

# Maintaining the resilience of digitalized ecosystems

Effective oversight of FMIs

---

**Anne Leslie**

Senior Managing Consultant

Security Intelligence & Operations Consulting

IBM Security Centre of Competence Europe

# International context

Financial Services is one of the

**most attacked  
sectors**

# 72%

of the Financial Security Board's (FSB) members indicated in 2017 that they intend to release new standards or supervisory initiatives on cyber security in financial services\*

Building cyber resilience in the financial services sector is a fast-growing priority for all industry stakeholders, from the financial institutions (FIs) themselves, to their technology and service providers and especially policy makers, regulators and supervisors.

While banks are mobilizing significant resources to improve their defenses and ability to respond to cyber threats, supervisory bodies are also increasingly active. Given the potential divergence between the cyber priorities of individual FIs and the systemic viewpoint of supervisors (whose mandate is to ensure financial stability of the industry as a whole), we may see supervisory bodies compelling FIs to revise their cyber strategy and reprioritize certain actions deemed essential from a systemic perspective.

# An indication of future challenges...

**Anil Kashyap, a member of the Bank of England Financial Policy Committee, has warned it is only “a matter of time” before Britain is hit by a state-backed cyber attack that could corrupt the financial system. UK banks should be prepared to tackle huge data breaches and a cyber attack that may corrupt their records.**

Banks' cyber security efforts have mostly been concerned on how to prevent service outages, and the authorities so far haven't paid much attention to probable attacks that seek to falsify transaction records or corrupt data illegally. However, the supervisory focus of the authorities is shifting.

**Operational resilience of the banks is now considered just as important for regulators and supervisors as solvency and liquidity resilience, the areas that failed in the 2008 financial crisis.**






The image is a screenshot of a news article from the Central Banking website. The header features the 'CENTRAL BANKING' logo and a search bar. A navigation menu includes links for Monetary Policy, Financial Stability, Fintech, Economics, Governance, Reserves, Currency, and Directory. The article is categorized under 'CYBER' and is dated '19 Jun 2019'. The main headline reads 'BoE's Kashyap warns banks vulnerable to state-sponsored cyber attacks'. Below the headline is a graphic showing several padlocks of various colors (blue, red, white) against a dark background with glowing binary code and hexadecimal characters. The article text states that Bank of England policy-maker Anil Kashyap has warned banks may not be able to defend themselves from a state-sponsored cyber attack. A quote from Kashyap is provided: 'A "data integrity breach" is a key concern, said Kashyap, an external member of the BoE's financial policy committee, during remarks to the UK's Treasury Committee.'

# Industry trends in Financial Services

# More open systems, outsourcing and third party services

In response to the systemic digitalization of financial services and the advent of Open Banking, outsourcing is allowing financial institutions (FIs) comparatively early access to new technologies, generating:

-  Access to economies of scale (more efficient resource utilization, 'state-of-the art systems')
-  Changes in corporate cost structures (with 'pay-as-you-use' models transforming large upfront fixed costs into variable costs, and re-directing investment formerly consumed by in-house personnel, infrastructure development and maintenance)
-  Flexibility and scalability (on-demand infrastructure, scaling up and down as needed, to align with the agility required to execute on business strategy)

These benefits are crucial enablers of innovation and competitive advantage, allowing FIs to re-engineer how their businesses operate from the inside out, adapting their cost structure and organizational agility to the reality of a low-interest rate environment, high regulatory scrutiny, ferocious competition and changing customer expectations. However the evolving business/technological environment is causing parallel changes in the threat landscape and risk profile of individual firms and the financial system as a whole.

# The Financial Services Threat Landscape.

February 2019



- Hackers try o withdraw **€13 Mn**
- Systems shutdown
- **Branches & ATM closed**
- Mobile & Internet banking and **Internal email** suspended

December 2018

**Multiple Eastern Europe Banks**

- Millions lost from **physical cyber attacks**
- **Raspberry Pi** devices plugged into meeting rooms & offices
- GPRS/3G/4G/LTE used to access Web Servers, shared folders, etc.

October 2018



- **\$15.3 Mn across 5 entities lost** in cyber attack
- **Electronic payments infrastructure** targeted

June 2017



- **Extortion** campaign linked to **NotPetya**
- **3400 staff** and operations in **16 countries impacted**

January 2017



- Massive **DDoS attacks last 2 days**
- **Disruption** of various online banking
- Several customers impacted

November 2016



- Customer online accounts frozen for 48 hours
- **£2.26 Mn stolen**
- **Oct 2018** - £16.4 Mn fines

## ➔ Multiple threat actors groups

Nation-state Actors

Insiders

Cyber Criminals

3<sup>rd</sup> Parties

Hacktivist

.....More

## ➔ with varied motivations...

Financial Theft

Extortion / Ransom

Customer PII Data

Disrupt Services

Sensitive IP Theft

Fraud

## ➔ attacking critical systems...

Online Banking

Mobile Banking

Payment Infra (SWIFT)

ATM Systems

Customer PII

.....more

## Cyber attack could cost bank half of its profits, warns IMF

“In a severe scenario – in which the frequency of cyber-attacks would be twice as high as in the past with greater contagion – **losses could be 2.5-3.5 times as high as this, or \$270 billion to \$350 billion.**”

– June 2018



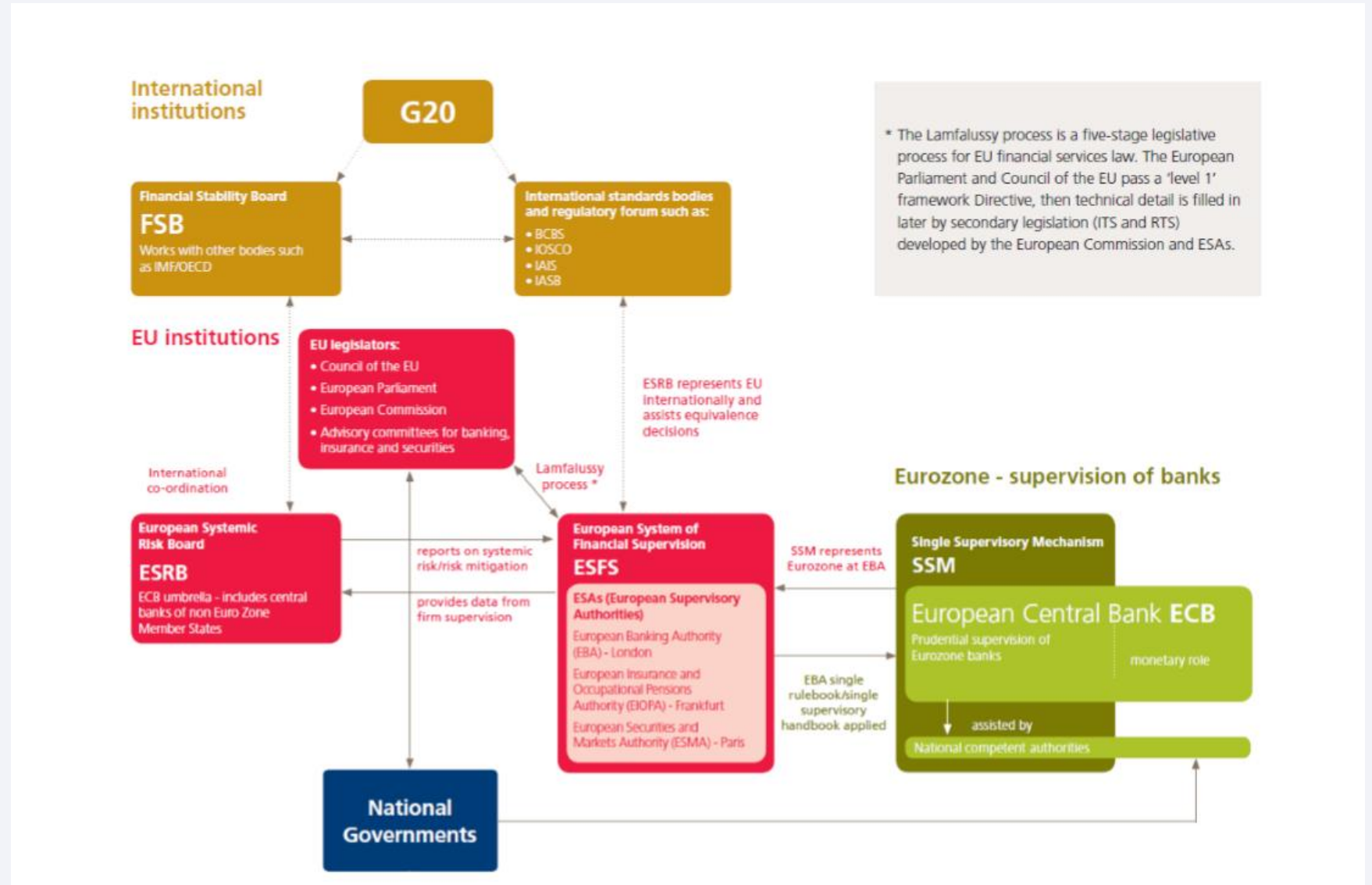
# Focus on EU Supervision & Regulation of Cyber & IT Risk

