Compliance & Risks

Webinar

Cybersecurity Compliance *Decoded*

Emerging Requirements Impacting **Product Compliance**

30th October, 2024

→ | complianceandrisks.com

Q&A Session

Slides & Webinar Recording

Request a Demo

Webinar Platform Tips

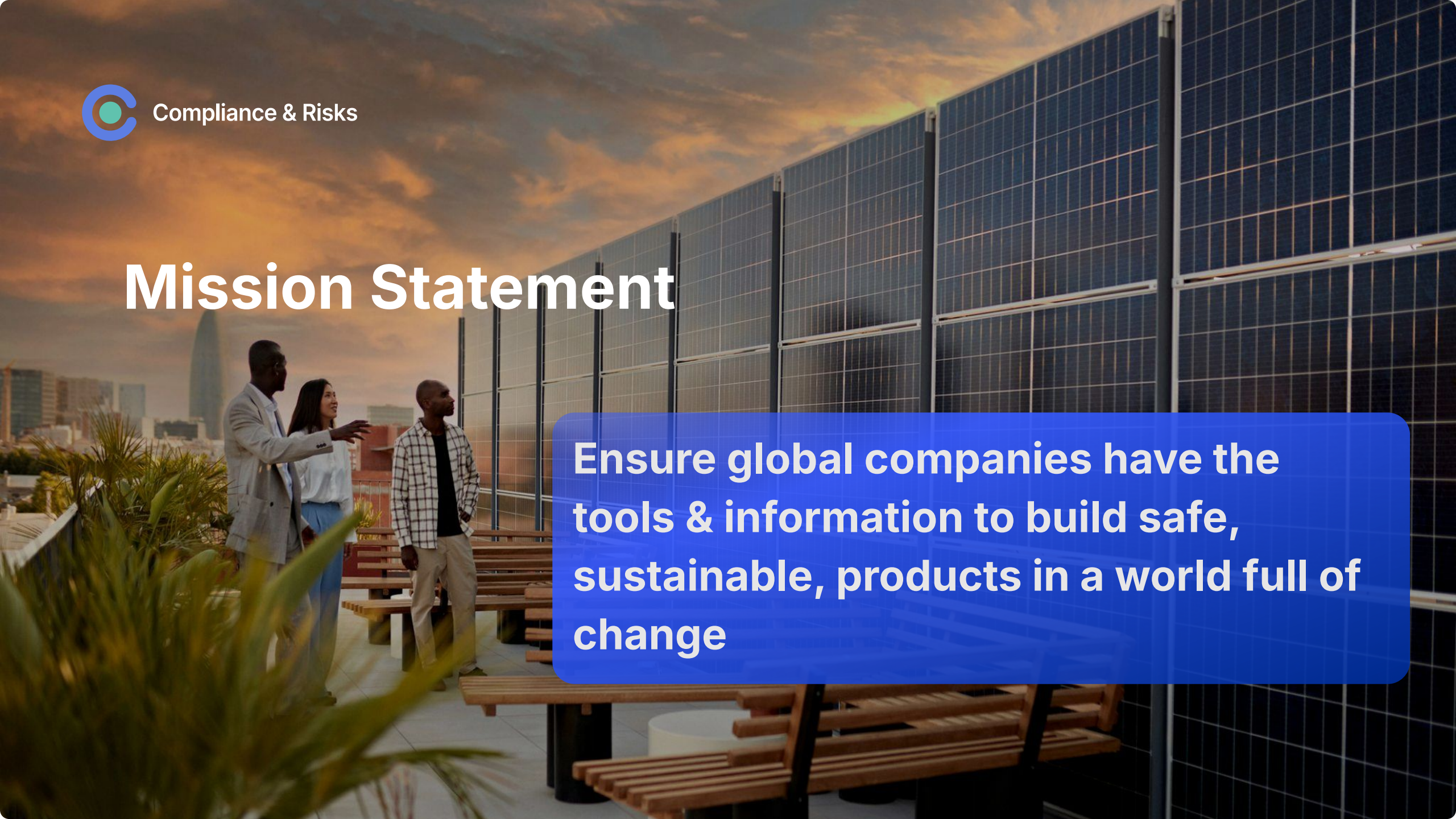
Compliance & Risks

Meet the Team

Ashley Weeks
