Cyber resilience in Financial Services

A whole ecosystem approach

September 2026

CREST

Contents

1. Executive summary 3

2. Introduction: The case for an ecosystem approach 5

2.1. The three domains 6

2.2. The benefits of alignment between domains 7

2.3. Principles underpinning the model 7

3. Financial institutions: enhancing resilience progressively 8

3.1. A three-part assessment model 9

3.2. Inherent risk and tiering 10

3.3. Control frameworks 12

3.4. Maturity levels 14

4. Financial supervisors: building proportionate and system-wide oversight 17

4.1. Existing guidance and methodologies 17

4.2. A maturity model, with institutional and service providers in mind 20

5. Cyber service providers: bringing assured expertise and independence 22

5.1. The foundations of trusted provision 23

5.2. A provider maturity pathway 24

5.3. Developing local capacity towards international standards 26

5.4. Case study: Threat-led penetration testing in financial services 27

6. Strength through ecosystem alignment 28

6.1. Alignment of the three maturity models 28

6.2. Setting out a multi-year programme 29

7. The role of international and non-governmental organisations 30

7.1. Case study 1: Cyber Risk Institute (CRI) 30

7.2. Case study 2: International Monetary Fund (IMF) 31

7.3. Case study 3: CREST International (CREST) 32

8. Conclusion 33

9. References 34

Executive summary

Cyber resilience in the financial sector is often framed as an institutional responsibility whereby each bank, insurer, payment company, market infrastructure or FinTech must protect its systems and when needed, rapidly recover from disruption. However, financial institutions operate as an interconnected system, dependent on shared infrastructure, technology and data providers, specialist cyber firms and public authorities. A weakness in any critical part of that system can reduce the resilience of the whole.

This paper argues that financial sector cyber resilience should be developed as an ecosystem capability. Within that ecosystem, three groups ("domains") have distinct but interdependent roles:

- Financial institutions must build and maintain strong resilience within their organisations and across the critical business services on which customers and markets rely.
- Central banks, financial services regulators and other financial authorities (Financial supervisors) must establish proportionate expectations, supervise individual institutions and understand resilience collectively across the sector.
- Cyber service providers must supply high-quality specialist advice, assessment, threat intelligence, testing and response capability, supported by demonstrable organisational quality and competent practitioners.

A national cyber authority sits alongside these groups, connecting the sector to economy-wide policy, critical-infrastructure protection, incident coordination and skills development. Financial authorities should align closely with it while recognising that the systemic importance and interdependence of financial services usually justify sector-specific requirements.

The proposed whole-ecosystem maturity pathway helps a jurisdiction assess its current position, establish a realistic target state and sequence development across all three groups. It provides a common structure within which international guidance, national regulation, industry frameworks and independent assurance can work coherently.

It also helps deal with ecosystem-wide challenges such as the impact of frontier technologies including Artificial Intelligence (AI) and Post Quantum Cryptography (PQC). These topics will inevitably be regulated. Institutions must adapt their cyber resilience to accommodate them and service providers must bring aligned specialist skills and experience to bear.

Executive summary

For financial institutions, the model combines inherent risk and systemic importance, an appropriate control framework and evidence of capability maturity. For authorities, it progresses from initial sector mapping and minimum expectations to tiered requirements, independent testing and adaptive system-wide oversight. For providers, it creates a route from generalist experience to independently accredited financial services specialists.

The three pathways must be planned together. For example, regulatory requirements that outpace institutional readiness, supervisory capability or provider capacity can produce limited assurance and in the worst cases, divert time and resources away from actual capability development. Alternatively, a lack of local advanced service provider capabilities can lead to poor testing outcomes and over-reliance on expensive overseas consultancy. Lessons from the 2008 financial crisis show clearly the impact of under-developed regulatory oversight and the positive impact since of a more active, system-wide resilience focus.

Taken together, the model points to three priorities for building stronger and more sustainable cyber resilience across the financial ecosystem:

- **Ecosystem measurement:** Make the ecosystem maturity, including shared dependencies, a key measurement of national cyber resilience.
- **Common language**: Adopt a common language and framework for institutional requirements, supervisory approach and trusted provider capability, enabling cross-border consistency.
- **Development support:** Recognise the areas in each part of the ecosystem that need to accelerate and bring them forward in unison, ensuring no part gets left behind.

Introduction: The case for an ecosystem approach

From institutional cyber security to system-wide resilience, why financial services cyber resilience is reliant on an ecosystem-wide approach

Financial services are built on confidence and continuity. Customers need to access money and make payments on demand to manage their lives in the modern digital world. Firms need to settle transactions, manage liquidity, price risk, protect assets and communicate securely to support the smooth running of the economy. Markets depend on data, messaging, clearing and settlement to maintain dynamic financial systems. Public authorities depend on reliable information and functioning institutions to preserve financial stability and protect civil society. Whilst digital technology has been ubiquitous for many years now, the growth in adoption of frontier technologies by both financial institutions and adversaries is putting the spotlight once again on how connected the defenders across the ecosystem are.

This also leads us to an important distinction between cyber security and cyber resilience. Cyber security controls seek to prevent, detect and respond to malicious activity. Cyber resilience is broader: it is the ability to anticipate and adapt to threats, withstand and contain disruption, recover safely and continue delivering critical business outcomes.

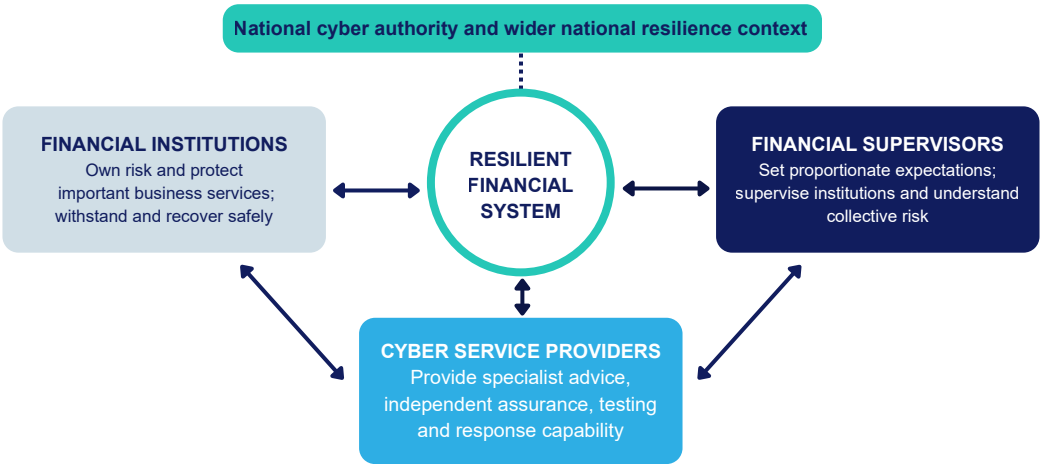
Prevention remains essential, but risk management will never eliminate all risk. It is unrealistic to assume that every attack can and will be stopped. Institutions must be able to operate through disruption and recover as rapidly as possible.

