LLOYD'S

DORA – Beyond January 2025

LLOYD'S

Beyond January 2025

LLOYD'S

Common Challenges for DORA

Governance Model

Aligning governance approaches across organisations

Enhancing resilience frameworks for international regulations

Coordinating with various EU regulatory bodies

Third Parties

Information provision from critical third parties

Recognising critical subcontractors

Revising contractual terms and conditions

Strategic

Sustaining organisational emphasis on DORA

Developing comprehensive ICT Risk Management frameworks that align with DORA

Incident Reporting

Setting guidelines for incident detection and reporting

Delivering timely notifications and updates

Deciphering regulatory requirements

CIFs

Enhancing the maturity of identifying and mapping Critical Important Functions

Intra-group agreements and internal operations

LLOYD'S

Third Party Risk

Challenges for Third Parties

Maturity

- Numerous third parties have either not established their DORA readiness or are still in the early stages
- ICT service partners frequently lack familiarity with financial service regulations and the required outcomes
- Dedicated DORA capabilities are either not established or depend on traditional Business Continuity/Disaster Recovery (BC/DR) functions.
- Strategies for collecting and understanding customers' Critical Important Functions have not been set
- Reviews of sub-contracting frameworks and terms have either not begun or will require an extended period to complete

Challenges for Firms

Contracts

- Defining terms for exit planning and termination
- Resistance to rights for audit and inspections
- Supplying data for Information Registers
- Third-party testing and supporting resilience exercises with companies

Sub-Outsourcing

- Establishing criteria for identifying and reporting critical sub-outsourcers
- Rights for approving or exiting sub-outsourcers
- Reporting and audit rights
- Support for testing critical functions

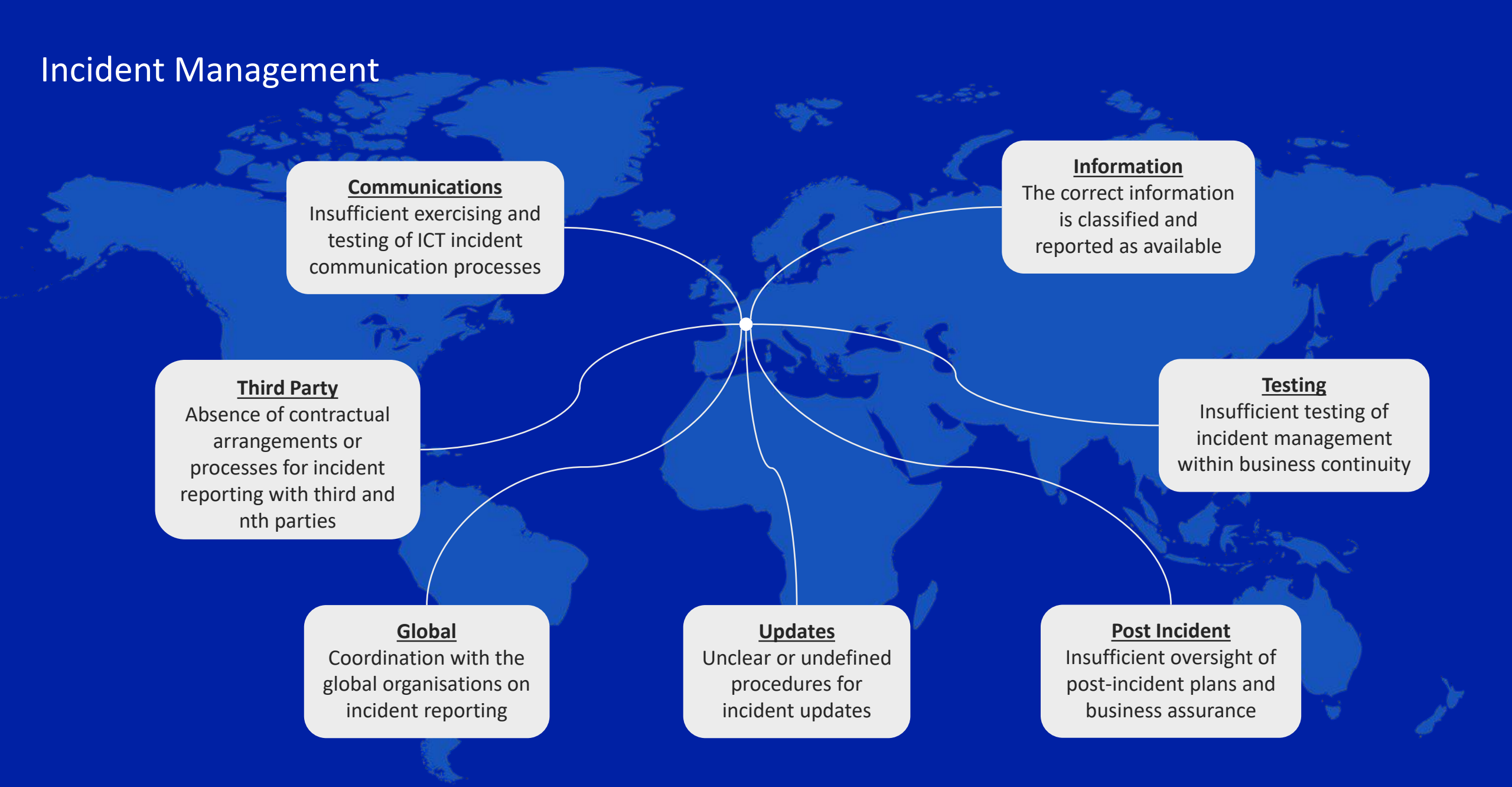
LLOYD'S

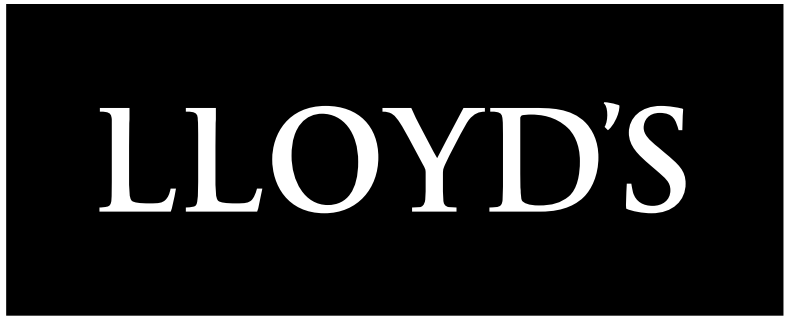
Register of Information

Creating a sustainable model for Registers of Information

Questions	What can we do?
Do we have access to the data needed and produced maps? Does the required data exist?	• Develop strategies for the organisation's Information Register • Design data maps and methodologies for the register • Conduct a gap analysis on data availability
Can we align the information across our registers to ensure consistency and accuracy?	• Define validation rules for data maps to detect discrepancies • Implement technologies for capturing and reporting data
Have we specified the appropriate level of detail for each of our registers?	• Evaluate the depth of data in relation to our Critical Important Functions • Refrain from establishing data requirements for information that we are unable to capture or utilise
What processes will we use to maintain and periodically review the information in our registers?	• Integrate oversight of the Register of Information into ongoing DORA Governance capabilities • Develop Key Performance Indicators for the Register of Information

Incident Management




LLOYD'S