Senior Regulatory Compliance Consultant, RINA Tech UK Ltd

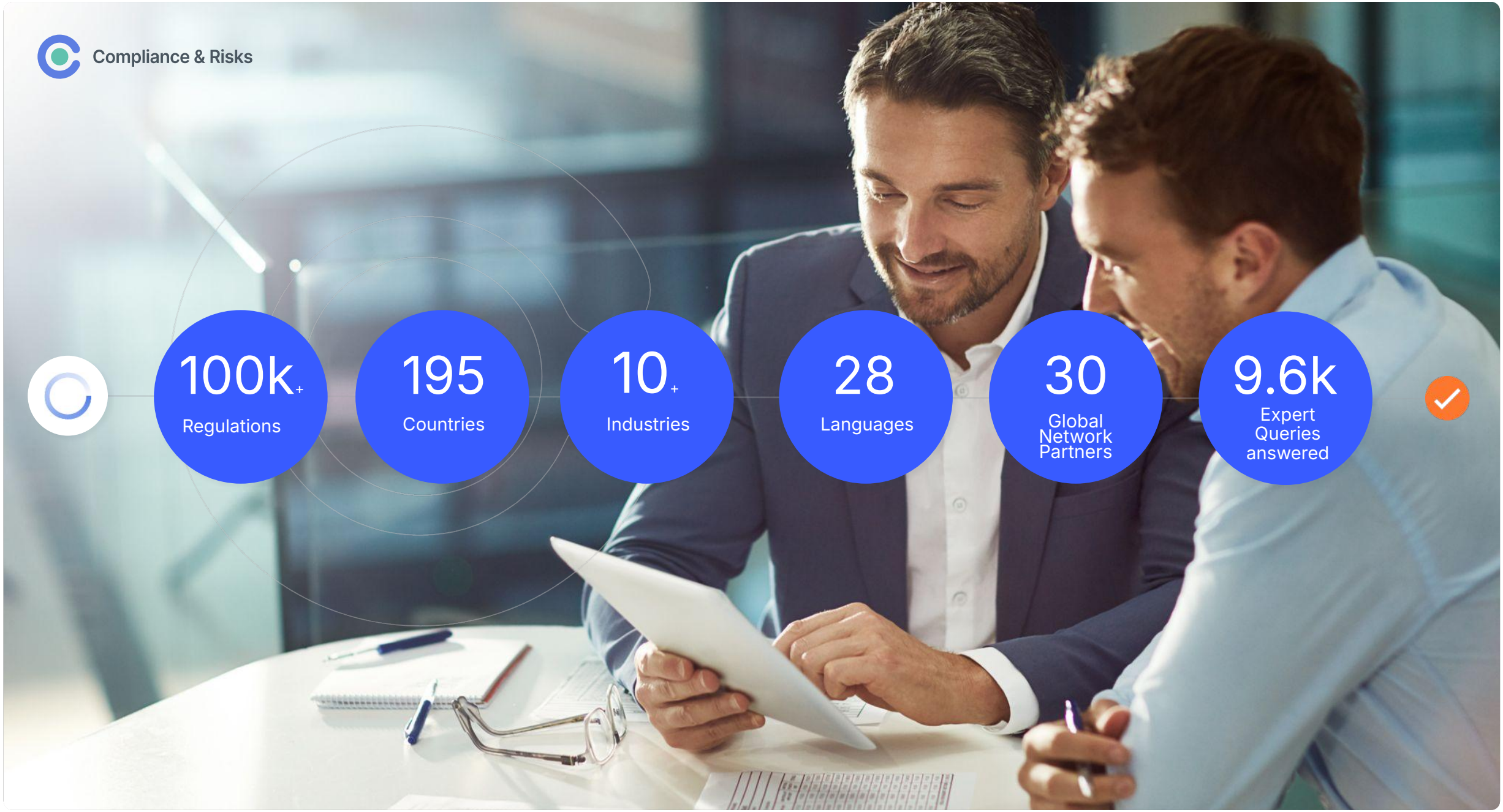
Therese Hogan
Product Manager, Compliance & Risks

Orlaith Morris
Content Marketing Manager, Compliance & Risks


Compliance & Risks
Mission Statement
Ensure global companies have the tools & information to build safe, sustainable, products in a world full of change