International guidance for the finance sector has long emphasised that cyber resilience is a collective endeavour, because individual entities are embedded in a wider ecosystem of participants, linked infrastructures and critical service providers.[1] More recent work by financial authorities has reinforced the significance of interconnectedness, common critical third parties, cross-border spillovers and consistent incident information.[2] The implication is clear: the resilience of an institution cannot be assessed solely within its own boundary.

In this paper we focus in on the impact of three specific domains within the financial services cyber resilience ecosystem and the importance of identifying them, assessing them and maturing them in unison. The weaknesses that adversaries exploit can often be found within the gaps between these domains, from the structures within single institutions through to differences in international regulations. The ecosystem approach seeks to narrow these gaps through a holistic view, common frameworks and a collective commitment to the highest standards.

The three domains

- **Domain 1: Financial institutions** must build and maintain strong resilience within their organisations and across the critical business services on which customers and markets rely. External consultancy and regulatory oversight do not transfer this responsibility.
- **Domain 2: Central banks, financial services regulators and other financial authorities ('Supervisors')** must establish proportionate expectations, supervise individual institutions and understand resilience collectively across the sector. The model groups them for simplicity while recognising the need for clear roles and cooperation.
- **Domain 3: Cyber service providers** supply high-quality specialist advice, assessment, threat intelligence, testing and response capability, supported by demonstrable organisational quality and competent practitioners. Given the kind of high-risk work these organisations perform, the strength and depth of this community is core to market resilience.



Distinct accountabilities, shared evidence and coordinated improvement

A cyber technical authority plays an important role at the national level, sitting alongside these three domains. It may, for example, lead economy-wide cyber strategy, critical-infrastructure protection (of which financial services is one element), incident coordination, national CERT or CSIRT functions, threat information sharing and skills development. Financial supervisors typically align closely with it on critical-service definitions, incident escalation, information sharing and cross-sector exercises, while recognising that the financial sector may have unique or expanded requirements that go further or develop faster than general national baselines.

This paper provides a common language for diagnosing the current position of each of the domains, supports the sequencing of multi-year development programmes and shows where standards, independent accreditation and professional certification can support trust. The development pathways are illustrative rather than a new compliance standard or a prescriptive implementation approach.

The benefits of alignment between domains

This model allows for independent progression of each domain whilst also acknowledging where alignment is preferable. Some examples include:

- The authority's supervisory capability should develop before, or at least alongside, the requirements it introduces.
- The provider market should be assessed as being at the desired level before the use of providers' services is mandated.
- Institutions with the greatest systemic impact should face the highest expectations first.
- Advanced testing of institutions should follow sufficient evidence of success at the baseline levels.
- Mandating the use of local providers should follow local maturity development, accepting there may be pressure to reduce reliance on international expertise.

Principles underpinning the model

The following principles are assumed for each of the three domains:

- **Standards-based and mapped**
  Recognised international and sector frameworks should be mapped to a coherent primary structure so that common outcomes can be assessed once and maintained as requirements change. Multi-national alignment helps reduce administrative burden and ensures resources are prioritised for genuine resilience improvements.

- **Evidence-led and independently assured**
  Self-assessment is a practical starting point, but this should progress to validation through independent review, technical testing and evidence of remediation.

- **Continuously improving**
  Incidents, exercises, intelligence, technology change and market developments should feed back into policy, investment, standards and provider development. With the acceleration of frontier technology capabilities, standing still is really falling behind.

It is acknowledged that there is significant detail and value to be found in the plethora of standards and frameworks that exist to support each of the domains and this paper does not seek to diminish their criticality or replicate them.

Financial institutions: enhancing resilience progressively

Ownership of resilience lies with the institutions themselves, but frameworks exist to help accelerate maturity

The first responsibility in the model sits with financial institutions. A board and executive team are ultimately accountable for cyber resilience with responsibility generally delegated to the business divisions, supported by the security and technology functions. They must determine what outcomes the institution needs to protect, what level of disruption can be tolerated, which investments are required and whether weaknesses are being remediated at the pace demanded by the risk.

This often begins with critical business services and takes an end-to-end process or customer-centric view rather than an internal functional lens. Taking a critical business service approach means spotting those services whose disruption could cause material harm to customers, threaten operational resilience or contribute to broader financial instability. Typically, they then map the people, processes, information or data, technology, physical infrastructure and third parties that support those services. This service-led view puts technical risks within the context of broader business goals, making it meaningful to decision-makers and revealing dependencies that could otherwise be missed.

Once the critical business services and associated risks relating to cyber security have been identified, the institution will typically look to establish a baseline assessment of risk and control at a more detailed level. Many standards and frameworks exist to support this, produced by national or regional regulators, non-profits and other non-governmental bodies. The multi-national institutions are particularly exposed to variation in these frameworks as they can find themselves having to perform similar but separate exercises across entities, jurisdictions and teams.

A three-part assessment model

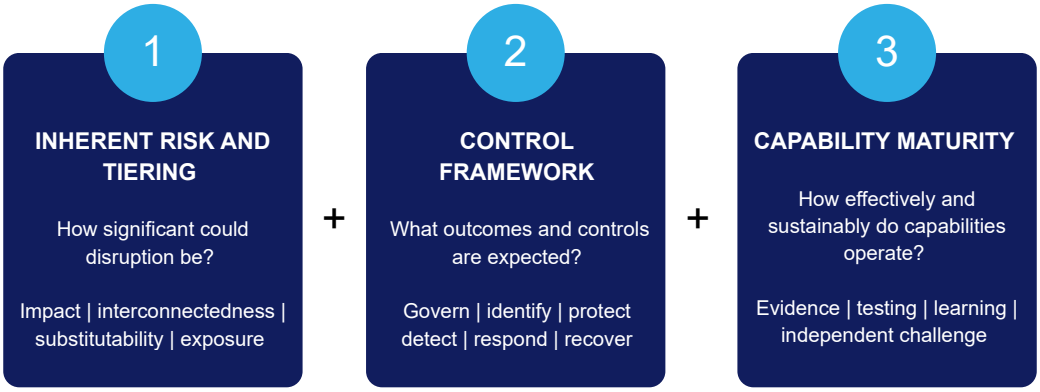
There are, however, common attributes to most of these frameworks which can be summarised as follows:

- Inherent risk and tiering: proportionate risk management means tailoring the framework to the characteristics of the institution using it, using standard tiers. This will consider factors such as the institution's size, customer base and market share, significance to the national economy, risk of contagion to other market participants and international footprint.

- Control frameworks: a control framework typically provides a repository of standard controls and varying levels of guidance for implementation and auditing. The controls are often mapped to risks, tiers (per part 1 above), other frameworks (e.g. NIST CSF 2.0 [3]) and national regulations. Control frameworks can be used for internal self-assessment, as the basis for external accreditations or as evidence provided to third parties and regulators.

- Maturity levels: often performed following the control assessment is the positioning of the organisation (or specifically the service being assessed) on a maturity pathway, based on how well the controls have been determined to be designed and operating effectively. This helps provide the institution with an objective view as to where they are relative to an accepted benchmark and creates a basis to plan and measure remediation.

