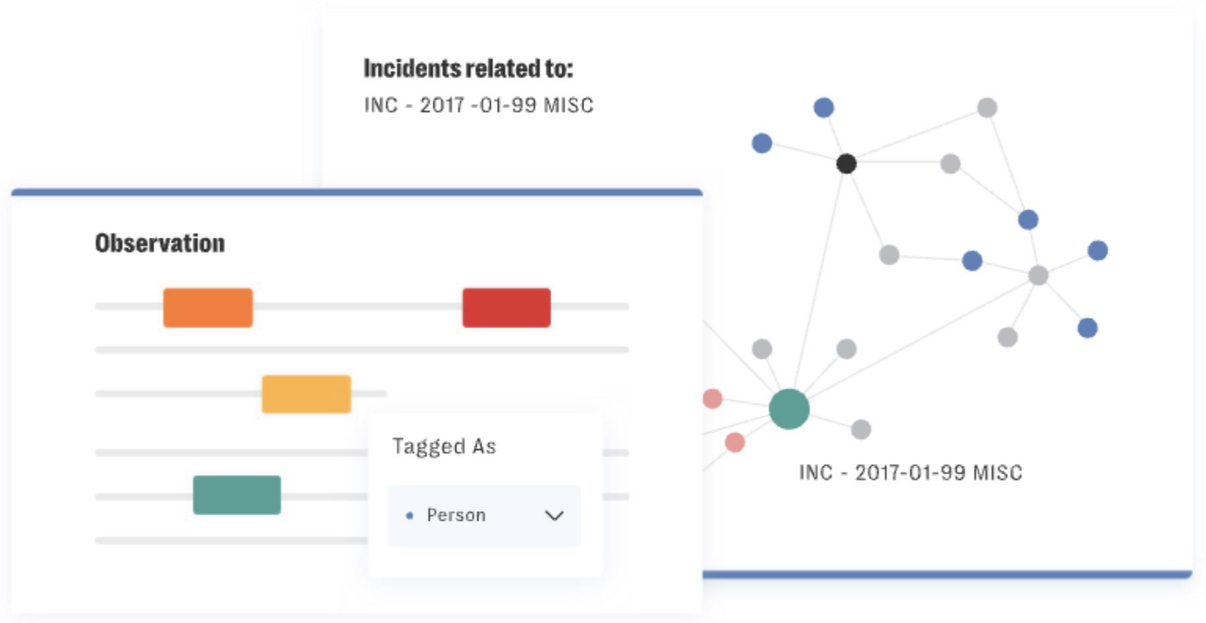
  Establish procedures to identify, track, log and categorize, and classify ICT-related incidents according to their priority and severity.

- **Automated Response Workflows**

  Streamline reporting, communication, and response workflows for ICT incidents to enhance efficiency.

- **Incident Analysis and Root Cause Identification**

  Facilitate post-incident reviews to analyze causes and identify areas for improvement effectively.