Trusted by the World's Leading Brands

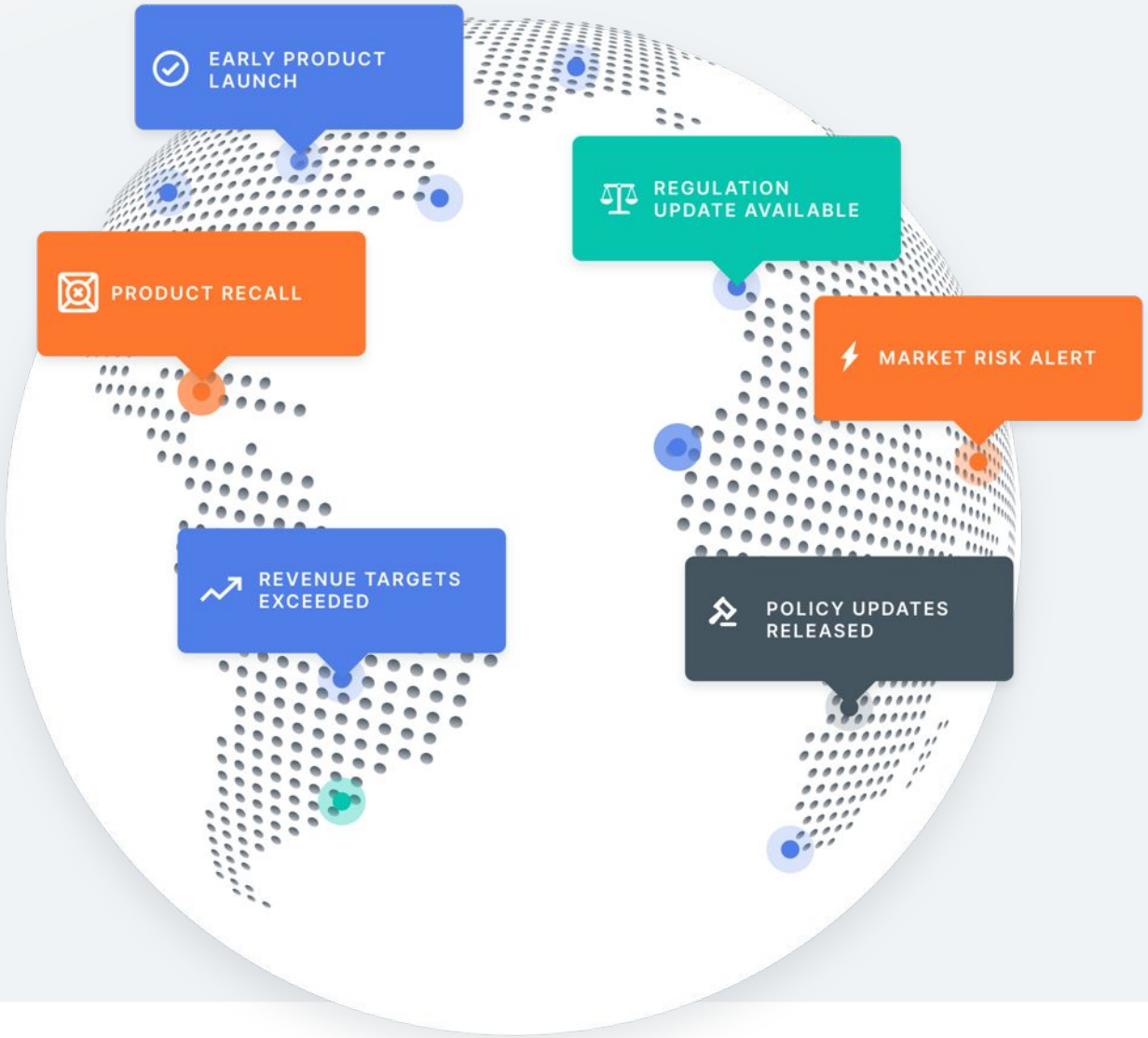
Compliance & Risks



WHAT WE DO

Unlocking Market Access

Keep on top of regulatory changes and their impact worldwide. Early warning alerts, impact probability, productivity workflow tools and so much more.