A three-part model for assessing financial-institution cyber resilience



Proportionate expectations | Meaningful assurance | Comparable improvement over time

Inherent risk and tiering

Tiering provides the basis for proportionate risk management, identifying where disruption could have broader or more severe consequences and where additional assurance is justified.

The Cyber Risk Institute (CRI) Profile[4] provides one example of such a model, using a four-tier approach ranging from national or super-national impact to localised impact. This has reference to national regulator tiering definitions to aid alignment.

Tier	Indicative impact	Indicative characteristics
1	National or super-national	These institutions are designated most critical by one or more global regulatory agencies and/or bodies (e.g., the Basel Committee's Global Systemically Important Bank (GSIB) designation or Executive Order 13636's Section 9 designation). This category assumes the gross cyber risk exposure of an institution or service categorised as Tier 1 would have the most potential adverse impact to the overall stability of a national economy, and potentially, the global market.
2	Sub-national	These institutions provide mission critical services with millions of customer accounts. This category assumes the gross cyber risk exposure of an institution or service would have the potential for a substantial adverse impact to the financial services sector and sub-national regional economy but does not rise to the level of Tier 1.
3	Sector	These institutions have a high degree of interconnectedness, with certain institutions acting as key nodes within, and for, the sector. The nature of the services that these institutions provide to the sector plays a significant role in determining their criticality.
4	Localised	These institutions have a limited impact on the overall financial services sector and national economy. Typical characteristics include: (a) institutions with a local presence and less than 1 million customers (e.g., community banks, state banks) and (b) providers of low criticality services.

Table 1: Tiering definitions sourced from CRI Profile version 2

Some of the factors that tiering models often consider are:

Impact factors

- Potential effect on financial stability, market functioning, safety and soundness or customer protection.
- Number and type of customers, counterparties or market participants affected.
- Value, volume and time-criticality of transactions or assets processed.
- Potential for direct financial loss, data compromise, fraud or loss of confidence.
- Cross-border reach and the possibility of international spillover.

Structural factors

- Interconnectedness with other institutions and infrastructures.
- Substitutability, or whether another provider could take over the service quickly and safely.
- Concentration risk, typically whether the institution is a key node or relies on common third parties.
- Complexity of business model, legal structure, technology estate and change programme.
- Dependence on legacy platforms, cloud services, outsourced operations or specialist vendors.

Threat and exposure factors

- Relevance to sophisticated criminal, state-linked, insider or disruptive threat actors.
- Exposure through internet-facing services, open banking, application programming interfaces, remote access and digital channels.
- Sensitivity and value of data and credentials held.
- History of significant incidents, near misses and recurring control failures.

Tiering should be reviewed periodically and after material changes such as mergers, rapid growth, entry into critical services, significant outsourcing or technology transformation. It should also be capable of operating at more than one level. An institution may be placed in an overall tier while particular business services or infrastructures are treated as especially critical.

A tier should drive proportionate expectations in areas such as governance, reporting, assessment frequency, independent assurance, recovery objectives, scenario testing and supervisory intensity. It may also drive the applicability of certain controls identified in standard control frameworks, as is explored below.

Control frameworks

Once the impact of the institution relative to the broader market is understood, they need a structured definition of expected outcomes and controls. A recognised framework offers several benefits: it increases the chance of having a robust control catalogue, supports common terminology, enables repeatable internal assessments and helps institutions explain their position to boards, auditors, providers and supervisors. It may also enable a low friction way to comply with national regulations if suitably aligned and mapped.

Many standards, frameworks and related regulations already exist, for connected purposes, for example:

Area	Primary purpose	Illustrative examples
Cyber control frameworks	Defines a structured set of cyber outcomes and controls	NIST CSF 2.0; CRI Profile; national baselines.
Cyber regulations	Set by government agencies and sector regulators, they create legally binding requirements.	EU's DORA[5]; UK's CBEST[6]; prudential, payments, insurance or market rules.
Cyber guidance and principles	Established to support the implementation of frameworks or regulations. They seek to provide additional clarity but are generally optional or advisory in nature.	ECB's CROE[7]; IOSCO's CPMI guidance[8]; G7 element[9].
Cyber testing and service requirements	Define how particular assurance or testing activities should be governed and delivered. This includes demonstrating cyber service provider quality and individual competence.	UK's CBEST; EU's TIBER-EU[10]; CREST's TLPT-FS accreditation[11]; CREST's Red Team Specialist certificate[12]; national red-team frameworks.

Table 2: Types of standards, frameworks and related regulations

As an example, the NIST Cybersecurity Framework 2.0 organises outcomes around Govern, Identify, Protect, Detect, Respond and Recover and is designed for organisations of different sizes and sectors. Some national frameworks are targeted at critical national infrastructure as a whole (which would include financial services), recognising the heightened risk and therefore increased resilience expectations of these sectors.

A financial-sector framework such as the CRI Profile adds sector-specific language, diagnostic statements and mappings to financial regulation. Adopting a globally recognised financial services specific framework can help institutions simplify their assessment activities and more easily map a single control programme to various national and regional requirements. Whilst local variation may still be required, this reduces duplication and inconsistency.

Linking back to the tiering model above, the CRI Profile defines increasing expectations based on tier, enabling the proportionate risk management approach favoured by both institutions and supervisors. The following table illustrates the increasing number of control statements that are applicable based on the increasing tiers. The 'Profile' requirements are mapped to NIST CSF v2 functions and various regulatory frameworks including APRA, ASIC, CIS, DORA, EBA, ECB, FFIEC, HKMA, JFSA, NAIC, MAS, NYDFS, OCC, OLIR, SEC and OSFI:

	Functions (# of diagnostic statements to assess against)							
	Govern	**Identify**	**Protect**	**Detect**	**Respond**	**Recover**	**Extend**	**Total**
Tier 1: National/ Super-National Impact	97	64	74	24	16	11	32	318
Tier 2: Sub-National Impact	93	62	74	23	16	11	32	311
Tier 3: Sector Impact	85	58	68	20	16	10	25	282
Tier 4: Localised Impact	64	37	49	14	12	10	22	208

Table 3: Summary illustration of varying control expectations by tier

Maturity levels

Within the world of risk management, assessing relative maturity of the control environment means describing how developed, systematic, consistent and effective the organisation's approach to managing that risk is. Key to this is how embedded and repeatable the capability is across a critical service being evaluated, the critical services of the organisation as a whole or even a snapshot of the national ecosystem.

Typical maturity models have three to five stages of maturity, with detailed definitions or criteria for assessing the current state and indicating what would need to be developed to move to the next level. This can help an organisation to benchmark it against a common standard, identify areas of control weakness and plan remediation activities. For Boards, executive teams and supervisors it provides an independent measure of risk exposure and progress over time.

One such example is the European Central Bank's (ECB) Cyber Resilience Oversight Expectations (CROE) for financial market infrastructures. This uses three maturity levels (Evolving, Advancing and Innovating) across domains including governance, identification, protection, detection, response and recovery, testing, situational awareness, and learning and evolving.[5] The World Bank has also used the CROE approach as a reference point beyond the Euro area.[6]

Table 4 provides an illustrative expanded version of this model, breaking it into five stages predominantly to make the early stages of development more granular and visible as this is where more support and clarity is often required.