Resolver.
A KROLL BUSINESS

Cyber Risk & Compliance

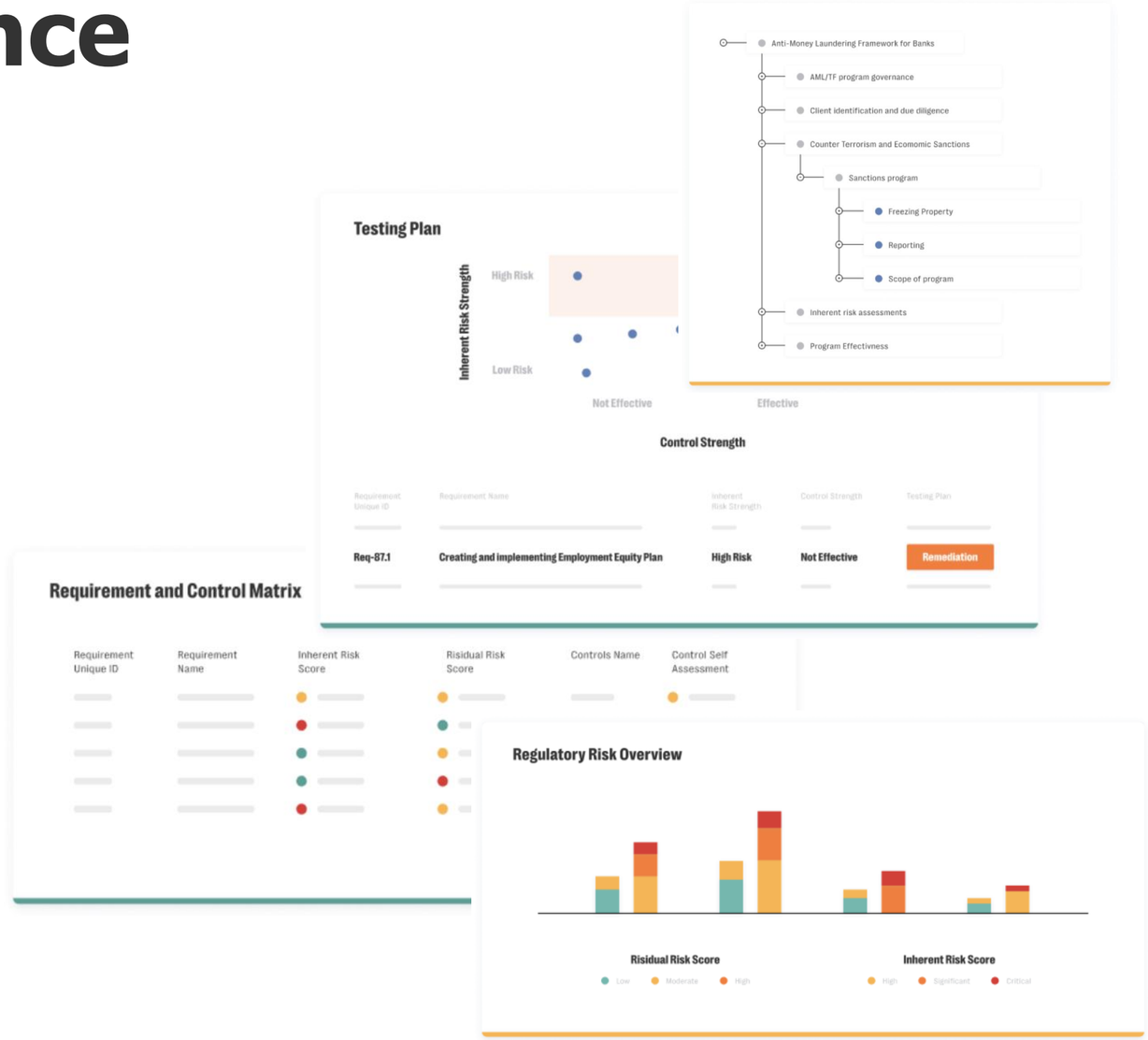
- **Risk Visibility**
  Achieve 360-degree visibility of ICT risks by linking IT assets to threats and vulnerabilities.

- **Central Risk & Controls Repository**
  Maintain a single repository for all ICT risks, assets, threats, and controls.

- **Risk Assessment and Scoring**
  Evaluate and prioritize risks based on impact and likelihood.

- **Continuous Control Monitoring**
  Maintain IT controls and map them to processes, risks, and regulations.

- **Standardize Control Sets**
  Apply uniform control sets across multiple IT standards to eliminate duplication.



Resolver.
A KROLL BUSINESS

Third-Party Risk & Due Diligence

- **Simplified Vendor Onboarding**
  Automate IT vendor screening and onboarding with reliable alerts and validations.
- **Pre-Defined Assessment Questionnaires**
  Ready-to use questionnaires to systematically evaluate vendor risks.
- **Periodic Due Diligence**
  Regularly assess and manage risks from IT vendors and third parties to ensure compliance.
- **Automated Workflows**
  Automate risk assessments, vendor monitoring, and mitigation strategies to save time.
- **Structured Information Management**
  Centralize and manage contracts and third-party risk information for transparency and compliance.

