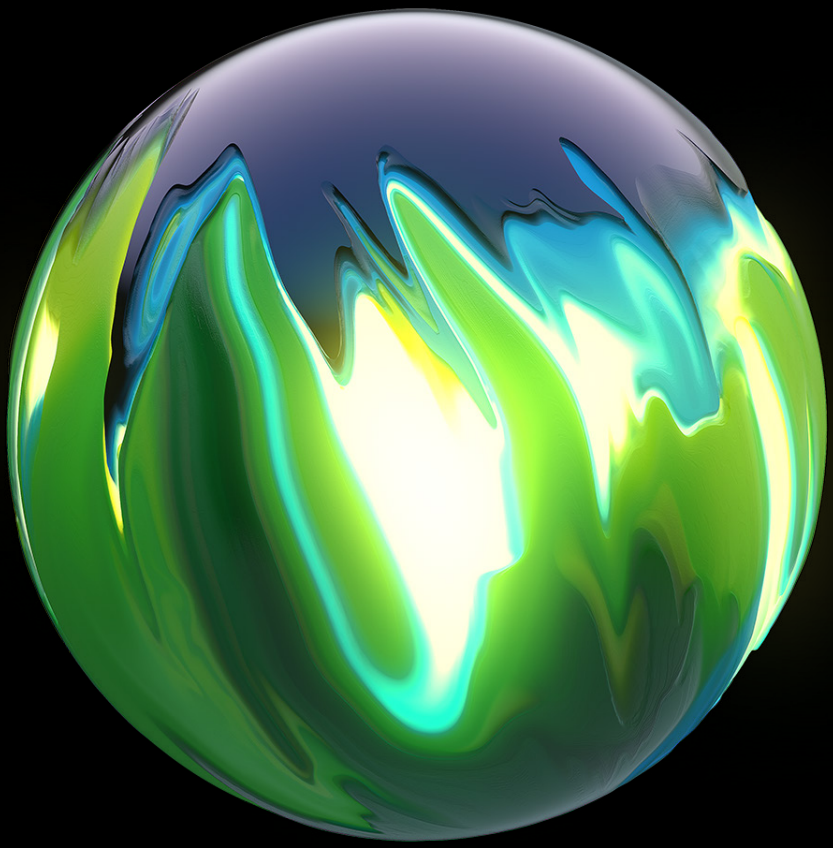
Deloitte.



Cyber-Financial Services

The threat landscape within financial services is increasing even as organisations accept working practices suitable for a diminished threat landscape, representing a potential mismatch that could expose organisations to considerable risk.

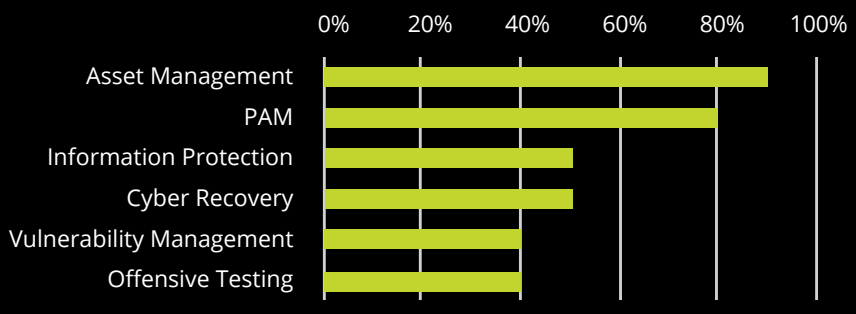
With increased attacks from both organised criminal and state actors, regulatory bodies are not relaxing on the need to protect consumers and information.

With ransomware now the most significant threat facing organisations today and with the attacks becoming more sophisticated and challenging to prevent, building operational resilience to cyber risk in the financial services is a rapidly growing priority for regulators.

Organisations must reconcile a growing threat landscape with their continuity measures.

Industry Survey

Based on a survey undertaken with selected organisations across the **financial services** industry, we identified six key priorities for cyber. Asset management was highlighted as the number one priority indicating the need to identify and assign ownership to the "crown jewels". The benchmark also highlights that organisations have started or are continuing their journey to secure privileged access, as this is considered one of the most significant security threats affecting the industry today.



