Corporate
Governance
Institute

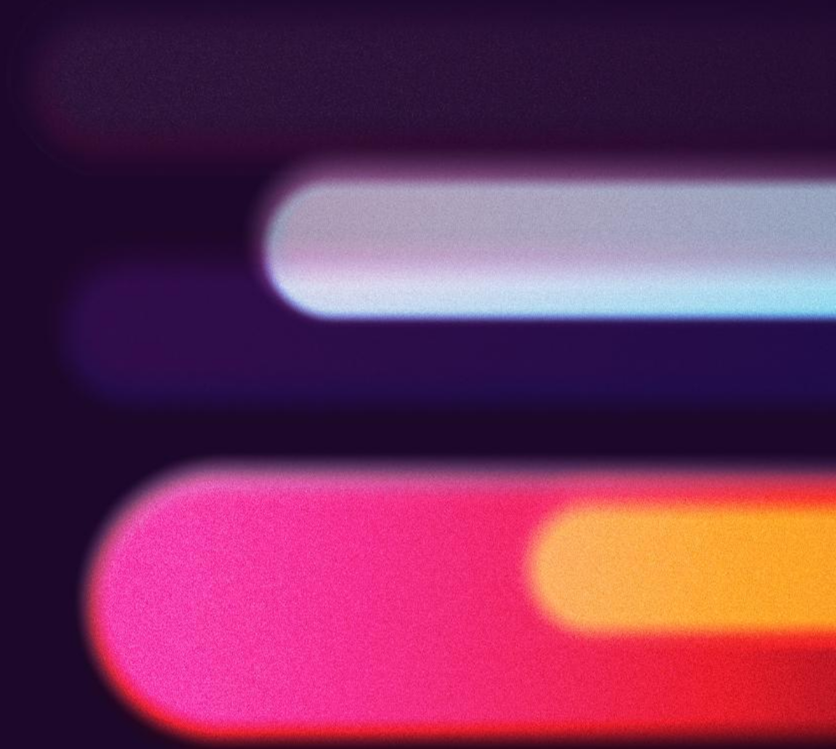
Cyber Resilience: Prepare to be Aware

Noelle Brisson

Co-Founder, CyberReady, LLC

Michael Savoie, Ph.D.

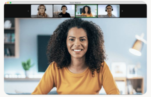
Co-Founder, CyberReady, LLC



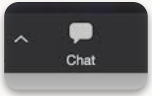
CGI Webinar

Corporate Governance Institute

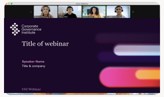
Before we get started



Today’s webinar is scheduled to last **1 hour** inclusive of Q&A.

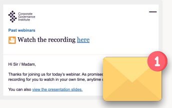


The slides will be shared and can be accessed in the **chat box**.



The presentation will last approximately **25 - 35 minutes**. So we will have plenty of time for your questions.

The webinar recording and slides will be available on **The Corporate Governance Institute website** tomorrow.



Corporate Governance Institute

Past webinars

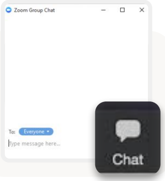
Watch the recording here

Hi Sir / Madam,

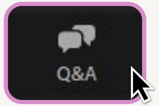
Thanks for joining us for today's webinar. As promise recording for you to watch in your own time, anytime

You can also view the presentation slides.

This webinar is being recorded and will be sent out in tomorrow’s newsletter. → Please note that the slides will not be sent out today and therefore **you should access them now**.



We have a global network of members and followers. Say hello and tell us your **name and where you are** tuning in from in the **chat box**.



Have a question?
Pop it into the Q&A box, so that we can dive straight into the questions when we get to our dedicated Q&A.

Corporate
Governance
Institute

Presentation Outline

1. What’s New in Compliance
2. Board Responsibilities in a Hyper-Connected World
3. Questions the Board should ask Regarding:
   a. Third-Parties
   b. Data Governance
   c. Business Continuity
4. Summary
5. Takeaways
6. Questions

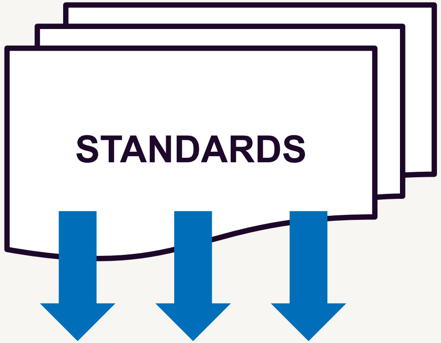
Inflation of laws, directives, and standards

- GLBA, SOX
- Sectorial laws (CFAA, HIPAA, FERPA…)
- SEC Rules
- State data privacy laws