Resolver.
A KROLL BUSINESS

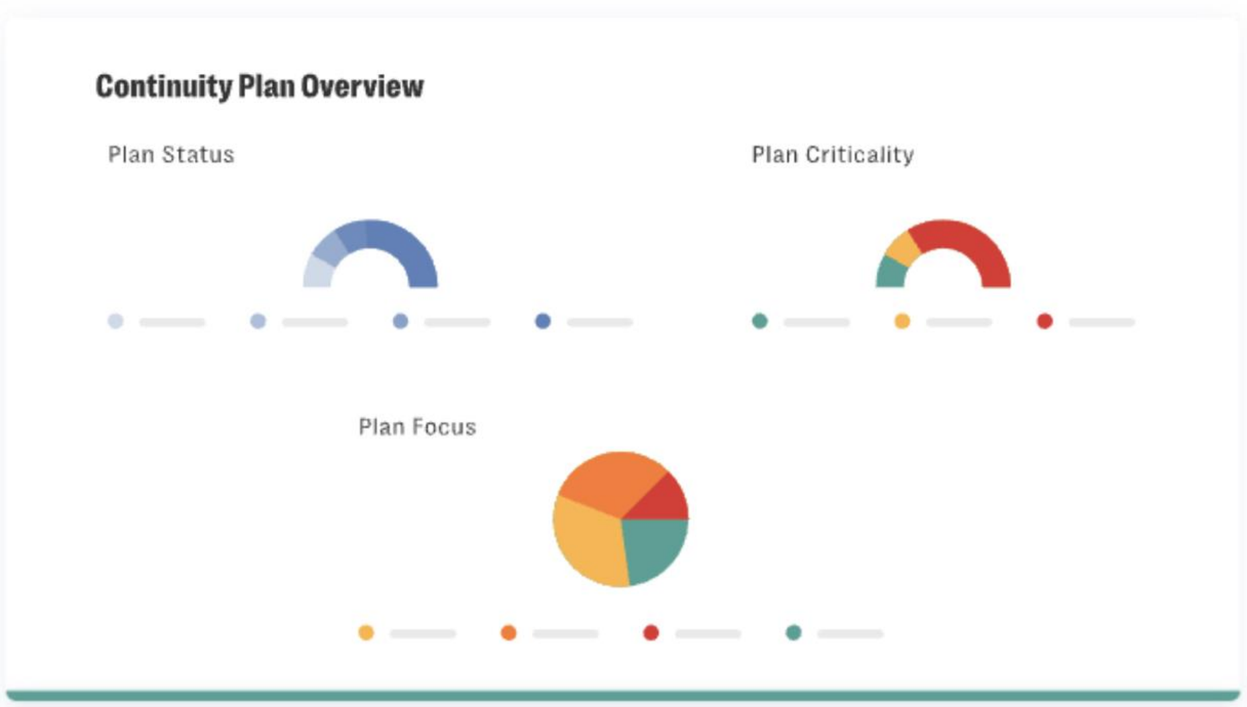
Business Continuity Management

- **Resilience Planning and Testing**
  Develop and rigorously test business continuity and operational resilience plans to ensure robust preparedness for disruptions.

- **Impact Analysis**
  Conduct detailed business impact analyses to identify critical functions and dependencies, prioritizing recovery efforts accordingly.

- **Crisis Management**
  Establish crisis management capabilities to effectively coordinate response efforts and sustain operations during disruptions.