Another example is the CRI Profile Maturity Model (CPMM) which is an extension of the CRI Profile leveraging the same Functions, Categories, Subcategories, Diagnostic Statements and tiers. It provides financial institutions with a structured way to assess how consistently and effectively cybersecurity and technology risk practices are implemented across the organisation. The CPMM evaluates maturity at the Diagnostic Statement level across five stages from Ad Hoc to Advanced, allowing institutions to move beyond a simple assessment of whether a control exists and consider how well it is embedded, governed, measured, and improved over time. The model can help institutions identify gaps, prioritise investment, establish target maturity levels based on risk, and communicate progress to senior management and boards using a common framework.

The CPMM establishes five distinct maturity levels reflecting progressive steps forward in process standardisation, institutionalisation, governance oversight, coverage, reliability, and risk management effectiveness:

Level 1: Ad-hoc – Processes are generally reactive and responsive to immediate needs and lack consistent control.

Level 2: Initial – There is an initiation of process control at a foundational level, but inconsistency exists across different assets, processes, projects, and organisational areas.

Level 3: Established – A defined set of standard control processes are implemented and followed consistently across most key assets, business processes, projects, and organisational areas.

Level 4: Reliable – Processes are monitored to assess reliability and effectiveness, metrics and results are reported to leadership, and coverage extends organisation-wide.

Level 5: Advanced – Processes are adaptive and continuously optimised in a proactive approach through feedback loops and applied innovation.

The CPMM details people, process and technology characteristics for each of these levels and examples of evidence that may be effective in assessing and demonstrating the maturity level of a given Diagnostic Statement.

Regardless of the maturity model used, assessment should use a combination of documentation, interviews, observation, data, sampling and technical validation. Self-assessment can establish ownership and identify gaps whilst independent assessment provides challenge and comparability. An indicative model based on these examples follows:

Stage	Institutional state	Indicative evidence and assurance	Priority to progress
1. Ad hoc / informal	Basic cyber hygiene is incomplete; important services and dependencies are not reliably understood; no structured framework assessment.	Limited or inconsistent evidence; reactive vulnerability work; untested incident and recovery arrangements.	Establish governance, map services, complete a baseline self-assessment and close urgent hygiene gaps.
2. Foundational / Initial	Basic hygiene is in place; self-assessment (e.g. using the CRI Profile) has identified gaps and remediation is being funded; selected key systems are being tested.	Framework (e.g. CRI Profile) self-assessment; remediation metrics; targeted vulnerability assessment, penetration testing and tabletop exercises.	Close critical gaps, broaden coverage and improve evidence quality.
3. Established / Evolving	Expected controls are substantially implemented and materially effective; limited material remediation still underway; independent assessment and broader technical testing are introduced.	Independent review of the very highest criticality areas; technical testing across all key services; selected threat-led penetration testing (TLPT) and advanced incident exercises.	Resolve material gaps, integrate third parties and repeat testing to validate remediation.
4. Reliable / Advancing	No material unresolved gaps against the required baseline; threat intelligence informs assurance; important services receive realistic testing.	Independent control assessment (e.g. by consultants aligning to CRI Profile); breach simulation, purple teaming and regular proportionate TLPT exercises.	Advanced higher risk testing, root-cause remediation and collective exercises.
5. Advanced / Innovating	Resilience is integrated into strategy and change; strong internal advanced testing capability; the institution contributes to ecosystem resilience.	Continuous metrics and targeted independent challenge; internal and external TLPT incorporating frontier technologies; evidence of rapid learning and adaptation.	Adapt to emerging technology and threats while maintaining independent challenge and avoiding complacency.

Table 4: An illustrative five-stage pathway for financial institution cyber resilience maturity

Financial supervisors: building proportionate and system-wide oversight

The authority's role and approach develops in scope and assertiveness

Financial supervisors typically promote the cyber resilience of individual regulated institutions as well as understanding and reducing the risk of contagion whereby cyber disruption could spread across the financial system.

The supervisory role may sit with a central bank, prudential supervisor, payments overseer, securities regulator, insurance supervisor, market conduct regulator or several supervisors working together.

The financial supervisors will typically work closely with national cyber technical authorities and those overseeing critical national infrastructure. This ensures that they stay aligned with national baselines and laws whilst allowing for financial sector specific differences such as the macro-economic and consumer impacts.

Existing guidance and methodologies

Legal powers and institutional structures differ, but an effective model generally aligns around a common set of functions, as illustrated by the International Monetary Fund's (IMF) 'Elements of Supervision' from their Cybersecurity Risk Supervision paper[2].

The IMF's work emphasises the need to build on operational and technology risk supervision, which pre-dated the separate but related focus on cyber, while recognising the distinctive speed, intent and system-wide potential of cyber events. This has further evolved in recent years to elevate the importance of third-party risk management and the susceptibility to supply chain compromises.

The paper's seven elements are summarised here:

Identifying the threat landscape

Supervisors should build a continuously updated picture of attackers, methods and incidents by drawing information from security agencies and law enforcement, national computer emergency response teams (CERTs), overseas supervisors, private sector specialists and financial-sector sources. This intelligence supports a threat profile for each supervised firm and, when aggregated, a sector-wide profile.

Mapping the cyber and financial system

The paper proposes mapping at two levels. Supervisors first identify each firm's critical ICT systems, business dependencies and material technology providers, then combine this information with financial flows to create a sector-wide network map. The resulting map reveals shared platforms, cloud or telecommunications concentrations, critical payment and clearing nodes, and routes through which a disruption could spread.

Regulation

Regulation should establish enforceable authority while remaining flexible enough to keep pace with changing threats and technology. The IMF favours a combination of high-level principles, outcome-focused rules and baseline requirements expressed as control objectives. Every firm should cover the same core areas, including board accountability, independent security leadership, asset identification, access control, monitoring, testing, continuity, outsourcing and incident reporting. The maturity of implementation should rise with the firm's risk, complexity and systemic importance (as articulated in the section on Financial Institutions above).

Supervisory assessment

Cybersecurity should form part of routine supervisory review, given due attention rather than covered superficially through other operational risk oversight. As with other areas of risk, supervisory methodologies should distinguish the firm's inherent cyber risk, the maturity of its controls and the residual risk remaining after those controls operate. Indicators can include critical systems' dependence, the complexity of the ICT estate and the prevalence of legacy infrastructure. Higher exposure or greater systemic importance calls for stronger control maturity, validating any self-assessments through independent testing.

Information sharing and reporting

Supervisors should support structured information exchange among firms, regulators, security agencies and critical-infrastructure bodies, using sufficiently detailed anonymised data to improve collective detection and response.

A collation of related methodologies from the United States, European Union, United Kingdom, Australia, Japan, Singapore and South Korea has been published by The Center for Strategic & International Studies, enabling a wide range of examples from which a supervisor can develop their own approach [13].