Compliance & Risks

RINA Overview

→ | complianceandrisks.com

RINA Tech UK Ltd – Regulatory Compliance Group

We support authorities, manufacturers, importers and distributors of products, to identify, understand and meet technical and environmental legislation.

Global Market Access

- Low Voltage
- Electromagnetic Compatibility (EMC)
- Pressure equipment
- Radio Equipment
- Medical Devices
- Machinery
- Hazardous Area (ATEX)
- Substances (RoHS/REACH/CLP/BPR/POPs/Cal. Prop. 65)
- Ecodesign
- Electrical waste (WEEE)
- Batteries
- Conflict Minerals
- Transportation

Compliance & Risks

Cybersecurity - emerging requirements impacting product compliance

Ashley Weeks
Senior Product Regulatory Consultant

Webinar Objectives

- What is happening in the UK? An introduction to UK PSTI
- What is happening in Europe? An introduction to EU CRA
- What will trigger the legislation for a business?
- Assessing vulnerability requirements i.e. are processes working
- Relationship with other legislation – RED Directive (Article 3.3), new Machinery Regulation
- How cyber-attacks can impact ESG matters (Where is the “C” in ESG?)

Why is Cybersecurity a concern in relation to Product Compliance?

Why is it prominent?

How do cyber-attacks happen?

Lack of support!

Are current products on the market cyber-secure?

Compliance & Risks

UK Legislation

The Product Safety & Telecommunications Infrastructure Act (PSTI)

→ | complianceandrisks.com

PSTI Act and Regulations

Came into effect on the 29th April 2024

Aim:

- This Regulation aims to provide baseline security requirements for IOT devices who sell to UK consumers

Scope:

- Products that fall within scope of PSTI are defined as “Relevant Connectable Products” (RCPs)

RCPs are defined as:

- Products which are internet connectable, and are not an excepted product
- Products which are network connectable, and are not an excepted product

Excepted Connectable Products

Excepted connectable products

- Products made available for supply in Northern Ireland to which relevant legislation applies
- Charge points for electric vehicles
- Medical devices
- Smart meter products
- Desktop and Laptop computers, Tablets which do not have the capability to connect to cellular networks (unless for children under 14 years)

PSTI Act and Regulations

Who has to comply?

The Act sets out the duties of the relevant persons, in a similar way to how European Directives/Regulations lay out obligations of ‘economic operators.’

- **Manufacturer** must ensure that products placed on the market have met security requirements
- **Authorised representative:** If acting on behalf of a manufacturer
- **Importers and Distributors** also have duties placed upon them to not make available a product unless it is accompanied by a statement of compliance with proof of meeting those security requirements.

All have a duty to ensure consumers are protected!

PSTI Act and Regulations

How to comply?

- **Banning universal default and easily guessable passwords** - Passwords must be unique per product, not based on incremental counters, nor based on publicly available information etc.
- **Publishing information on how to report security issues** - at least one point of contact to allow a person to report security issues, which must be free of charge, they must acknowledge and offer status updates until resolution has been resolved.
- **Publishing information on minimum security update periods** - The defined support period must be published, if it changes or is extended, it shall be defined as soon as practicable.

Where to find more information

https://www.legislation.gov.uk/ukpga/2022/46/section/56/enacted
https://www.legislation.gov.uk/uksi/2023/1007/contents/made
https://www.gov.uk/guidance/regulations-consumer-connectable-product-security

Compliance & Risks

EU Legislation

The EU Cyber Resilience Act (CRA)

complianceandrisks.com

EU Cyber Resilience Act

Expected to enter into force Q1 2025

Aim:

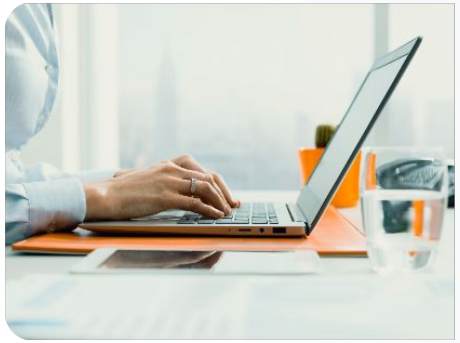
- To fill the gaps, clarify the links, and make the existing cybersecurity legislative framework more coherent, ensuring that products with digital components, for example IoT products, are made secure throughout the supply chain and throughout their lifecycle.