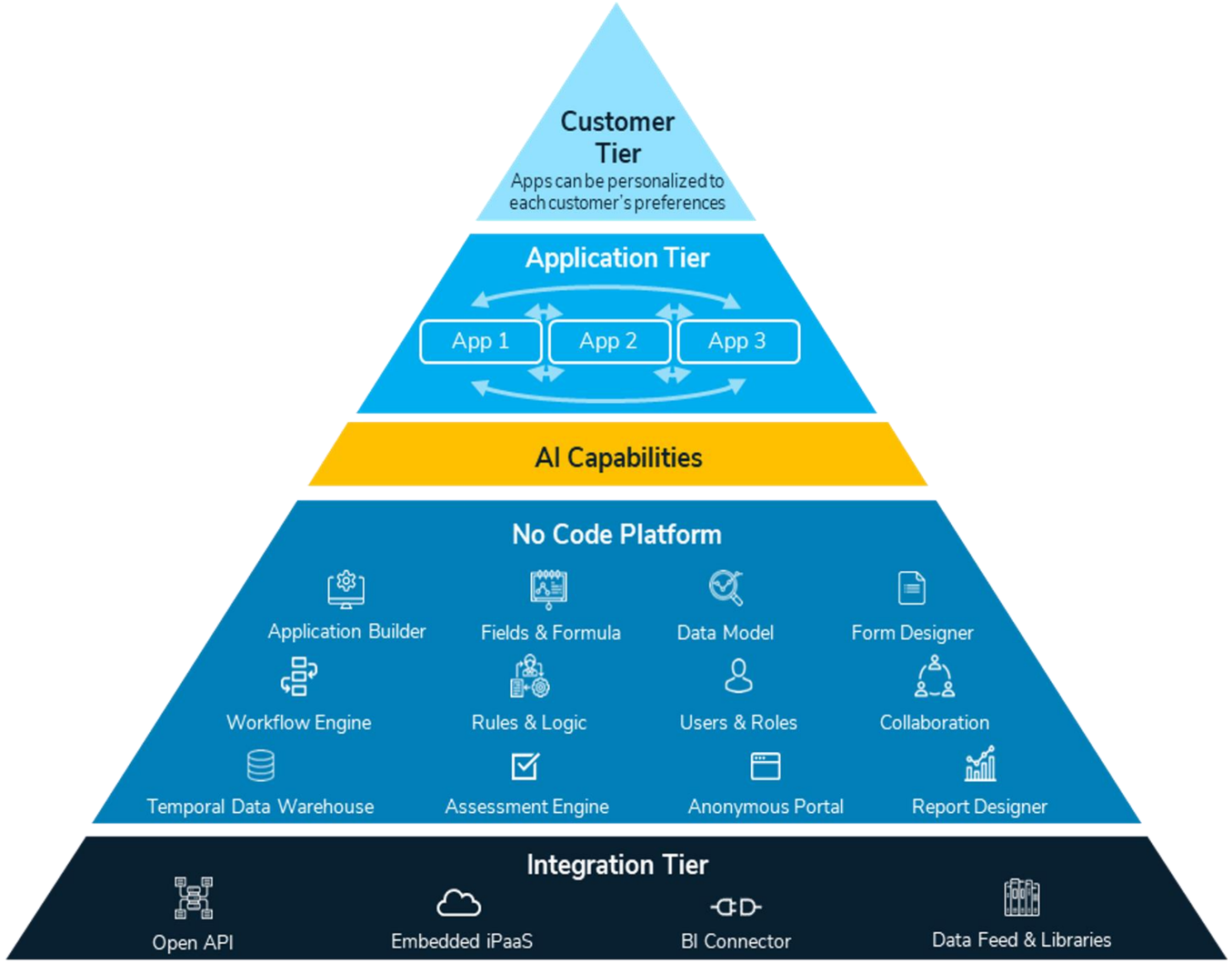
- **Real-Time Monitoring and Reporting**
  Continuously monitor and report on the status of resilience and continuity measures in real-time, to facilitate continuous improvement.



Resolver.
A KROLL BUSINESS

Product Pyramid: Resolver CORE

- ✓ No-code platform (CORE)
- ✓ Strong Integrations (using Workato)
- ✓ Analytics, AI, Automated Reporting



Resolver.
A KROLL BUSINESS

Resolver's Enterprise Resilience Value Chain

01

Understand Risk

Use **Risk Intelligence** to see the full business impact of risks across your enterprise, so you can prioritize and address them effectively, safeguarding your organization.

02

Build Resilience

Withstand or quickly bounce back from any risk event, incident, or crisis. Proactively plan and prepare for future challenges to reliably meet objectives.

03

Get Stronger

Achieve Enterprise Resilience to fortify your business. Protect your brand, save money through efficient risk workflows, and increase your market valuation.

Resolver.
A KROLL BUSINESS


Thank you
Resolver.
A KROLL BUSINESS