# The European System of Financial Supervision

The European System of Financial Supervision (ESFS) is a network centered around three European Supervisory Authorities (ESAs), the European Systemic Risk Board and national supervisors. Its main task is to ensure consistent and appropriate financial supervision throughout the EU.

As the Eurozone banking supervisor, the ECB closely cooperates with the ESAs, especially the European Banking Authority (EBA).

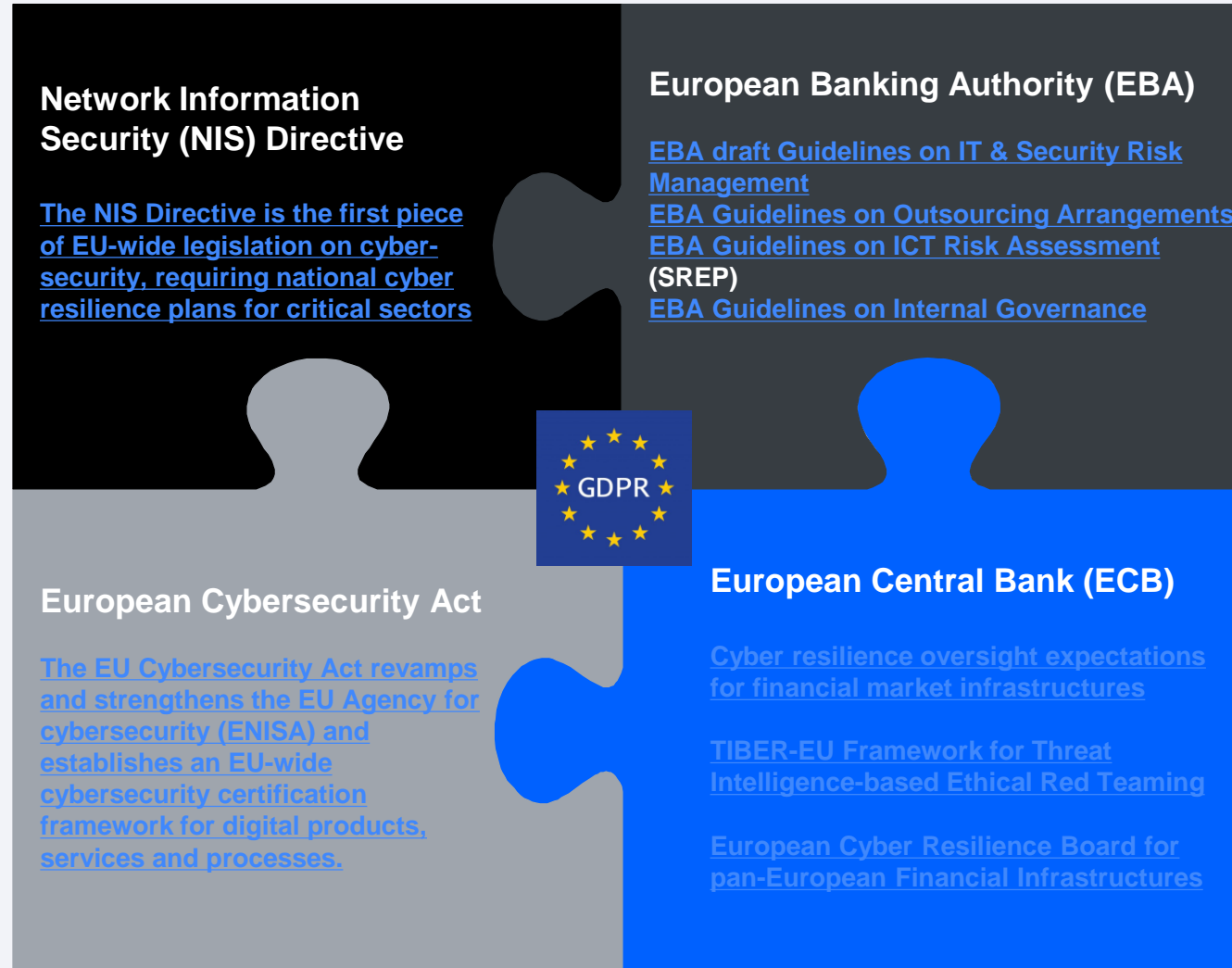
The ESFS covers both macro-prudential and micro-prudential supervision.



# Cyber resilience regulatory initiatives in the European Union

The European Union is actively reinforcing its policy arsenal in the area of cyber resilience.

Individual member states may have additional policy requirements which 'gold-plate' the European baseline, and which supplement the effort required for financial institutions and their providers.



# Examples of Member State cyber resilience regulatory initiatives

## UNITED KINGDOM

- [Financial Policy Committee](#)
- [CBEST testing](#)
- [Senior Managers Regime](#)
- [FCA Guidance on Cloud Computing](#)



## FRANCE

- [ACPR cyber security self-assessment for less significant institutions](#)
- [ACPR Guidance on Cloud Computing](#)



## ITALY

- [Bank of Italy \(BOI\) retail payment system regulations](#)
- [Bank of Italy cyber security guidance](#)
- BOI/CONSOB regulation of banks investment firms and trading venues



## GERMANY

- [IT Security Act](#)
- [BaFIN/MaRISK](#)
- [Banking Act](#)



## SPAIN

- [National Centre for the Protection of Infrastructure and Cyber Security](#): assessment of operational risk in critical firms



## NETHERLANDS

- [TIBER](#): red team [scenario testing](#) for the cyber resilience of critical firms



# Operational resilience: a new area of regulatory & supervisory focus

*“Banks must continue to provide good value for money and high-quality services to their clients. Regulators and supervisors must continue focusing on maintaining the stability of banks and the banking system. Let us therefore embrace technological change where it helps us achieve these stable long-term objectives. I believe we are already making on all sides significant progress in this work.*

*If we continue with the right attitude, we have an exciting time ahead - and together we can help generate a better banking system for customers and citizens into the future.”*