Scope:

- Applies to “Products with Digital Elements (PDEs) whose ‘intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network”.

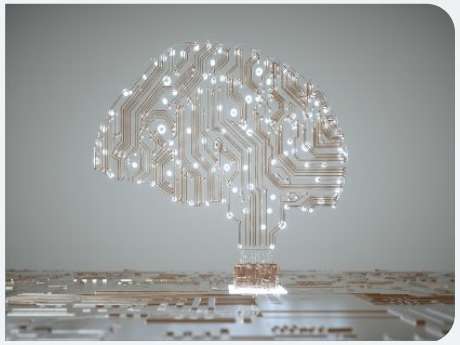
PDEs are defined as:

- Any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately.



PDE end devices (laptops)

PDE software (mobile apps)



Components (CPU’s)

Exclusions

The regulation proposes the following exclusions

- **PDEs** covered by Regulation (EU) 2017/745 (Medical Devices)
- **PDEs** covered by Regulation (EU) 2017/746 (In Vitro Diagnostic Medical Devices)
- **PDEs** covered by Regulation (EU) 2019/2144 (Motor Vehicles)
- Products certified in accordance with (EU) 2018/1139 (Civil Aviation)
- Equipment that falls within scope of Directive (EU) 2014/90 (Marine Equipment)
- **PDEs** developed exclusively for national security or military purposes
- Spare parts made available to replace identical components in PDEs

Relationship to Sectoral Legislation

EU AI Act

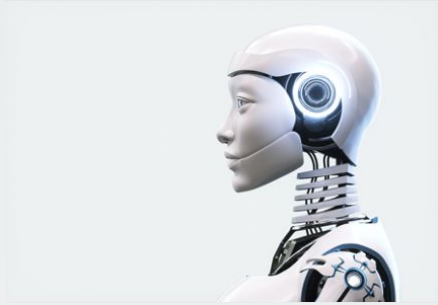
- PDEs classified as high-risk AI systems which fulfil the essential requirements of the CRA, shall be deemed compliant against the cybersecurity requirements set out in the AI Regulation.

New Machinery Regulation

- Machinery Products which are PDEs and have a DOC against the EU CRA, should comply with relevant essential health and safety requirements of the new Machinery Regulation 2023/1230/EU. However, there is currently no synergy between the legislations, Synergies may take place at standards level.

Radio Equipment Directive

- The CRA is aligned with the requirements of the RED Delegated Regulation 2022/30/EU (Cybersecurity Requirements).



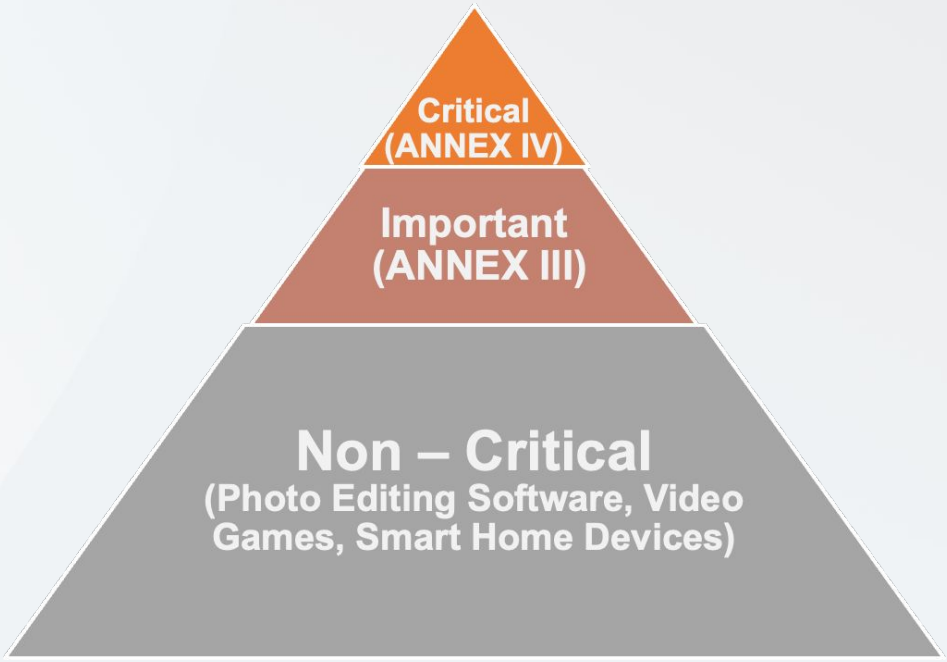
Criteria and Requirements

Different requirements apply to economic operators that are consistent with other CE marking-type legislation