In addition, the Cyber Threat Alliance and the Institute for Security and Technology worked with CREST and other industry experts to publish a Cyber Incident Reporting Framework in 2022[14], containing definitions, principles and common reporting formats for regulators to adopt to drive quality and harmonisation.

Role of the supervisor to encourage adequate response and recovery

Supervisors should require firms to prepare for successful attacks through incident-response plans, tested business-continuity arrangements, secure backups, fallback data centres or cloud environments and other redundancy arrangements. Recovery time and recovery point objectives should reflect business-impact analysis, critical dependencies and financial-stability priorities while allowing time to confirm that systems and data are free from residual impacts.

Specialist service providers (as detailed further below) should conduct technical testing both standalone and with supervisory involvement where appropriate. Sector-wide tabletop and TLPT exercises test coordination, decision-making, communications and recovery across firms and the public sector.

Preparedness of supervisory agencies for a cyber attack

Supervisory agencies need their own crisis capability, supported by clear legal powers, adequate resources, efficient procedures and plans that evolve with the threat landscape and financial system. Authorities responsible for supervision, central banking, payments, clearing, cyber response and law enforcement should establish roles, reporting lines, succession arrangements and alternative communications before an incident occurs, then test them through joint public-private exercises.

Other useful contributions to the supervisory approach include a report on cybersecurity practices for regulators (BCBS[15]), guidance on cyber resilience for financial market infrastructure (CPMI-IOSCO[16]), insurance supervisor standards and guidance (IAIS[17]), work to reduce regulatory fragmentation (IIF[18]) and principles for regulating cyber risk (Chicago Booth[19]).

A maturity model, with institutional and service providers in mind

Having established the key elements of a supervisory framework, it is possible to also set out a maturity pathway for the supervisors recognising that they, like other organisations in the ecosystem, will be at different stages of development. Some may have well established cyber focused divisions and frameworks whilst others may only recently have broken cyber out from broader ICT operational risks.

It recognises that the ambitions of the supervisory approach must be aligned with the capacity and capability of the supervisory team as well as the development of both the financial institutions and the service providers.

At the early stages, the priority is rapid visibility of the national sector landscape, including mapping institutions, services and dependencies, establishing a risk-based baseline and building supervisory skills. After this the focus is on tiered self-assessment, thematic reviews, exercises and provider-market development. At the more advanced stage supervisors introduce formal independent validation and threat-led testing for higher-impact institutions, alongside adaptive, system-wide oversight informed by incidents, intelligence and cross-border cooperation.

The IMF published a technical note and guidance in 2025 [20], drawing on lessons from their own surveys of 32 national supervisors (predominantly using responses from low and lower-middle income countries). The note highlighted concerted efforts needed to (i) develop national and financial sector focused cybersecurity strategies; (ii) build cyber risk regulatory and supervisory capacity; and (iii) address resource constraints.

Whilst explicitly not a maturity model for supervisors, the questions surveyed and the observations within the note provide a useful basis for considering the path supervisors may take in maturing their capability. As such elements of the IMF observations have been incorporated into this illustrative model:

Stage	Authority state	Indicative outputs and evidence	Priority to progress
1. Baseline mapping, mandate and strategy	Cyber moves beyond minimal treatment within general operational risk; the sector participants, dependencies and current capability are mapped. Starting to work with security agencies and criminal-justice to define deterrence and legal framework requirements.	Sector mapping; draft tiering; roles and legal powers reviewed; authority capability baseline; strategy and governance established.	Resolve mandate gaps, address urgent weaknesses and confirm priorities and resources.
2. Foundational regulation, reporting and supervision	Formal regulatory and reporting foundation established. A summarised controls baseline for institutions is published (e.g. aligned to elements of the CRI Profile), as a minimum starting with highest priority domains. Threat intelligence being gathered and utilised. Supervisory teams developing with onboarding of specialised staff and experienced leadership. Legal frameworks formalised and enforcement capability realised.	Published expectations; incident reporting regime; self-assessment; supervisory method and initial training.	Improve implementation support and build supervisory and industry capability.
3. Supervised implementation, capacity building and coordination	Tiered self-assessment against a comprehensive baseline (e.g. the full CRI Profile), threat-led thematic reviews, exercises and sector collaboration deepen capability. Supervisory teams comprise specialised staff and experienced leaders. Supervisory teams may seek independent assessment for their own in-house cyber services. Legal frameworks actively in use.	Peer analysis; workforce planning; information-sharing; scenario, vulnerability and penetration testing; provider quality criteria; local capacity programmes; supervisor earned accreditations; threat and incident data analysis and theme sharing.	Pilot formal independent assurance and test scheme governance.
4. Risk-based assurance, advanced testing and systemic analysis	Mandatory tiered baseline requirements, independent validation required including regular testing for all and advanced testing for higher tier institutions. Powers to mandate additional third-party technical testing and how that testing should be performed. Powers extended to critical supply chain.	Defined scope, provider eligibility, test governance, regulatory summaries, remediation closure and enforcement.	Aggregate quantitative evidence, extend into critical supply chains and harmonise regulatory approaches.
5. Adaptive resilience and cross-sector oversight	Cyber is embedded in ongoing supervision and system-wide analysis; standards adapt continuously. Quantitative risk analysis and stress testing are mandated and proportionate. International collaboration on legal frameworks and cross-border cooperation.	Current dependency mapping; cross-sector exercises; continuous threat intelligence and related themes; third party concentration risk indicators; international cooperation and peer review.	Recalibrate using evidence, reduce fragmentation and manage emerging systemic dependencies.

Table 5: An illustrative five-stage pathway for supervisors

Cyber service providers: bringing assured expertise and independence

Trusted specialists providing vital support to the rest of the ecosystem

Financial institutions and supervisors depend on specialist providers for capabilities that are scarce, highly technical or require independence. This dependence becomes greater as expectations progress from basic technical assessment to advanced threat intelligence, live-system testing and major incident response.

The depth, quality and distribution of service providers affect whether a national cyber resilience strategy is achievable. A small market with limited assurance capabilities can create several risks:

- institutions may buy services from organisations whose capability is inferior and they therefore may gain false confidence in their security posture;
- supervisors may place reliance on ‘clean’ test reports provided by basic or poor-quality tests and similarly draw incorrect conclusions. They may also receive reports that are inconsistent, difficult to compare and unreliable;
- advanced tests may be performed by teams without sufficient experience or safety controls, leading to a worse outcome than if the tests were not undertaken at all;
- a scarcity of providers may create concentration risk, stifle innovation and create scheduling constraints;
- overseas teams may lack local context, language, legal understanding or long-term availability. They may also come at increased cost;
- mandates may increase cost without producing sustained capability or remediation.

Supervisors and non-governmental organisations seek to establish transparent quality expectations, independent assurance capabilities and a development route for providers to mitigate these risks and mature the service provider market.