**Penti Hakkarainen**

ECB Supervisory Board, June 2018

# Key risk drivers in banking identified by the ECB for 2019



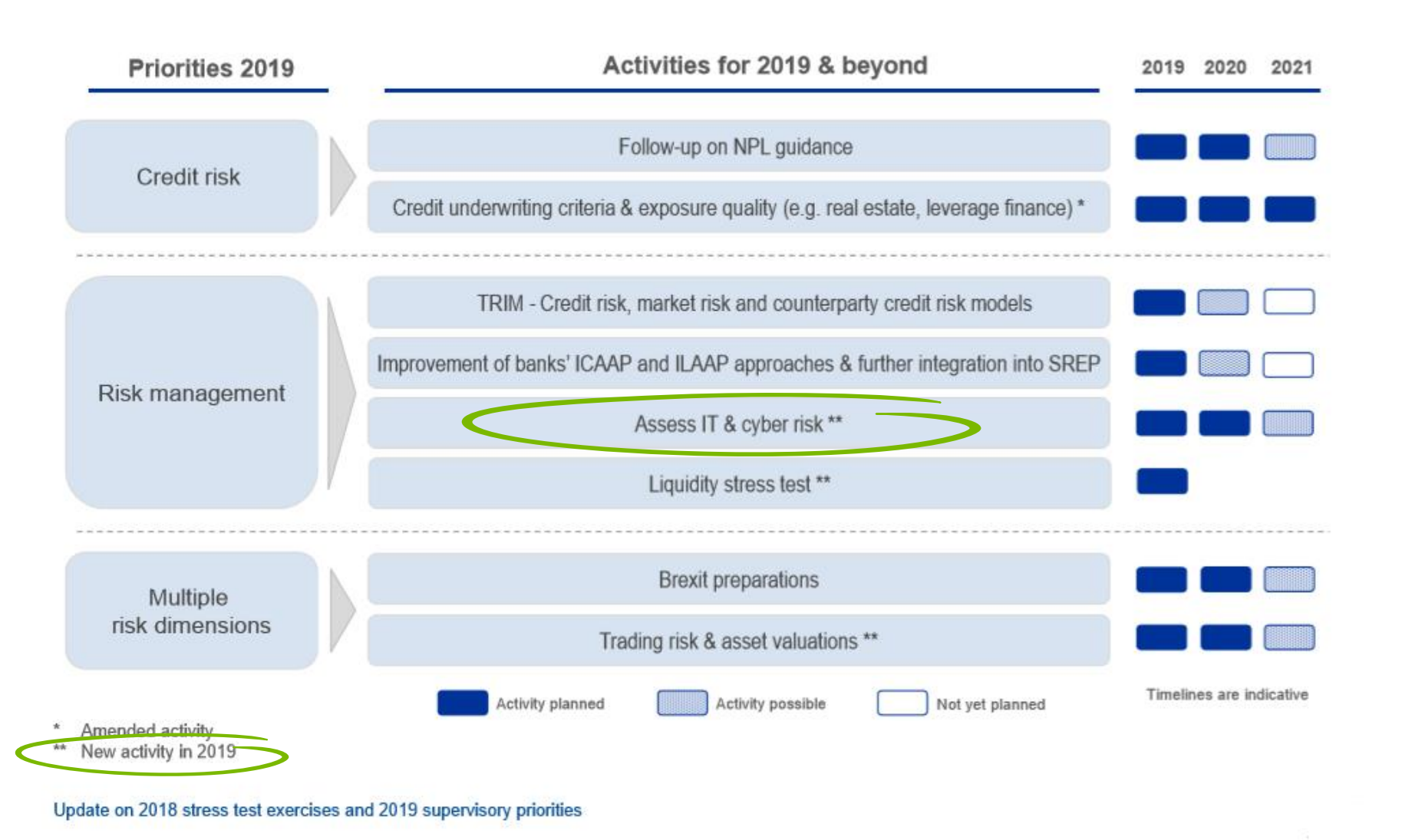
**Geopolitical uncertainties**

**Legacy and potential future non-performing loans (NPLs)**

**Cybercrime and IT disruptions**

*These are followed by repricing in financial markets, the low interest rate environment and banks' reaction to regulation*

# ECB Supervisory Priorities & Activities





# ECB Banking Supervision monitors how Eurozone banks manage their IT risks



**Continuous off-site supervision and risk assessments**

**Thematic and horizontal reviews of focus areas (e.g. cyber security, IT outsourcing, data quality)**

**Targeted on-site inspections (on IT risk areas in general, but also focused on IT security and cyber risk)**

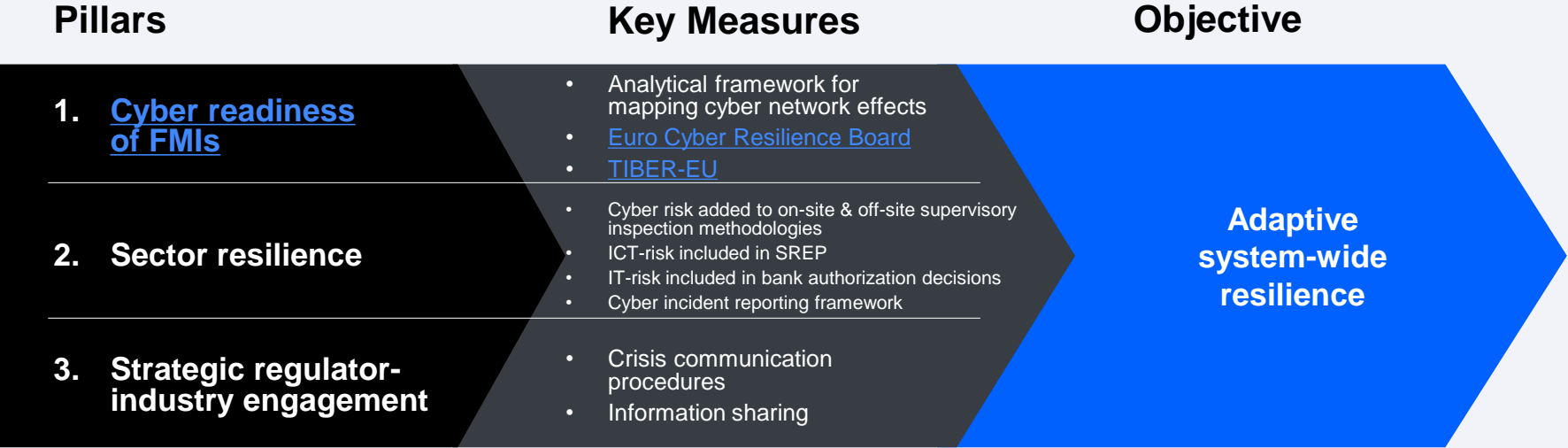
*Work is ongoing to issue guidelines on IT risk management (including cyber risk) for [significant credit institutions](#)*

# ECB Cyber Security Strategy

# ECB Cyber Strategy – supervision, capacity-building & engagement

The ECB has signaled that its cyber workstream will continue to gather pace in 2019 and beyond:

- TIBER-EU red-team testing framework
- Crisis communication procedures
- Regulator-industry information sharing