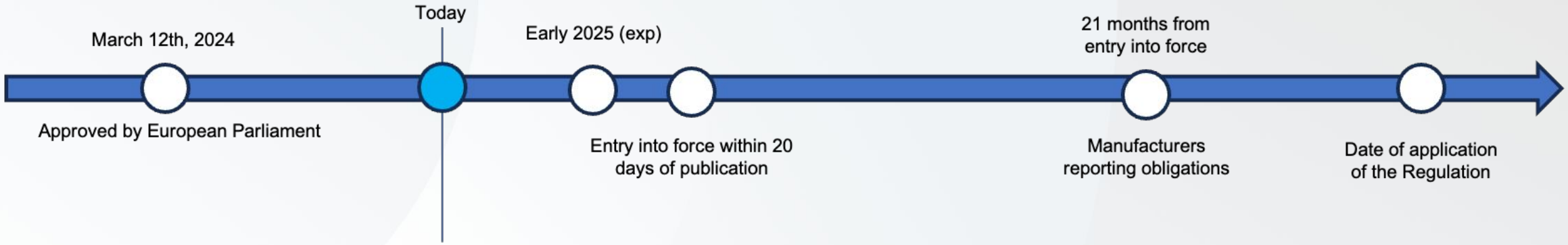
The CRA provides two sets of basic essential requirements:

- **Essential cybersecurity requirements** in Annex I, Section 1 of the CRA proposal
- **Vulnerability handling process requirements** in Annex I, Section 2 of the CRA proposal.

Products subject to more stringent requirements are listed in Annex III (Important Products) or listed in Annex IV (Critical Products).



EU CRA Timeline



Upon the CRA Act entering into force, Guidance from the EU Commission is expected in relation to the scope of the CRA.

Where to find more information -
https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_5375

Penalties

Penalties for infringements by economic operators lie with individual Member States. However, the regulation sets onerous administrative fines starting from €5 million and can result in much larger fines.

Compliance & Risks

Global

Overview of Global Cybersecurity Requirements

→ | complianceandrisks.com

IoT Cybersecurity Regulations Across the World

There is no Silver Bullet!

Legislation is rapidly evolving, and that is being reflected in IoT Cyber Security Regulations across the world. Examples include:

- **Australia** Code of Practice
- **Canada** Personal Information Protection and Electronic Documents Act (PIPEDA)
- **China** Guidelines for the Construction of IoT Basic Security Standard Systems
- **Japan** IoT Security Safety Framework
- **USA** IoT Cybersecurity Improvement Act of 2020
- **U.S** Cyber Trust Mark (Voluntary)

Why is ETSI EN 303 645 key?

ETSI EN 303 645 is a globally applicable standard for consumer IoT cyber security. It was developed to provide the foundation of the “basic”-level IoT assurance under the EU Cybersecurity Act (CSA)
Compliance with ETSI EN 303 645 is a requirement in several jurisdictions (Australia, India, UK, Singapore)
ETSI EN 303 645 can be used (in part) to comply with regulations in other markets (Canada, China, USA, Japan)

Compliance & Risks

EU Legislation

The Rising Role of Cybersecurity in ESG

→ | complianceandrisks.com

The 17 Sustainable Development Goals (SDGs)

The Rising Role of Cybersecurity in ESG

How can organisations address cybersecurity concerns?

- Integrate Cybersecurity into ESG Strategy
- Invest in Employee Training
- Explore Emerging Capabilities
- Establish Strong Governance Mechanisms
- Leverage Advanced Technologies

How can RINA Help?

