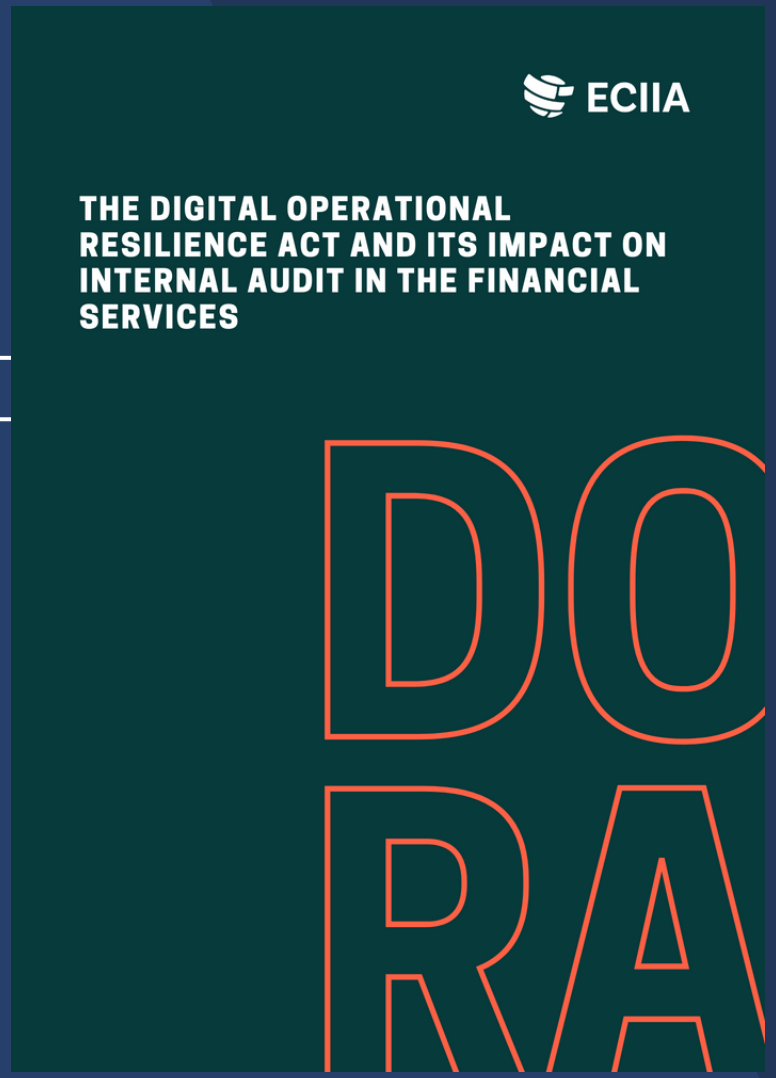
DIGITAL EUROPE: NEWS ON EU REGULATIONS IMPACTING THE PROFESSION

WEBINAR | 13 DECEMBER | 11:30-12:30 (CET)

ECIIA



PUBLCIATION

AVAILABLE AT ECIIA.EU

Learning Objectives

Increasing stakeholder awareness of the importance of managing ICT risks

- We will focus on the Digital Operational Resilience Act (DORA). DORA aims to improve the existing cybersecurity posture of EU Financial Institutions, that is being transposed by EU Member states in 2024.
- We will analyze the potential effects of the DORA regulation on covered entities.
- We will debate the role of internal audit in the implementation project and the oversight, assurance and assessment of cyber risk to board subcommittees, accountable executives and Board attestation.
- We will debate the risks and opportunities facing internal audit in providing assurance of cyber regulatory compliance.

Internal audit are critical to the oversight, assurance and attestation of cyber risk management regulation

THE AUGUSTA GROUP

ECIIA

EU Digital Operational Resilience Act (DORA)

Operational resilience for the European Union's Finance industry

Title

Directive (EU) 2022/2554 of the European Parliament and of the Council on Digital Operational resilience for the Financial sector

Status

- Added to the EU Journal 17th January 2023.
- Transposed by member states by October 2024.
- Compliance starts on the 17th January 2025.

Scope

The scope is extensive across Financial Institutions and includes credit and payment institutions, central counterparties, trading venues, investment firms, electronic money firms, crypto asset providers, (re)insurance firms, (re)insurance intermediaries, pension funds, credit rating agencies, financial management companies and ICT third-party providers.