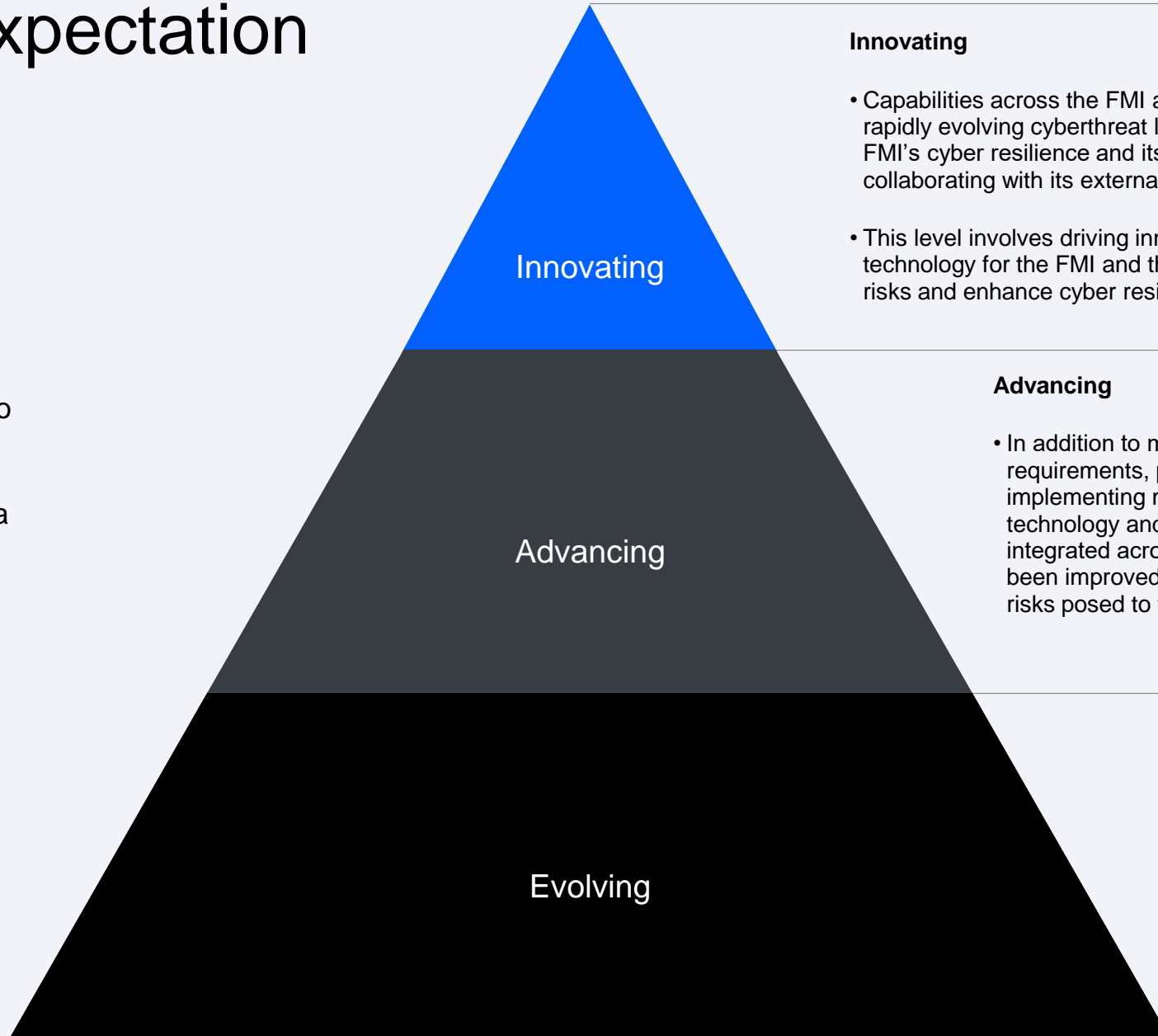


# 3 Levels of Expectation

The **continuous improvement** and **maturing** on the part of FMIs is the essence of these three levels of expectation.

Indeed, the levels of expectations are not designed to establish static requirements and an end state of cyber resilience, which risks creating a culture of complacent compliance.

Rather, **FMIs are expected to be constantly evolving, advancing and innovating in the light of the continuously evolving cyber threat landscape.**



## Innovating

- Capabilities across the FMI are enhanced as needed within the rapidly evolving cyberthreat landscape, in order to strengthen the FMI's cyber resilience and its ecosystem and by proactively collaborating with its external stakeholders.
- This level involves driving innovation in people, processes and technology for the FMI and the wider ecosystem to manage cyber risks and enhance cyber resilience.

## Advancing

- In addition to meeting the evolving level's requirements, practices at this level involve implementing more advanced tools (e.g. advanced technology and risk management tools) that are integrated across the FMI's business lines and have been improved over time to proactively manage cyber risks posed to the FM

## Evolving

- Essential capabilities are established, evolve and are sustained across the FMI to identify, manage and mitigate cyber risks, in alignment with the cyber resilience strategy and framework approved by the Board.
- Performance of practices is monitored and managed.

Essential capabilities are established, evolve and are sustained across the FMI to identify, manage and mitigate cyber risks, in alignment with the cyber resilience strategy and framework approved by the Board. Performance of practices is monitored and managed;

In addition to meeting the evolving level's requirements, practices at this level involve implementing more advanced tools (e.g. advanced technology and risk management tools) that are integrated across the FMI's business lines and have been improved over time to proactively manage cyber risks posed to the FMI.

Capabilities across the FMI are enhanced as needed within the rapidly evolving cyberthreat landscape, in order to strengthen the FMI's cyber resilience and its ecosystem and by proactively collaborating with its external stakeholders. This level involves driving innovation in people, processes and technology for the FMI and the wider ecosystem to manage cyber risks and enhance cyber resilience.

Domain	Expectations Level 1: Evolving	Expectations Level 2: Advancing	Expectations Level 3: Innovating	
Governance	<ul style="list-style-type: none"> <li>Internal cross-disciplinary steering committee</li> <li>Cyber resilience strategy</li> <li>Cyber resilience framework</li> <li>Involvement of the Board and senior management</li> </ul>	<ul style="list-style-type: none"> <li>Level 1 + Maturity models and metrics to assess adherence</li> <li>Formal process for continuous review &amp; adjustment</li> </ul>	<ul style="list-style-type: none"> <li>Level 2 + Cyber resilience strategy outlining future state resilience in terms of maturity and/or risk with short and long-term perspectives , continual improvement</li> <li>Structured contribution to resilience of ecosystem</li> </ul>	
Identification	Document all critical functions, key roles, processes, information assets + dependencies on 3 <sup>rd</sup> party providers; maintain up-to-date inventory of assets & accounts; use an ERM framework; conduct risk assessments; maintain simplified network map of resources.	Use automated AIM/IAM tools to ensure inventories and credentials are updated accurately and relevant staff are informed in a timely manner; maintain up-to-date and complete maps of network resources, data flows, etc.	Use feeds from AIM/IAM tools to identify emerging risks, update risk assessments and take mitigating actions in line with risk tolerance; coordinate with ecosystem to address collective vulnerabilities and threats.	
Protection	Processes and assets Control implementation & design Network & infrastructure mgmt Logical & physical security mgmt People/supplier/3rd party mgmt	Implement a defense-in-depth set of security controls to achieve the security objectives needed according to the risk assessment in the <i>Identification</i> phase and linked to the threat landscape. Monitor & audit effectiveness regularly.	Implement a bespoke ISMS based on international standards to establish, implement, operate, monitor, review, maintain & improve a comprehensive cybersecurity control framework. Embed resilience at get-go of all IT projects.	Perform frequent reviews of the ISMS using certification/audits/other assurance; develop processes and explore new technologies to constantly refine counter-measures; leverage intelligence and peer best practices.
Detection	Define and document baseline profile of system activities to detect deviation; monitor user activity/exceptions/cyber events/connections/external providers/devices/software; build multi-layered detection controls with alert thresholds.	Develop and implement automated mechanisms to correlate all alerts (SIEM); acquire a SOC-type capability to continuously monitor the IT environment, detect anomalous events and alert staff automatically to respond accordingly.	Predict attacks with intelligence-driven approach; develop threat detection capabilities of known/unknown threats, with correlation of vulnerabilities and threats; explore ways of inhibiting lateral movement (deception).	
Response & recovery	Incident management Data integrity Communication & collaboration Forensic readiness	Plan to operate in a diminished capacity in a range of scenarios; define RPOs/RTOs; develop & test incident response/resumption/recovery plans; define alert parameters & thresholds; conduct root cause analysis.	Design and test systems and processes to enable critical operations to be resumed safely within 2 hours of a cyber disruption and enable complete settlement by the end of the day, even in the case of extreme but plausible scenarios.	External collaboration to develop common plans in case of ecosystem-wide impact; implement a CSIRT; implement processes to manage incidents through automated responses triggered by pre-defined criteria.
Testing	Vulnerability assessments Scenario-based testing Red-team testing	Risk-based testing programme performed annually on critical systems, applications and data recovery, response, resumption, recovery, crisis communication , information back-ups; prioritization and remediation policies.	Embed testing in ERM; use threat intelligence to inform/update testing programme; use best practices and automated tools; perform SDLC testing at every stage and across all business levels.	Develop, monitor & analyze metrics to assess performance Regularly conduct tests with peers Engage proactively in industry/cross sector exercises Test the cooperation/sharing arrangements in place
Situational awareness	Cyber threat intelligence Information sharing	Establish a cyber threat intelligence gathering process from internal & external sources, including analysis and information sharing processes with internal and external stakeholders.	Continuously use cyber threat intelligence to anticipate attacks; develop/review/update a cyber risk dashboard ; include in threat analysis extreme but plausible events.	Ensure cyber threat intelligence gathering process includes threats from participants, service, utility providers and other FMIs; integrate and align cyber threat intelligence process with the SOC; bi-directional intelligence flow with SOC.
Learning & evolving	Cyber threat intelligence	Instill a culture of cyber risk awareness whereby the resilience posture, at every level, is regularly and frequently re-evaluated using : cyber threat intelligence/lessons learned/continuing cyber awareness training & materials/skills development/performance indicators on cyber resilience strategy and framework.	Monitor technological developments/new cyber risk management processes; possibly acquire such technology/know-how. Incorporate lessons learned into employee training and awareness programmes and risk mitigation capabilities, cyber contingency, response, resumption and recovery plans; track progress.	FMIs should have capabilities in place to use multiple sources of intelligence, correlated log analysis, alerts, traffic flows, cyber events across other sectors and geopolitical events to better understand the evolving threat landscape and proactively take appropriate measures to improve their cyber resilience capabilities.