- Provide technical training and high-level briefings
- Assess what cybersecurity regulatory requirements apply to your products and your business
- Assess compliance versus standards clause by clause
- Assess the adequacy of your due diligence efforts
- Assistance with Risk Assessments
- Review of Technical Files / Declaration of Conformity
- Assess Vulnerability Disclosure Policies

For more info:

Thank you for your attention

Ashley Weeks
Senior Consultant - RINA
ashley.weeks@rina.org

Compliance & Risks

Holistic Market Access Solutions

A Smarter Way to Manage Cybersecurity Compliance

→ | complianceandrisks.com

Supporting Your Product Compliance Journey

Identify Relevant Regulations

Upcoming & Proposed Regulatory Changes

Communicate Compliance Requirements

Manage Evidence Documentation

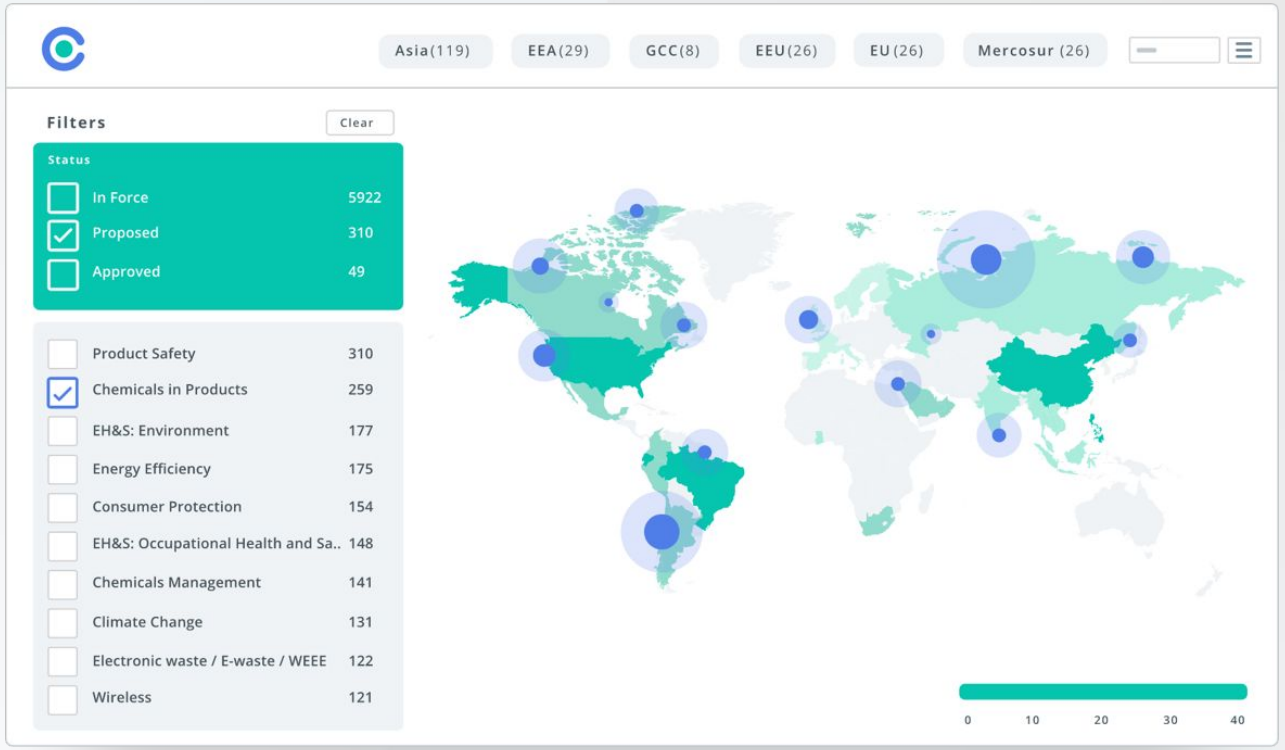
Extensive Regulatory Content Coverage

With C2P you have access to 100,000+ regulations, Standards & Product Requirements that enable you to gain and maintain market access for all your products globally.

- Artificial Intelligence (AI)
- Batteries
- Brexit
- California Proposition 65
- Carbon Footprint
- Chemicals in Products
- Chemicals Management
- Circular Economy
- Climate Change
- Conflict Minerals
- Consumer Protection
- COVID-19
- Cybersecurity
- Data Protection
- Drinking Water
- Ecodesign
- Ecolabeling
- Electromagnetic Compatibility (EMC)
- Electronic Waste / E-Waste / WEEE
- Energy Efficiency
- Explosive Atmospheres / ATEX
- EU Reach
- Food Contact Materials and Articles
- Globally Harmonized System (GHS)
- Illegal Logging
- Nanotechnology
- Packaging
- Product Safety
- Single-use Plastics
- Transboundary Movement of Hazardous Waste
- Transport of Dangerous Goods
- Water Efficiency
- Wireless

Manage all your Product Cybersecurity Compliance in One Place...