The foundations of trusted provision

A trusted cyber service depends on both the organisation and the individuals delivering it. For sensitive financial-sector work, quality must be verifiable, from organisational due diligence to skill, competence, sector experience and technical service delivery methodologies that meet international standards. CREST specialises in standard setting for cyber organisations and professionals, basing assessments on the following four dimensions:

Dimension	What good looks like
Organisation	The organisation needs to be subject to standard due diligence checks to meet local and client specific criteria. They also need to have in place additional practices including governance, ethics rules, information security, quality management, complaints handling, professional indemnity, conflict management and control of subcontractors.
Services	The organisation needs to operate their services to formal international or national standards, evidencing this through documented policies, methodologies and templates. This should be validated by independent third parties, either a national government certifying agency or an international standard setting body.
People	The people delivering services need to be skilled and competent to deliver the activities they are accountable for within the engagements they support. This means defining role-specific knowledge and practical competence, with experienced leaders required to exercise sound judgement under pressure and take ultimate accountability for delivery. A provider must be able to evidence the skill and competence of their people with reference to internationally or nationally accepted criteria and frameworks.
Sector experience	The organisation must have relevant financial services experience, drawing on their knowledge of the unique technological and environmental factors to ensure they can interpret client requirements and execute realistic testing effectively. This should include a good understanding of the local and regional laws and regulations facing both service providers and financial institutions.

A provider maturity pathway

Financial institutions want to know that the service providers they bring in, who have access to sensitive systems and data, are suitably capable and professional for the help they need. However, procurement teams are often not specialised or resourced enough to do deep analysis of prospective service providers for highly technical engagements. In addition, some services require more specialised skills than others, with vulnerability assessments at one end of the scale and complex tests in production environments at the other.

Equally, supervisors are reliant upon institutions getting the support of service providers to improve their cyber resilience and will sometimes mandate the use of certain service providers for regulated activities. They similarly are generally not resourced to perform technical due diligence on the service provider market nor is it their role to advance their capability and capacity.

International organisations like CREST help to close this gap by setting standards, supporting organisations to develop towards them and quality assuring them once they are ready.

The 'CREST Pathway to Accreditation model' (CREST Pathway) [21] describes a journey that a cyber service provider can take from initial commitment to international CREST standards (Pathway status), to self-assessment against the standards (Pathway+ status) and then to full quality assurance and accreditation (Member status).

In Table 6, an illustrative cyber service provider model for financial services builds on the CREST Pathway model to establish a tailored maturity level assessment for providers to financial services organisations:

Stage	Provider state	Evidence of development or assurance	Appropriate role
1. Unvalidated provision	Organisation may be at early stages of growth and may not have operated in a regulated environment before.	No recognised independent assurance relevant to the service. Customer due diligence only; capability may be strong but is not externally demonstrated.	Lower-risk work where the buyer can validate quality, or entry into a development pathway.
2. Standards commitment	Organisation may be delivering services within financial services, potentially unregulated activities only.	Organisation registers core information, commits to a code of conduct and works towards recognised standards (e.g. CREST Pathway status or similar and a documented development plan; not accreditation). Services likely have minimal documentation and standardisation.	Capability development, lower-risk or lower-complexity engagements (e.g. vulnerability assessment) and workforce building.
3. Structured self-assessment	The organisations is growing in its financial services experience and developing the maturity of its service offerings	Organisation assesses itself against company and service requirements and closes identified gaps. Services may be partially documented and repeatable. (i.e. CREST Pathway+ or equivalent self-assessment, ability to evidence capability against standards on request; not independent accreditation).	Joint or supervised delivery while preparing for separate external review.
4. Independently accredited	Organisation is experienced and highly professional, meeting international cyber service delivery standards and delivering consistent, quality work.	Organisational and relevant service capability are independently reviewed; services are formal, documented and repeatable. In-scope people meet competence requirements (i.e. CREST accredited for defined service scope like Penetration Testing or Threat Intelligence; registered professionals; ongoing proven quality systems).	Independent assessment and specialist delivery within the accredited scope which may include higher risk systems.
5. Specialist financial-sector provider	Strong organisational experience and capability are coupled with excellent specialist financial services knowledge and advanced service offerings.	CREST core accreditations are supplemented with evidence of substantial financial-sector experience and ability to safely deliver high-risk work including TLPT (i.e. with CREST TLPT-FS accreditations - Threat Intelligence for Simulated Attacks and / or Intelligence Led Pen Testing). Highly experienced teams with verified credentials, specialist methods and strong control of sensitive live-system testing.	Regulated or voluntary TLPT exercises, complex sector exercises, mentoring and contribution to scheme development.

It is important to note that unvalidated provision will not necessarily be poor quality, but the buyer must perform more of their own due diligence and potentially limit engagements to lower risk ones.

Developing local capacity towards international standards

Many jurisdictions face a genuine capacity and capability challenge, particularly for the more complex and higher risk service areas. The most experienced providers and practitioners may be concentrated in a small number of markets, while local firms have limited access to experience gained on complex engagements, training, capital and recognised qualifications. Moving prematurely to mandating the highest international accreditations and certifications may exclude local providers if no development route exists, raise costs for financial institutions and in fact create risk where services have long lead times.

A balanced strategy can use several mechanisms:

- a transparent pathway from commitment and self-assessment to independent accreditation (as per the CREST Pathway)
- mentoring from experienced accredited providers;
- partnerships between international and local teams with explicit knowledge-transfer objectives;
- access to internationally recognised training and examinations;
- public or donor-funded capacity programmes to boost market funded investment;
- pilots and lower-risk engagements that allow local providers to build evidence safely;
- advocating for procurement approaches that reward quality rather than purely cost;
- communities of practice and technical knowledge sharing; and
- ethical commitments and guard-rails with meaningful disciplinary procedures and consequences.

The CREST Cyber Accelerated Maturity Programme (CREST CAMP) is an example of a capacity-building approach that combines standards, training, mentorship and accelerated progression through the CREST Pathway.[22] The model can be used to target the development of local providers to the financial sector, ahead of or in parallel with mandated regulation, to build affordable high-quality provision in a sustainable way.

Case study: Threat-led penetration testing in financial services

Threat-led penetration testing is one of the clearest examples of the three-part ecosystem needing to work together. It requires an institution that has high maturity in understanding and testing its core systems and the ability to control a high-risk exercise, a supervisor with a carefully crafted testing regime and specialist threat intelligence and penetration testing providers with the highest skills to deliver tests effectively and safely.

CREST's 2026 guidance, 'Threat-led Penetration Testing: Guidance for Financial Services' (TLPT-FS), describes a process to support all three domains.[23]

The methodology is used to assess the cyber resilience of a financial institution's critical business services, enabling them and their regulators to better understand vulnerabilities and take remedial actions. This in turn improves their resilience and, by extension, the wider financial systems.

It promotes a TLPT approach that mimics the actions of cyber threat actors intent on compromising an organisation as well as the technology assets and people supporting them.

The methodology can be used by an institution independently, or in consultation with their regulator.

1. Initiation	2. Threat intelligence	3. Penetration testing	4. Closure
Important services, scope, control group, senior accountability and risk controls.	Targeting, relevant threat actors, credible scenarios and intelligence reports.	Test plan, controlled live-system execution, evidence and collaboration.	Remediation plan, lessons, validation and regulatory reporting where applicable.
Control features: qualified providers and practitioners | secure information handling | escalation and stop conditions | need-to-know governance | remediation focused on root cause and important-service impact.			