A comprehensive cyber regulation affecting EU Financial Institutions

Regulatory highlights

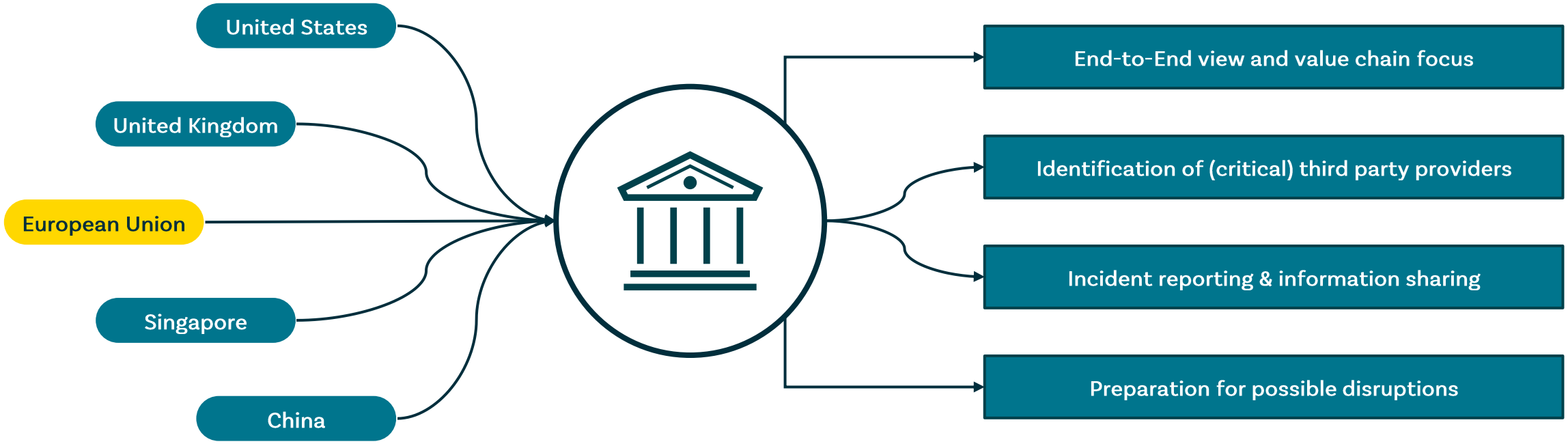
1. Covered Financial Institutions, and their management bodies are required to
   - Implement governance and control frameworks to ensure management of ICT risk.
   - Follow a risk-based approach to the management of ICT risks. Implementing security policies, procedures and risk mitigation.
   - Manage, oversight, assure and report compliance to their ICT risk management framework.
   - Monitor and oversea their third-party ICT risk exposure.
   - To have the knowledge and skills to assess and manage ICT risk.
   - Report on ICT risk management strategy, policies, procedures and risks to their regulator.
   - Threat Led Penetration Testing (TLPT).
   - Establish and test incident response plans and crisis management communications.
2. European Supervisory Authorities will independently oversight and assure critical ICT provider cyber risk management.

The 3rd Line is critical for compliance assurance and attestation.

The act provides for the imposition of criminal penalties (Article 52)