- Design, build & collaborate on new products with confidence
- Keep all compliance evidence up to date & live linked back to their Regulations, Standards & Requirements
- Continually monitor regulatory changes & keep ahead of proposed changes before they happen



Compliance & Risks

Industry Coverage

Consumer Electronics

Apparel

Household Appliances

Medical Devices

Home Furnishings

Automotive

Textile Manufacturing

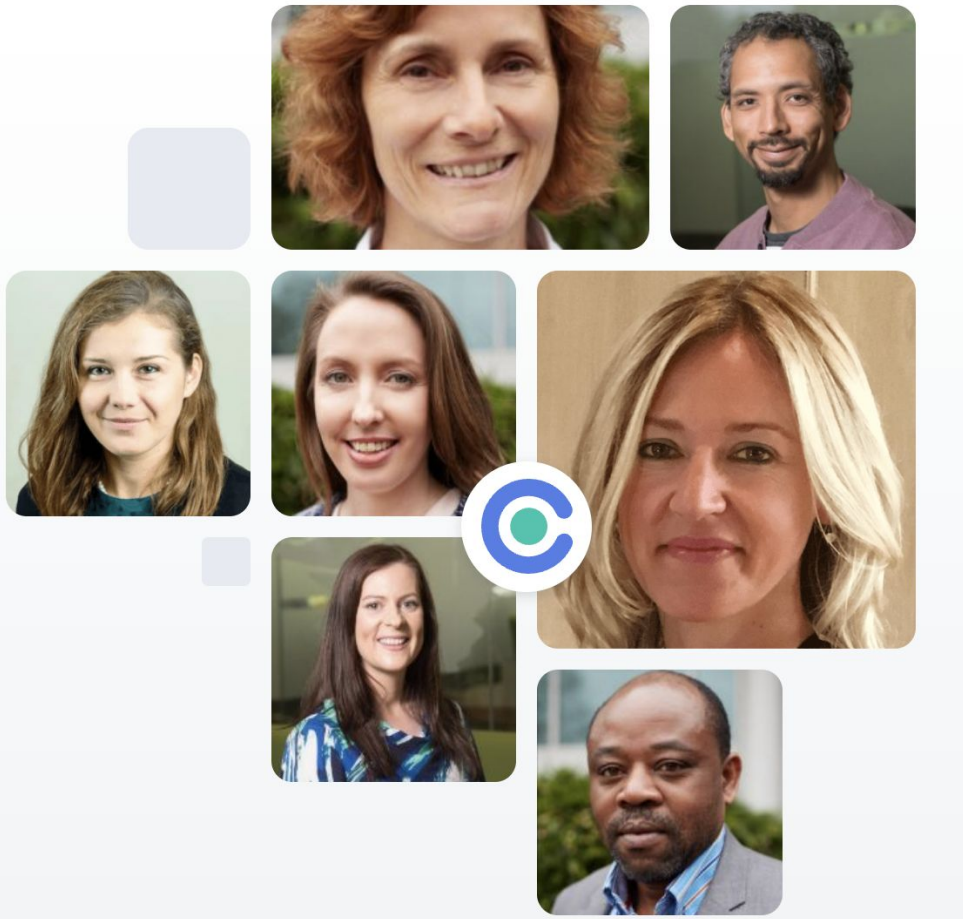
Power Tools & Garden Machinery

Leisure & Sporting Equipment

General & Online Retailers

Ask our Experts at the click of a button...

- 40+ Subject Matter Experts
- Extensive Knowledge Partner network
- Expertise across products, geographies & policy areas
- Addressing questions on laws & regulations including purpose, applicability, requirements highlights & more.



Compliance & Risks

Questions?

Thank You!

Ashley Weeks
Senior Regulatory Compliance Consultant, RINA Tech UK Ltd

Therese Hogan
Product Manager, Compliance & Risks

Orlaith Morris
Content Marketing Manager, Compliance & Risks

Compliance & Risks

→ | complianceandrisks.com