Table 7: Summary of TLPT stages

TLPT is most valuable when:

- the institution has a reliable understanding of the services, systems and people in scope;
- controls and incident arrangements are sufficiently mature to make the test meaningful;
- threat intelligence is current, relevant and translated into credible scenarios;
- the engagement can be managed through a small, senior, experienced and accountable control group;
- the testing team has appropriate organisational assurance, qualifications and experience;
- detection and response teams are well established and positioned to be able to learn from the activity;
- findings are prioritised, remediated and validated; and
- the authority, where involved, can interpret results and use them within the context of the analysis.

Strength through ecosystem alignment

Forming a national ecosystem-level assessment enables participants to look beyond the maturity of the individual domains and consider whether the three pathways are aligning as they develop.

Bringing together the three illustrative maturity models above, an ecosystem-assessment can be defined based on the ratings for each domain. This could be top-down, judgment based to begin with and as each domain matures this can be more bottom-up and evidence based.

Alignment of the three maturity models

Illustrative alignment of the three maturity pathways

	Stage 1	Stage 2	Stage 3	Stage 4	Stage 5
Financial institutions	Basic hygiene incomplete	Foundational controls and self-assessment	Materially effective; independent review	Advanced, threat-led assurance	Continuous improvement and innovation
Financial supervisors	Map sector, mandate and strategy	Foundational regulation and supervision	Build supervisory and sector capacity	Risk-based assurance and advanced testing	Adaptive, cross-sector oversight
Cyber service providers	Unvalidated provision	Standards commitment	Structured self-assessment	Independently accredited	Specialist financial-sector capability

Increasing assurance, capability and collective coordination

The assessment should first map the current maturity stage and then, importantly, identify the gaps to focus on to achieve the next stage of development. For example:

- If basic institutional hygiene is weak, the priority may be a minimum baseline and remediation before advanced testing.
- If institutions are ready but the authority lacks technical capability, supervisory capacity could be strengthened before new requirements are expanded.
- If requirements are established but provider supply is limited, capacity building and a pathway to international recognition may be valuable.
- If all three are relatively mature but incident coordination is fragmented, the next priority may be system-wide exercises and information convergence.

The clear message from assessing at the ecosystem-level is that delayed development in one domain undermines cyber resilience of the whole.

Setting out a multi-year programme

Taking this a step further, the supervisor or other market participants may wish to set out a multi-year, eco-system wide programme to give greater confidence that the separate domains will develop in parallel, in a coordinated way.

Table 8 provides an illustrative example:

Illustrative horizon	Financial institutions	Financial supervisors	Cyber service providers
Years 1-2: establish the baseline	Map important services; close urgent hygiene gaps; self-assess against a recognised framework; begin targeted testing.	Map and tier the sector; clarify roles; publish a baseline and strategy; strengthen internal and supervisory capability.	Assess market capacity; enter development pathways (e.g. CREST Pathway); strengthen governance, security and workforce.
Years 3-5: scale assurance	Independently assess against a financial-sector framework (e.g. CRI Profile); test all key services on a risk-based cycle.	Introduce tiered requirements; improve incident information; pilot or mandate independent testing for higher tiers.	Progress to independent accreditation (e.g. CREST member); build financial-sector experience and jointly deliver more complex engagements.
Years 5-10: embed advanced resilience	Undertake regular threat-led testing (e.g. CREST TLPT-FS or regulator equivalent) where proportionate; use continuous validation and contribute to sector learning.	Use system-wide exercises, intelligence-led oversight, supply-chain analysis and assertive remediation enforcement.	Maintain a diverse community of accredited providers with FS experience, including specialist CREST TLPT-FS capability and local leadership.

Table 8: Illustrative multi-year eco-system programme

Implementation could be governed through a senior cross-supervisor structure, supported by technical, industry and provider engagement and periodic independent evaluation.

The role of international and non-governmental organisations

There are many international and non-governmental organisations (NGOs) playing a key role in defining standards, publishing frameworks and performing independent quality assurance. A sample, but by no means all, such organisations that focus on each of the three domains of the ecosystem include:

Case study 1: Cyber Risk Institute (CRI)

The Cyber Risk Institute's mission is to advance the development and harmonisation of cybersecurity, technology, and AI risk management standards for the financial services industry. It is a not-for-profit standards development organisation focused specifically on the financial services sector. It is a member-driven organisation, with over 170 financial institutions making up its membership. CRI also works closely with its 'Innovators' and 'Affiliates', organisations leveraging CRI products into their offerings and services for financial institutions.

CRI's principal resources include the CRI Profile, Profile Maturity Model, Cloud Profile and Financial Services AI Risk Management Framework. The CRI Profile provides a common framework through which financial institutions can connect cyber threats, risk-management controls and regulatory expectations. Based on the NIST Cybersecurity Framework (aligned to CSF version 2), the latest Profile v2.2 maps about 40 regulatory references and industry standards into a more manageable set of diagnostic statements. It is intended to support self-assessment, regulatory engagement, evidence gathering, internal reporting and third-party risk management.

CRI's work supports the harmonisation and practical implementation of risk-management expectations within financial institutions. It also gives supervisors, auditors, technology suppliers and professional advisers a common structure and vocabulary through which to assess, evidence and discuss cyber risk.

Domain	CRI activities
Financial institutions	The CRI Profile, a tiered financial-sector-specific control framework for assessing cybersecurity risk, mapping controls to multiple regulatory expectations, identifying the diagnostic statements appropriate to them and assessing control effectiveness. Supporting guidance helps institutions organise evidence, monitor progress, engage boards and assess third parties. The Cloud Profile[24] and Financial Services AI Risk Management Framework[25] extend this approach to cloud and AI risk.
Financial supervisors	A consistent taxonomy and evidence structure that institutions can use when engaging regulators. The Profile's regulatory mappings can help supervisors and institutions compare internal controls with different regulatory requirements, while retaining supervisory judgement over whether the institution is managing its risks effectively.
Cyber service providers	A common framework that consulting firms, GRC providers, software companies and other suppliers can incorporate into their tools and services. CRI's Affiliate and Innovator programmes[26] support providers in integrating CRI resources into their offerings and using the same risk and control language as their financial-sector clients. A related maturity model[27] helps the service providers to assess client maturity based on their CRI Profile results and other inputs.

Case study 2: International Monetary Fund (IMF)

The International Monetary Fund is a global, member-country-governed organisation whose mandate includes supporting international financial stability.[28] It undertakes economic and financial surveillance, provides policy advice, financial assistance and delivers technical assistance and training to public authorities. Its role in cybersecurity is principally concerned with the potential consequences of cyber incidents for financial stability and with the ability of national authorities to regulate, supervise and coordinate the financial sector's response to cyber risk.

Through the Financial Sector Assessment Program[29], the IMF conducts in-depth assessments of countries' financial systems. Where cyber resilience is within scope, these assessments can examine the quality of cyber-risk regulation and supervision, the resilience of financial institutions and market infrastructures, oversight of third-party dependencies, sector-wide incident arrangements and authorities' ability to manage systemic disruption. The resulting recommendations are advisory and remain for national authorities to implement.