# Euro Cyber Resilience Board

The [Euro Cyber Resilience Board](#) for pan-European Financial Infrastructures is a forum for strategic discussions between financial market infrastructures. Its objectives are to:

- raise awareness of the topic of cyber resilience
- catalyse joint initiatives to develop effective solutions for the market
- provide a place to share best practices and foster trust and collaboration

[ECRB Mandate](#) : the ECRB is composed of the members, which are representatives of pan-European financial market infrastructures and of their critical service providers.

The Chair appoints the members of the ECRB and their eventual alternates upon proposal of the institutions that they represent. Members and their eventual alternates are persons working at executive board level who are responsible for the daily conduct of business of the institutions they represent. Members and their eventual alternates are appointed for a period of two years. The representatives of the active participants are also persons working at executive board level. Those of the observers are persons working at least at senior management level.

## Initial list of institutions in accordance with Article 3(2)

*TARGET2/Target2Securities,  
EBA CLEARING (EURO1, STEP2-T),  
STET,  
equensWorldline,  
Iberpay,  
RPS/EMZ,  
Euroclear Group,  
London Stock Exchange Group (Monte Titoli , LCH Clearnet),  
BME Group,  
KDPW,  
EuroCCP,  
NasdaqClearing,  
Deutsche Börse Group (Eurex Clearing, Clearstream),  
SWIFT,  
SIA,  
Mastercard,  
Visa*

# TIBER-EU Framework

[TIBER-EU](#) is the European framework for threat intelligence-based ethical red-teaming. It is the first EU-wide guide on how authorities, entities and threat intelligence and red-team providers should work together to test and improve the cyber resilience of entities by carrying out a controlled cyberattack.

The [TIBER-EU framework](#) is designed for (supra)national authorities and entities that form the core financial infrastructure, including those whose cross-border activities fall within the regulatory remit of several authorities. It is applicable to entities not only in the financial sector but also in any other critical sector.

To ensure that the providers of threat intelligence and red-team services meet the appropriate standards for conducting a TIBER-EU test, entity being tested should carry out due diligence to make sure its selected provider meets all the requirements set out in the [TIBER-EU Services Procurement Guidelines](#).

The TIBER-EU framework is currently (being) implemented in [Belgium](#), [Denmark](#), Ireland and the [Netherlands](#) as well as by the ECB in its oversight capacity. Other jurisdictions are expected to follow soon.



A changing paradigm: from IT risk & cyber risk to operational risk



# 53%

of IT leaders don't know if their cybersecurity controls are working

# Cyber Risk is Operational Risk is Enterprise Risk

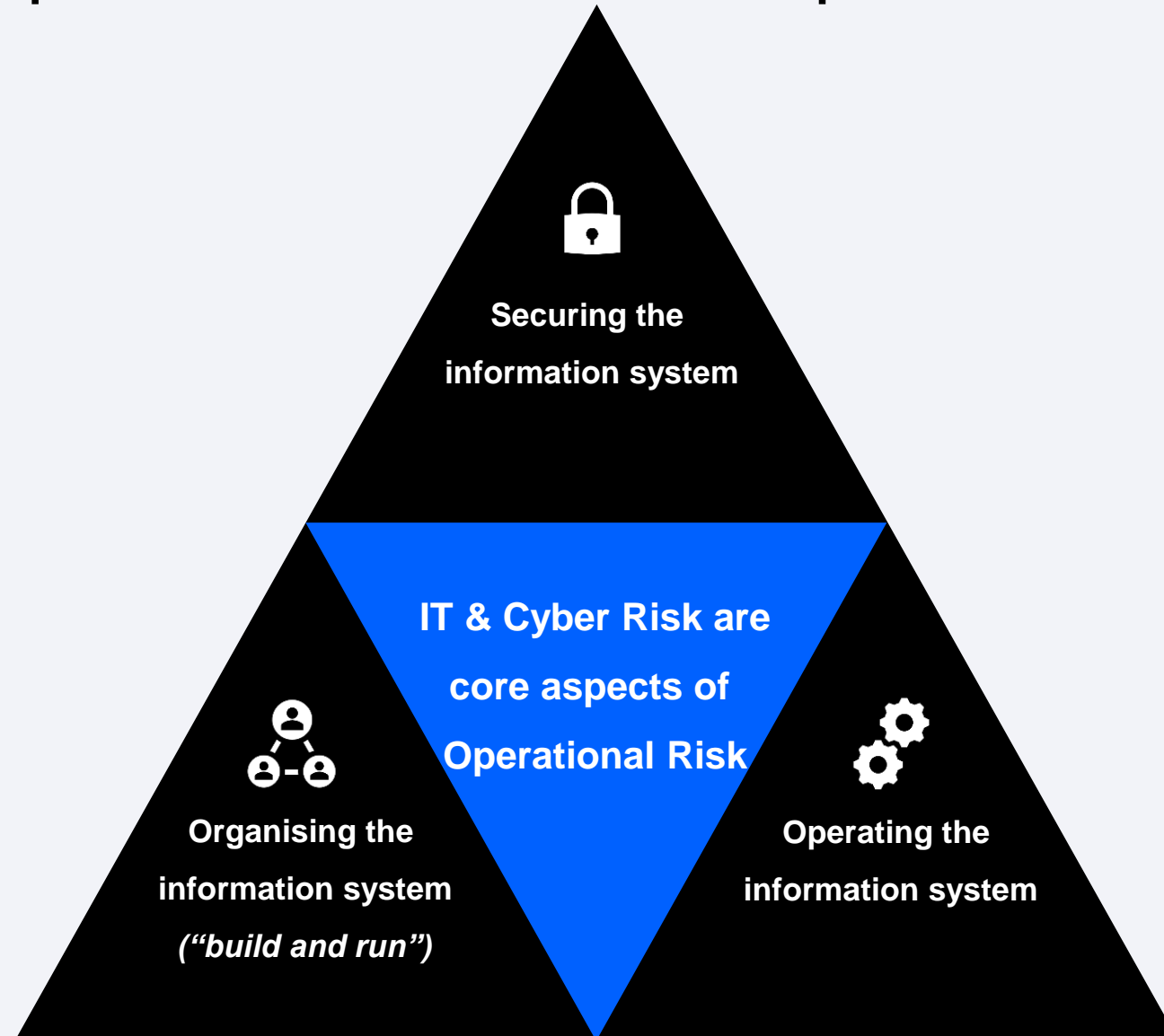
## A change of paradigm

**Financial institutions** have long relied on sound IT management principles published by various international standards bodies.

However, these **standards, developed by IT professionals, do not share the conceptual framework established by financial regulators**. The concepts of risk management, although similar, are not exactly the same and are not based on an internal control system.

Furthermore, **these standards are not embedded in the corporate governance system that regulators require institutions to put in place**.

Today, **IT & Cyber Risk Management is no longer a topic specific to IT teams** but must be deeply embedded within a holistic approach to risk control and risk management coordinated by the Enterprise Risk Management (ERM) function.



## Strategic alignment

**The management body of financial institutions must be directly involved in ensuring the alignment of the firm's IT strategy with its business strategy and risk appetite, as well as in implementing and monitoring the ERM framework.**

Firms' operational risk management reference frameworks must be refined to include all aspects of IT risk within the recognized categories of operational risk.