Industry Trends

Businesses are willing to accept increased risk and a **reduction in security and control requirements** in order to facilitate business continuity measures:

- 60% of the workforce globally now work remotely
- Many organisations have reduced numbers of staff to deal with any arising issues from the increased risk
- Increased reliance on unapproved personal devices
- Large increase in number of endpoints with fewer security controls applied
- Sensitive documentation is being accessed from an increased number of locations, which are less secure (e.g. call centre employees accessing confidential records from home

Industry Hot Topics

Cloud

Organisations are migrating entirely or partially to cloud requiring new security measures; multi-cloud environments present more vulnerabilities. Cloud capabilities and solutions focus on development, transformation and resilience of cloud security and on helping organisations throughout the complete cycle of moving business processes to the cloud and operating it in a secure and private way.

Cyber Financial Crime

Cyber crime has grown dramatically in the FS industry over the past few years as cyber criminals constantly adopt more profitable, effective, and efficient tactics. Cyber crime is on the rise, not only in the number of attacks but also in its severity. With businesses' digital activities continuing to grow, organisations are exposed to more security risks than ever before.

Zero-Trust & Identity

Managing identities, access, and privileges continues to be a foundational component of digital transformation, operational efficiencies, and compliance. Zero-trust network trusts no one by default, within or outside of the network, and reduces risks associated with excessive privileges and significantly improves detection and response.

Detect & Respond

Detect and Respond capabilities help organizations build and operate dynamic security monitoring and threat detection functions as well as respond to the identified threats and attacks. Security teams often do not have complete visibility of their entire threat landscape with relevant context, including internal and external data sources. This reduces their ability to detect and remediate major cyber attacks.

Red Teaming

With increasing pressure from the regulators globally to perform ethical hacking exercises and test organisations' readiness against cyber attacks, banks and insurers seek to perform red teaming exercises on their systems. Such exercises use various techniques, e.g. phishing and social engineering, to provide real-world attack simulations and improve organisations' abilities to respond to a cyber attack.

Cyber Financial Crime

Cyber crime has grown dramatically in the FS industry over the past few years as cyber criminals constantly adopt more profitable, effective, and efficient tactics. Cyber crime is on the rise, not only in the number of attacks but also in its severity. With businesses' digital activities continuing to grow, organizations are exposed to more security risks than ever before.

Digital Transformation

Any digital transformation effort the organisation is undergoing should be accompanied with secure digital applications, infrastructure, processes / training, etc. Our capabilities in this space focus on implementation of relevant solutions, supporting the change side of the transformation initiatives, and transition into BAU.

Recover & Transform

Recover and transform focuses on developing and updating methodologies and frameworks to empower businesses to become more resilient through recovery from incidents and further transformation. We help organisations design and implement transformational enterprise security programs with an emphasis on defending against, recovering from, and remediating major cyber-attacks.

Deloitte CISO Programme

Building connected leaders in the cyber community: a space for our security leaders to become better leaders.

What is the Deloitte CISO programme?

The programme provides tools to help our clients succeed in the CISO role, **with engaging events, international networking opportunities, executive coaching, transition labs and market leading insight**. An important focus of the programme will be on individual and personal career progression, developing both soft and technical skills to improve board relations, company support and investment in the CISO function.

This is an exclusive members-only community and there is no membership charge to be part of the programme.

Programme Activity:

- Small roundtable discussions
- Virtual webinars and seminars
- Thematic content
- CISO Forum
- Facilitated labs and workshop
- Events and conferences
- Insight papers and articles
- Networking opportunities

Deloitte CISO application process:

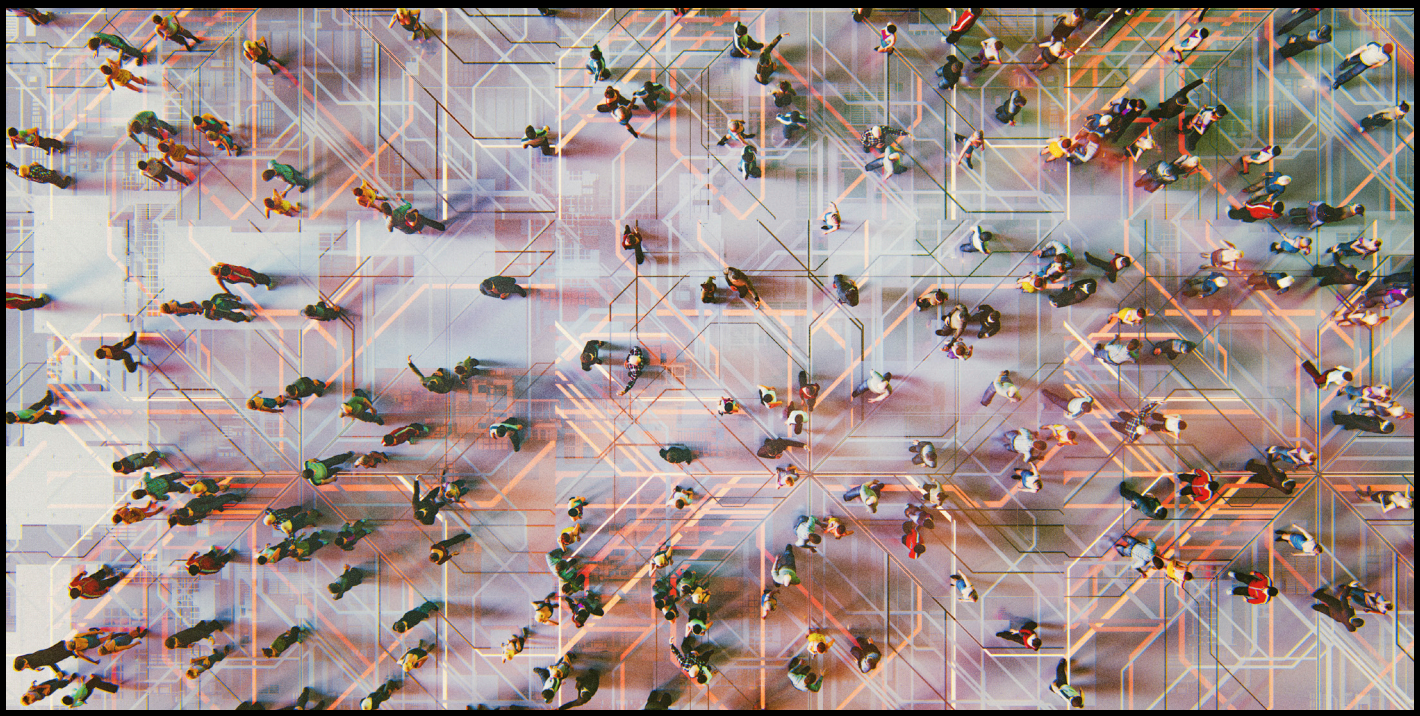
- Clients can apply by filling out an application form on this page.
- The application is sent to a central mailbox which the Irish Business Partnering team has access to. The request is then assessed and sent on to the Cyber team to see if they approve.
- Once approval has been received the client is added to the marketing list and we will receive all future invites and thought leadership.

Recent Initiatives:

- Operational Technology Security
- Future of Cyber
- Managing the successful convergence of information and operational technology
- Securing your move to – and operating in – the cloud

Why Deloitte Cyber

1. End-to-end solutions combining deep technical expertise with high-end advisory skills of Deloitte professionals.
2. Tailored on-site, near and offshore based cyber security services to support your agility needs at a competitive price point.
3. Market leading cyber capabilities and experience with large compliance and security projects across all industries.
4. Local teams of senior specialists across Europe and the world who are technically certified and experienced in complex programs.
5. Globally standardised offerings and strategic alliances with the leading international Vendors.



For further information please contact:

Colm McDonnell
Partner | Risk Advisory
+353 87 813 8198
cmcdonnell@deloitte.ie

Dublin
29 Earlsfort Terrace
Dublin 2
T: +353 1 417 2200
F: +353 1 417 2300

Cork
No.6 Lapp's Quay
Cork
T: +353 21 490 7000
F: +353 21 490 7001

Limerick
Deloitte and Touche House
Charlotte Quay
Limerick
T: +353 61 435500
F: +353 61 418310

Galway
Galway Financial Services Centre
Moneenageisha Road
Galway
T: +353 91 706000
F: +353 91 706099

Belfast
19 Bedford Street
Belfast BT2 7EJ
Northern Ireland
T: +44 (0)28 9032 2861
F: +44 (0)28 9023 4786

Deloitte.ie

Deloitte.

At Deloitte, we make an impact that matters for our clients, our people, our profession, and in the wider society by delivering the solutions and insights they need to address their most complex business challenges. As the largest global professional services and consulting network, with over 312,000 professionals in more than 150 countries, we bring world-class capabilities and high-quality services to our clients. In Ireland, Deloitte has over 3,000 people providing audit, tax, consulting, and corporate finance services to public and private clients spanning multiple industries. Our people have the leadership capabilities, experience and insight to collaborate with clients so they can move forward with confidence.