The IMF also publishes analysis and good-practice guidance, provides bilateral technical assistance and delivers training for national supervisors. Its 'Good Practices in Cyber Risk Regulation, 2026'[2] includes regulatory expectations and practices that the IMF believes contribute significantly to improving the cybersecurity posture of the financial system. Its wider guidance addresses governance, onsite and offsite supervision, security testing, oversight of third-party service providers, incident reporting, response and recovery, simulation exercises and sector-wide operational resilience.

The IMF's contribution is therefore weighted toward the supervisor domain, as a supportive function to them rather than a regulator itself.

Domain	IMF activities
Financial institutions	Primarily an indirect contribution. IMF assessments, analysis and recommendations inform the regulatory and supervisory expectations subsequently applied by national authorities. These cover areas such as governance, cyber-risk management, security testing, third-party dependencies, incident reporting, response and recovery, and operational resilience.
Financial supervisors	Independent assessment of financial-sector resilience and the quality of regulatory and supervisory arrangements through the Financial Sector Assessment Program, supplemented by bilateral technical assistance, supervisory tools, workshops and training. Support can include model regulation, assessment methodologies, onsite and offsite examination processes, cyber mapping, simulation exercises, incident arrangements and sector-wide crisis preparedness.
Cyber service providers	An indirect contribution through clearer expectations for systematic testing, evidence, operational resilience and the management and oversight of third-party service providers. These expectations help financial institutions and supervisors specify the outcomes they require from external providers.

Case study 3: CREST International (CREST)

CREST is a global not-for-profit focused on raising standards and building trust in cybersecurity. Within the financial-sector ecosystem model, CREST makes the capabilities of external cyber service providers and professionals more visible and comparable. It independently assesses provider organisations against published accreditation standards and assesses individual professionals through examinations, while also supporting providers in developing towards these standards.

CREST supports financial institutions in making informed buying decisions and supports supervisors in developing and implementing technical standards, assessment frameworks and regulated cyber testing programmes for providers and professionals.

Domain	CREST activities
Financial institutions	Guidance on specifying independently assured services through the procurement process, including the integration of accreditations into the purchasing requirements. CREST Marketplace to support selection of quality assured providers. Implementation guides and templates for use within cyber security engagements.
Financial supervisors	International experience on service provider standards, support setting standards for regulated cyber testing programmes; framework and guidance development support.
Cyber service providers	Open source standards with independent quality-assured accreditations, professional examinations and recognition, development through the CREST Pathway, capacity-building programmes, mentoring and international community engagement. Financial services specific accreditations and certifications to support evidencing capability.

Conclusion

Cyber resilience in financial services requires a holistic ecosystem approach, bringing together institutional maturity, empowered supervisors and a highly skilled service provider market. These elements reinforce one another and collectively grow confidence in the cyber resilience of the sector.

Financial institutions must own their critical business services and demonstrate that controls work under pressure. Supervisors must combine proportionate expectations with technical capability, system-wide insight and effective coordination. Cyber service providers must supply trusted expertise supported by organisational quality, competent people and safe methods. The national cyber authority must connect the sector to the wider national response and critical infrastructure system.

A whole-ecosystem maturity pathway provides a practical way to organise this work. It makes the starting point visible, reveals misalignment and creates a route from basic hygiene and mapping to independently assured, intelligence-led and continuously improving resilience.

Taken together, the model points to three priorities for building stronger and more sustainable cyber resilience across the ecosystem:

Ecosystem measurement: Make the ecosystem maturity, including shared dependencies, a key measurement of national cyber resilience.

Common language: Adopt a common language and framework for institutional requirements, supervisory approach and trusted provider capability, enabling cross-border consistency.

Development support: Recognise the areas in each part of the ecosystem that need to accelerate and bring them forward in unison, ensuring no part gets left behind.

The opportunity is to move beyond siloed initiatives and build a coherent programme that is risk-based, standards-led, independently assured and locally sustainable. The measure of success will be the financial system's ability to continue delivering critical services, contain harm, recover safely and learn faster in an era of AI-enabled adversaries and evolving threats.

References

1. Committee on Payments and Market Infrastructures and International Organization of Securities Commissions, Guidance on cyber resilience for financial market infrastructures, Bank for International Settlements, 2016. https://www.bis.org/cpmi/publ/d146.htm
2. Tamas Gaidosch, Emran Islam, Tanai Khiaonarong, Rangachary Ravikumar and Chris Wilson, Good Practices in Cyber Risk Regulation and Supervision, International Monetary Fund, 2026. https://www.elibrary.imf.org/downloadpdf/view/journals/087/2026/001/087.2026.issue-001-en.pdf
3. https://www.nist.gov/cyberframework
4. https://cyberriskinstitute.org/cri-profile-overview/
5. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
6. https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide
7. https://www.ecb.europa.eu/press/intro/cons/html/cyber_resilience_oversight_expectations.en.html
8. https://www.iosco.org/about/?subsection=cpmi_iosco
9. https://www.gov.uk/government/publications/g7-fundamental-elements-of-collective-cyber-incident-response-and-recovery-in-the-financial-sector
10. https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html
11. https://www.crest-approved.org/threat-led-penetration-testing-guidance-for-financial-services/
12. https://www.crest-approved.org/skills-certifications-careers/crest-certified-red-team-specialist/
13. https://www.csis.org/blogs/strategic-technologies-blog/select-list-global-cyber-incidents-reporting-requirements
14. https://www.cyberthreatalliance.org/resources/assets/cyber-incident-reporting-framework/
15. https://www.bis.org/bcbs/publ/d454.htm
16. https://www.bis.org/cpmi/publ/d146.pdf
17. https://www.iais.org/activities-topics/cyber-risk/
18. https://www.iif.com/portals/0/Files/private/iif_cyber_reg_04_25_2018_final.pdf
19. https://www.aeaweb.org/articles?id=10.1257/pandp.20191058
20. https://www.imf.org/en/publications/tnm/issues/2025/03/21/strengthening-cybersecurity-lessons-from-the-cybersecurity-survey-559636
21. CREST, The Accreditation Pathway. https://www.crest-approved.org/membership/crest-accreditation-pathway/
22. CREST, CREST CAMP and related capacity-building resources. https://www.crest-approved.org/membership/crest-camp/crest-camp-faqs/
23. CREST, Threat-led Penetration Testing: Guidance for Financial Services, 2026. https://www.crest-approved.org/threat-led-penetration-testing-guidance-for-financial-services/
24. https://cyberriskinstitute.org/cloud-profile/
25. https://cyberriskinstitute.org/financial-services-industry-unites-to-launch-comprehensive-ai-risk-management-framework/
26. https://cyberriskinstitute.org/how-we-work-together/
27. https://cyberriskinstitute.org/maturity-model/
28. https://www.imf.org/en/about
29. https://www.imf.org/en/publications/fssa



Seven Stars
House, 1 Wheler
Road, Coventry,
West Midlands,
CV3 4LB

© 2026 CREST (International), All Rights Reserved