ECIIA

Operational resilience as global priority with common focus areas



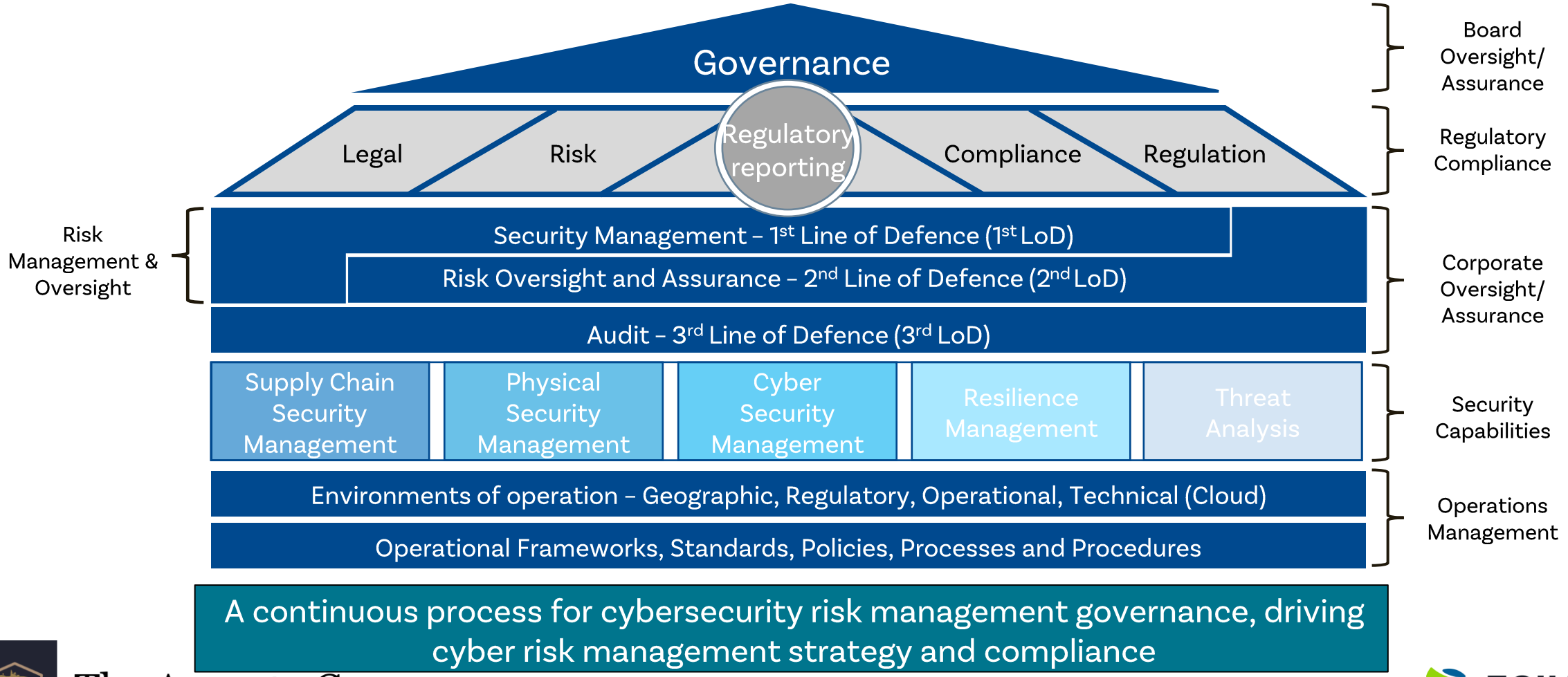
While there is a common understanding of key aspects to achieve operational resilience,
International efforts still show heterogenous maturity levels and deviating cross-jurisdictional designs

ECIIA

Regulatory compliance and corporate governance

A 3 Line of Defence for cyber risk governance, oversight, assurance and attestation

Cyber risk management Governance



The Augusta Group

ECIIA

Cybersecurity risk Governance process

A process to oversight, assure and attest cybersecurity risk management

The Governance process

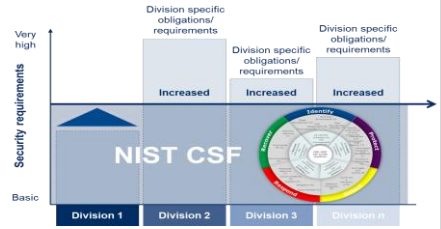
Cybersecurity risk management compliance is a continual process of evaluation, mitigation, oversight, and assurance of cyber risks based upon known threats and vulnerabilities, against a cybersecurity baseline. Reporting compliance status to the board for attestation.

Governance

Continuous evolution of cyber security risk, oversight, assurance

- Legal, risk and compliance evaluation, oversight, assurance.
- Cybersecurity standards.
- Cyber threats, vulnerabilities, risk taxonomy.
- KPIs, KRIs, Control effectiveness
- Governance [illegible]ting.

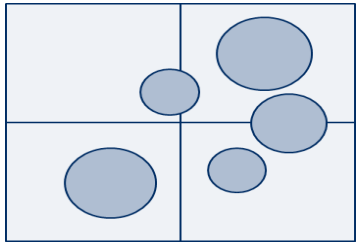
Risk assessment



Continuous cybersecurity risks baseline assessment and reporting.

- Evaluation inherent risk exposure in line with business strategy, markets and products.
- Evaluate cyber threats, vulnerabilities and risks.
- Evaluate control effectiveness.
- Evaluate of residual risk.