Through **assessment questionnaires and on-site inspections**, supervisory authorities are ensuring that institutions' IT risk management frameworks are not entirely decided and deployed by the IT department.

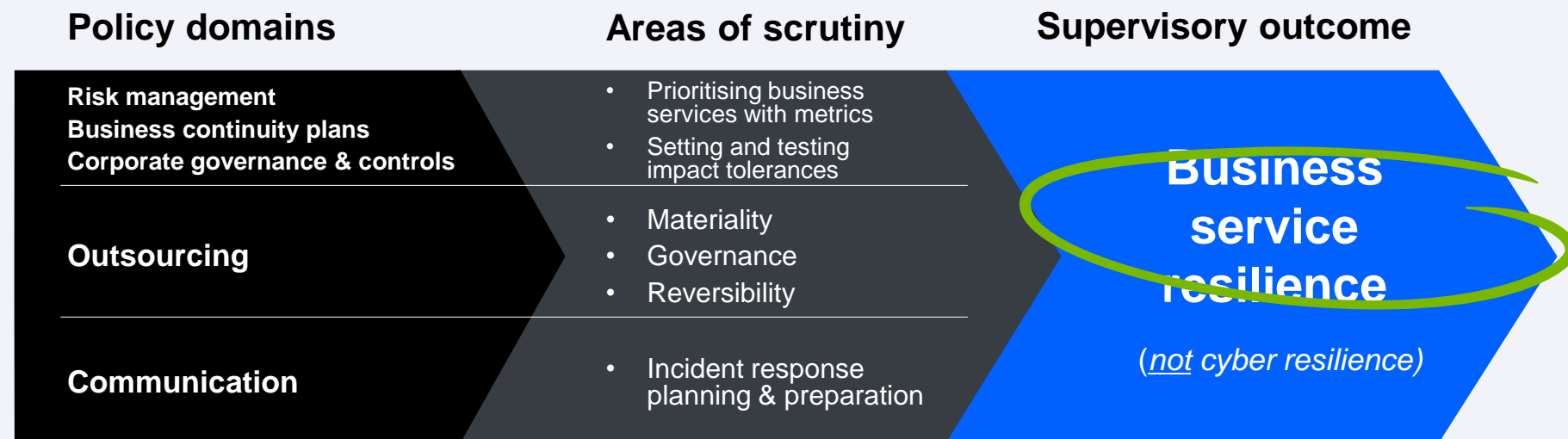
The requirement is that **security must be properly integrated into the firm's overall operational risk management framework** and managed with appropriate corporate governance mechanisms.

Looking forward: from operational risk to operational resilience

# Operational resilience: delivering continuity of business services in Financial Services

Supervisory authorities consider that firms and Financial Market Infrastructures (FMIs) are more likely to be operationally resilient if they **design and manage their operations on the assumption that disruptions will occur** to their underlying systems and processes.

Supervisors will be seeking assurance from firms that **appropriate impact tolerances** are set by the board and senior management, monitored and tested so that risks to financial stability and consumer harm are minimised.



# Operational resilience is everybody's responsibility

## Who is in scope?

Supervisory authorities, particularly in the UK, are considering that the requirements for operational resilience are applicable to all types of firms and financial market infrastructures (FMIs).

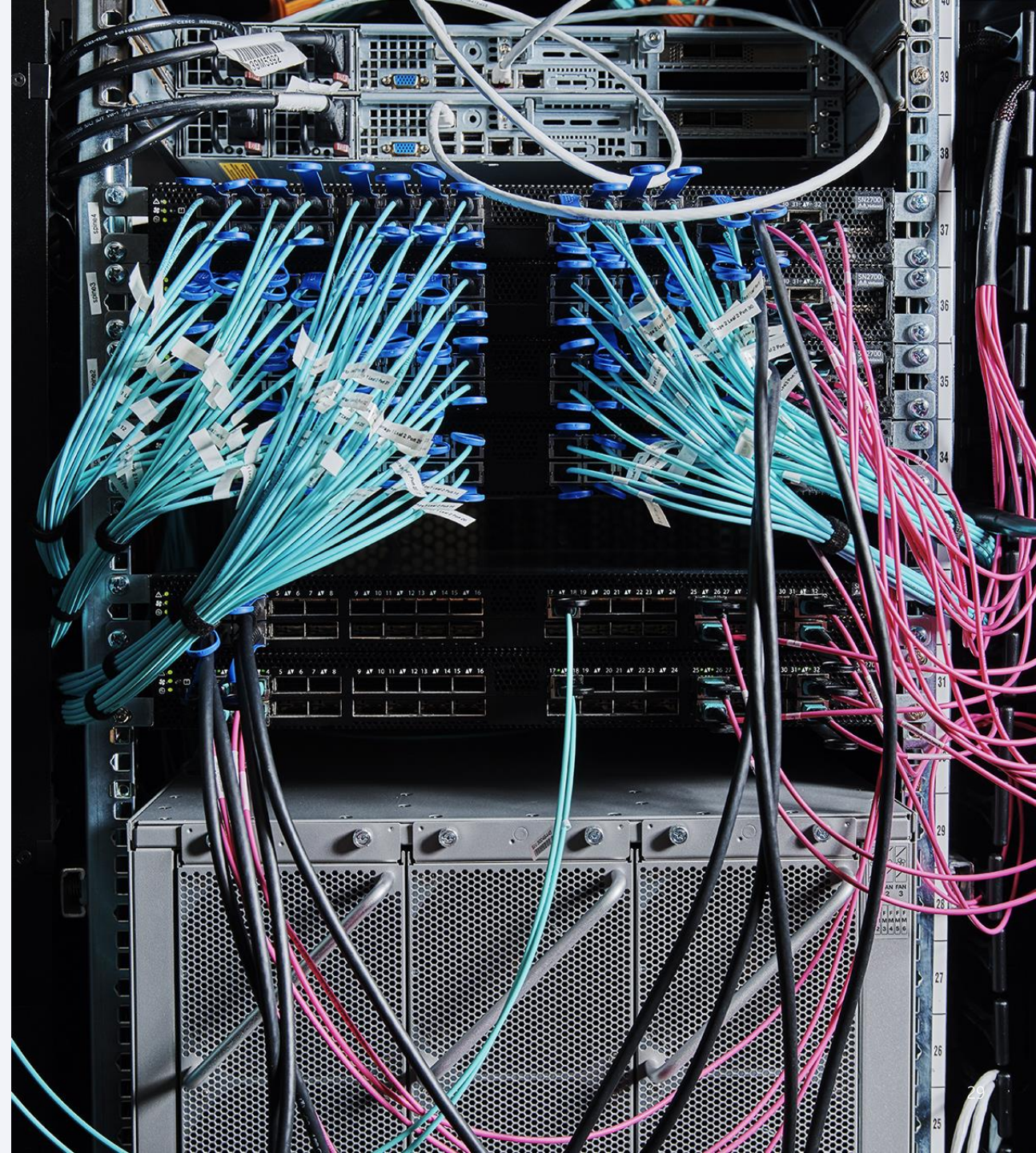
## To what extent?

The application of operational resilience requirements will vary depending on the nature and complexity of firms and FMI, as well as their size, activities and level of interconnectedness within the wider financial system.

## What action is required?

By answering the following two questions, firms and FMIs can identify how much work is ahead of them should supervisory policy change:

- ***Have we identified our business services in a way that allows us to link our activities to our business objectives and the objectives of the supervisory authorities?***
- ***Have we appropriately prioritized between business services to ensure the most important are resilient to operational disruption?***





# An iterative process for improving operational resilience



# Firms will need to be able to respond satisfactorily to regular supervisory reviews

- ✓ **Supervisory questionnaires**
- ✓ **Simulations**
- ✓ **Skilled persons' reports**
- ✓ **Thematic reviews**

## Policy Input:

- G7 Fundamental Elements of Cybersecurity

## Policy Input:

- CPMI – IOSCO Guidelines
- BCBS Corporate Governance Principles for Banks
- BCBS Principles for the Sound Management of Operational Risk

## Policy input:

- NCSC Cyber Assessment Framework
- NIST Cybersecurity Framework

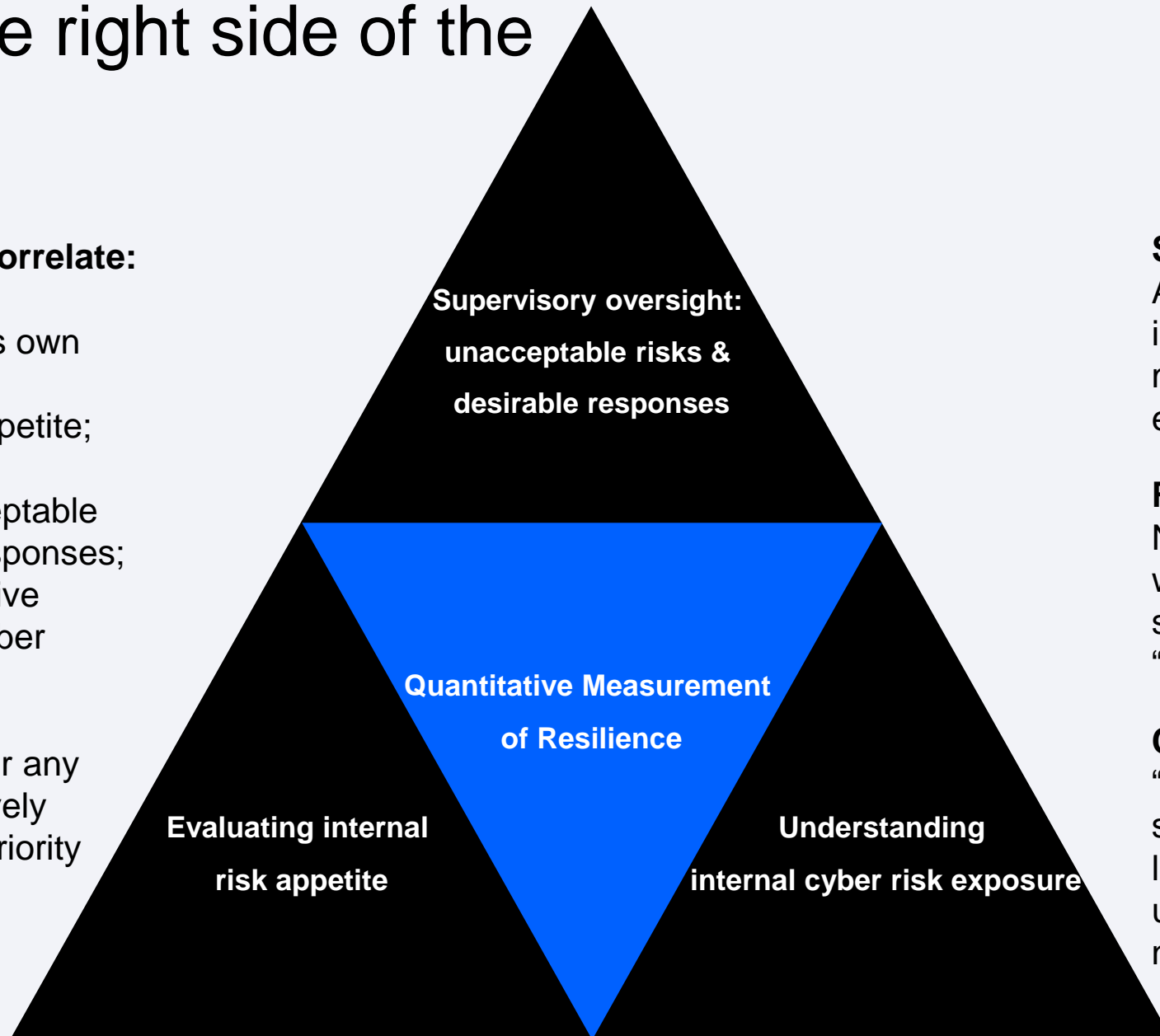
# Staying on the right side of the supervisors

Source: If applicable, describe source origin

## The ability for an FI to correlate:

- an understanding of its own cyber risk exposure;
- with its internal risk appetite;
- and the supervisor's perspective on unacceptable risks and desirable responses;
- resulting in a quantitative measurement of its cyber resilience

will be a valuable asset for any FI looking to engage actively with supervisors on this priority topic



## Supervisory oversight

Ability to cope with increasing scrutiny and more sophisticated evaluation methods

## Risk appetite

Necessary alignment of what FIs and their supervisors consider "acceptable risks"

## Cyber risk exposure

"*Know thyself*": the first step in building resilience lies in a comprehensive understanding of what needs to be done



From resilience to antifragility: cyber security is a journey,  
not a destination

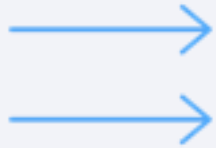
“Antifragility is beyond resilience or robustness. The resilient resists shocks and stays the same; the antifragile gets better.”

**Nassim Nicholas Taleb**  
**Antifragile: Things That Gain from Disorder, 2012**

# Shifting our thinking about security

## From security as a stand-alone function to security-as-a-system

Linear Thinkers	System Thinkers
Break things into component parts	Are concerned with the whole
Are preoccupied with content	Are concerned with the process
Try to fix symptoms	Are concerned with the underlying dynamics
Are concerned with assigning blame	Focus on enquiry in order to understand
Try to control chaos to create order	Try to identify patterns amid the chaos
Care only about the content of communication	Care about content but are more attentive to interactions and patterns of communication



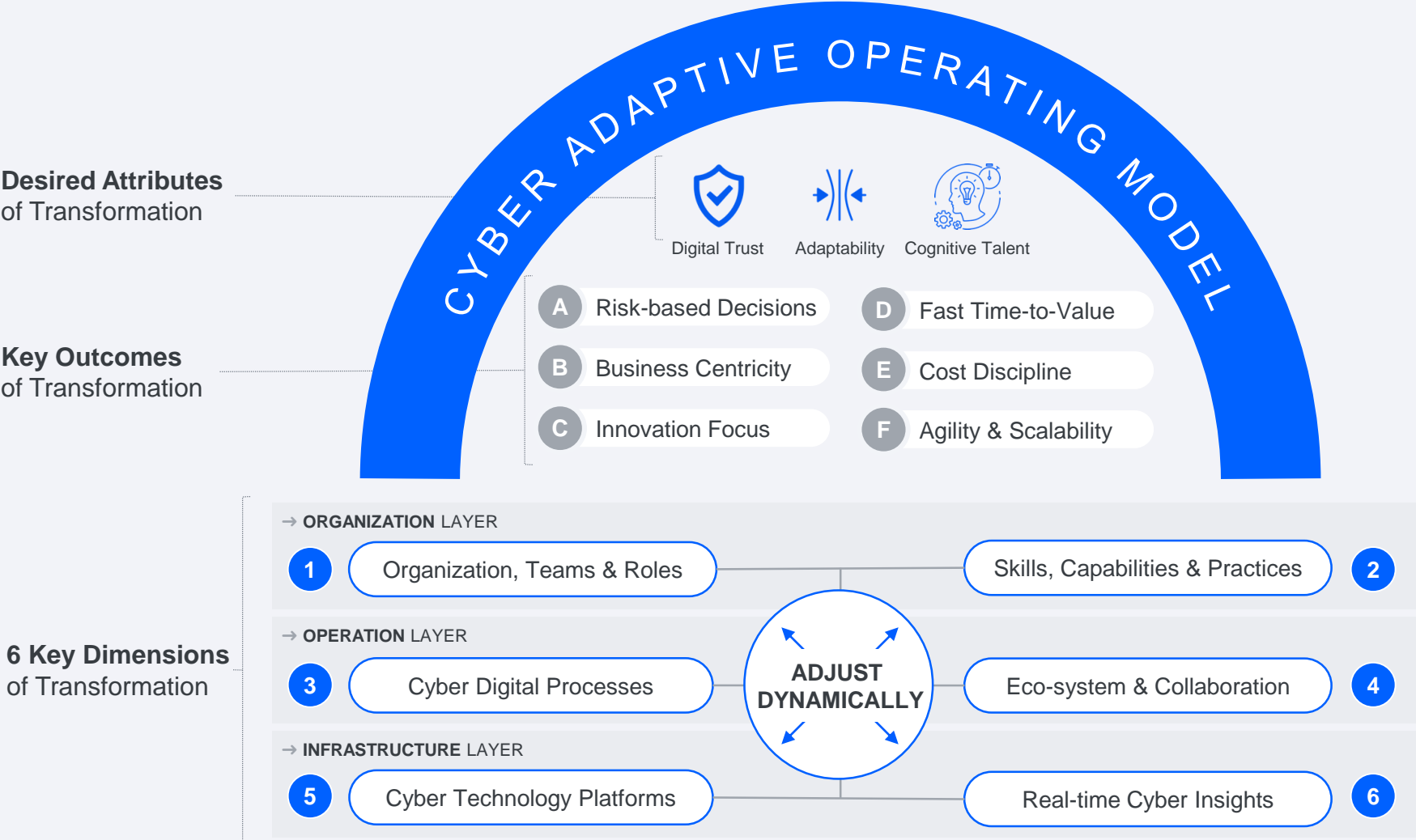
# We need a strategic and operational shift to build security-led resilience for better outcomes