Mitigation, evaluation



Risk treatment and mitigation planning

- Prioritize cyber risks.
- Prioritize cyber control effectiveness,
- Develop a risk mitigation program, action plans (POAM) and funding.
- Remediate known risks and re-evaluate residual risk.

Reporting

Management and regulatory reporting

- Audit oversight, assurance and reporting.
- Committee reviews of cyber risk management compliance.
- Management committee review of cyber risk management compliance.

The Augusta Group

ECIIA

Majority of requirements are already covered by Internal Audit functions

End-to-End view of important business processes

› End-to-End view, incl. sourcings, as basis for audit programs

› Importance of business processes as one key component for determining audit cycle

Regular BCM and incident management audits

› Regular BCM and incident management audits as backbone of audit programs

Third Party & Vendor Risk Management

› Right to access and right to audit incorporated into legal frameworks

› Pooled audit approach established, e.g. Collaborative Cloud Audit Group

Cyber resilience testing

› Regular cyber resilience audits along with accompaniment and integration into TIBER testing

Operational resilience assurance incorporated into audit programs.
International regulatory efforts require review and targeted enhancements of existing audit programs and practices.

ECIIA

Targeted review and improvements of audit programs necessary…

Theses of Impact Areas

01 With ESA's being appointed as lead overseer for each Critical Third Party Provider, FI's IA functions will have to evaluate the impact on their own audit plans as outsourcing entity and how to align on remediation activities. Audit results should be reflected in own audit activities.

02 FI's IA functions should elaborate a collaboration model among each other as well as with IA of relevant third parties in order to comply with regulatory expectations.

03 With an even higher attention on (sub)outsourcings, regular testing activities and full accountability for third parties' regulatory compliance, FI's IA functions should analyze whether their audit approach needs to be adjusted (e.g. stronger focus on concentration risks)

04 FI's IA functions should verify the appropriateness of their external follow-up processes to ensure a consistent remediation of findings at third parties.

05 …

ECIIA

… along with continuous assurance activities

Theses for Assurance Strategies

01 Given, that FI's have to deal with a complex international regulatory environment, IA functions should promote local best efforts to be implemented groupwide.

02 IA functions should design an individual assurance strategy, e.g. continuous monitoring review of operational resilience project activities, support with knowledge of end-to-end process, etc.

03 IA functions should integrate adjusted regulatory requirements into this and next years audit programs to evaluate the suitability of existing audit approaches.

04 Pooled audits on (cloud) service providers are possible to reduce the costs to an individual FI and to the service provider. Pooled audits must meet FIs' internal needs and regulatory requirements.

05 …

ECIIA

The Augusta Group

Author: Andy Watkin-Child

LI: www.linkedin.com/in/andywatkinchild/

email: andy@augustagrp.com, andy@parava.org

Web: www.augustargrp.com

Andy Watkin-Child CSyP, CEng, AMAE
Cyber risk management advisor, former Group VP Cyber Risk, CISO, Counsel appointed cyber adviser (https://www.linkedin.com/in/andywatkinchild/)

Note
* Most significant cyber regulations affecting international organisations in the authors opinion (2022/ 2023)
** SEC cybersecurity risk management proposal for entities covered by the Security and Exchange Act 1934.

Andy Watkin-Child CSyP, CEng, MSyI, MIMechE, AMAE

Chartered Security Professional, Risk Advisor, CISO, Counsel appointed Cyber Expert

https://www.linkedin.com/in/andywatkinchild/

- A technology, risk and security executive with over 20 years experience as Group VP cyber risk, Chief Information Security Officer (CISO), Head of IT and European head of cyber and risk.
- I have built and led global 1st and 2nd Line of Defence cybersecurity and risk management functions for several blue chip organisations.
- I hold Royal Chartered Security Professional (CSyP) and Chartered Engineer (CEng).
- Member of the Register of Chartered Security Professionals.
- Andy is member of the Board of the Security Institute (MSyI).
- Practicing Associate of the Academy of Experts (AMAE).
- Counsel appointed cybersecurity and risk expert and witness.
- A Freemen of the Worshipful Company of Security Professionals (WCoSP) 109th City of London Livery Company.
- Freeman of the City of London.
- Founding Partner of Parava Security Solutions and the Veritas Governance and Regulatory Compliance (Veritas GRC).
- Founding member of the CMMC AB Standards Working group.