Current state of affairs		A vision for the future
Uncoordinated effort in silos to meet protection goals	→	Integrated DevOps style Cyber Operations
Varying levels of cyber skills to execute mission	→	Rapid re-skilling to meet operational resilience mission of the business
Lack of a consistent way to deal with cyber events	→	Programmatic approach leading to faster response to cyber events
Blind spots arising from lack of visibility into cyber events	→	Data aggregation across the enterprise to uncover malicious activity
Rigid procedures that do not flex based on situation	→	Nimble processes augmented by automated cyber workflows & human cognition
Long project timelines to realize benefit from cyber initiatives	→	Fast time-to-value from Agile ways of working
Commercial inflexibility and pricing based on FTEs	→	Pricing based on Resource Units that flex based on business needs

Avoiding pitfalls of a piecemeal approach requires investing in a [holistic operating model](#) that supports the [digital enterprise](#), while dealing with asymmetric threats in an [adaptive](#) manner

# Cyber Adaptive Operating Model

The Cyber Adaptive Operating Model defines the **best deployment** of the elements across people, governance, technology, operations, partnerships, data, etc. to achieve the cyber-mission value proposition and business growth strategy.



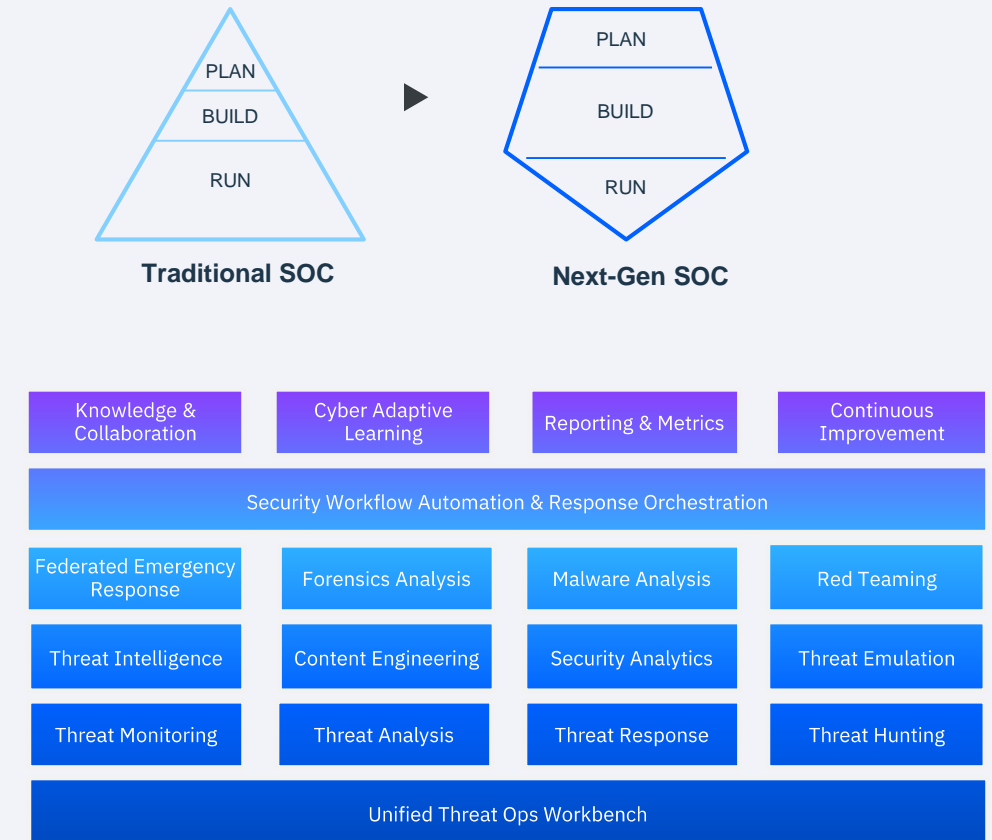
# Next Gen Threat Ops Solution Components



# An evolving Security Operations Centre (SOC) strategy

Strategy Drivers	Expression in the SOC Context
 <b>Talent Transformation</b>	High-value roles (e.g. CSIRT, Threat Intel, Threat Hunting, Use Case Design, etc.) & Immersive Learning
 <b>Cloud based Solutions</b>	Shifting from On-premise to Cloud based SOC architectures to support Big Data Security Analytics strategy
 <b>Cyber Threat Protection</b>	Security Insights that help develop better Counter-measures
 <b>Global Platform</b>	Unified Global SOC Platform that provides enterprise-wide insights into threats (both internal & external)
 <b>Integrated &amp; Secure Experience</b>	Augmented decision support for SOC analysts
 <b>AI based Automation</b>	Reduction in Manual Effort & Error Rates enabling Scalability
 <b>Data Driven Decisions</b>	Reduced response times using Advanced Anomaly Detection
 <b>Strategic Partnership</b>	Improving investments in SOC technology platform driven by next generation tools and co-innovation partnership
 <b>Global API Ecosystem</b>	Standard API based integrations for security data ingestions
 <b>New Ways of Working</b>	Design Thinking for Use Case Design & TTP Centric mindset

## A Shift in SOC Strategy



# Case in Point: How a European Bank got to their vision of being #1 in Cybersecurity

## 2020 Goals

## > Approach

## > Actions

**100%**

protection across bank

Board Level Sponsorship

**ZERO**

loss from cyber attacks

Strategic Review of Operating Model

**ZERO**

downtime from cyber attacks

Security Operations Center (SOC) at core of Cyber Talent

**95%**

cybersecurity awareness

Multi-stage SOC Transformation

1. Expanding scope of security operations beyond Threat Detection & Response
2. Establishing mechanisms for enterprise-wide cyber visibility
3. Machine Learning & AI capabilities for efficiency & effectiveness
4. Cyber talent transformation & experiential learning frameworks
5. Preemptive threat hunting for attacker behavior
6. Collaboration with partners with deep cyber research capabilities
7. Programmatic incident response across the enterprise
8. Automate IOC feed analysis and shift to attacker behavior analysis
9. Streamlining the Red Team, Blue Team and Purple Team dynamic
10. Building advanced capabilities such as Asset Correlation Maps, Deception, Endpoint & Network Behavioral Anomaly Analysis, Malware Analysis, etc.





# Thank you

Follow us on:

[ibm.com/security](https://ibm.com/security)

[securityintelligence.com](https://securityintelligence.com)

[ibm.com/security/community](https://ibm.com/security/community)

[xforce.ibmcloud.com](https://xforce.ibmcloud.com)

[@ibmsecurity](https://twitter.com/ibmsecurity)

[youtube/user/ibmsecuritysolutions](https://youtube/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.