Numerous European Directives

- GDPR
- DORA
- NIS1 → NIS 2
- AI Act

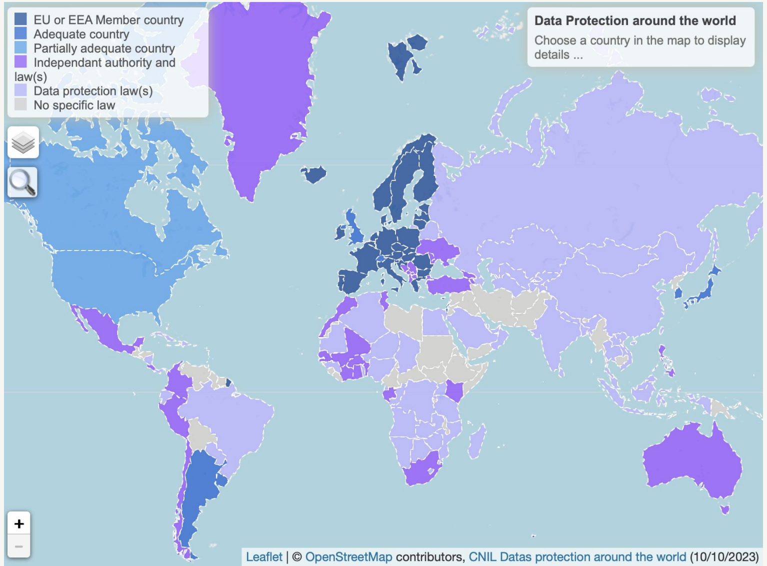
&



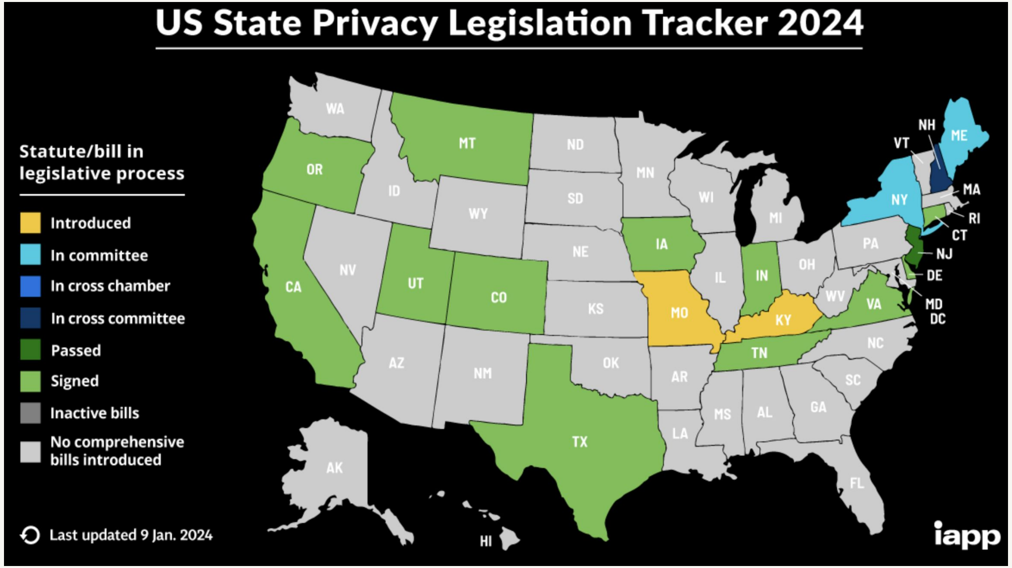
NIST COSO ISO

Data Security Laws

Gaining traction: an expanding patchwork


EU or EEA Member country
Adequate country
Partially adequate country
Independant authority and law(s)
Data protection law(s)
No specific law
Data Protection around the world
Choose a country in the map to display details ...
+
−

Leaflet | © OpenStreetMap contributors, CNIL Datas protection around the world (10/10/2023)



Last updated 9 Jan. 2024

What’s new with Compliance

- Speed of implementation
- Extraterritoriality: GDPR, AI Act, Patriot Act, Cloud Act or FISA (US) , PIPL (China)
- Risk Approach
- Measure of materiality
- Speed of reporting
- Heavy fines
- Accountability & cyber liability for c-suites and boards
- From compliance to business impact

➔ **Can not be a check-the-box exercise**

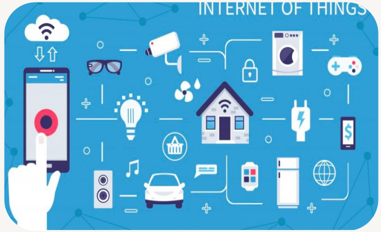
➔ **Also an opportunity**

Corporate
Governance
Institute

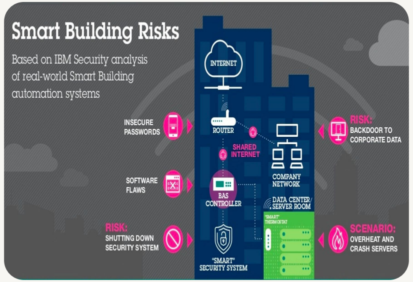
Board Responsibilities in a Hyper-Connected World

The Business World is becoming Hyperconnected

Remote Workers



IoT Devices


Smart Building Risks
Based on IBM Security analysis of real-world Smart Building automation systems
INTERNET
INSECURE PASSWORDS
ROUTER
SHARED INTERNET
SOFTWARE FLAWS
BAS CONTROLLER
COMPANY NETWORK
DATA CENTER/ SERVER ROOM
"SMART" THERMOSTAT
RISK: SHUTTING DOWN SECURITY SYSTEM
"SMART" SECURITY SYSTEM
RISK: BACKDOOR TO CORPORATE DATA
SCENARIO: OVERHEAT AND CRASH SERVERS

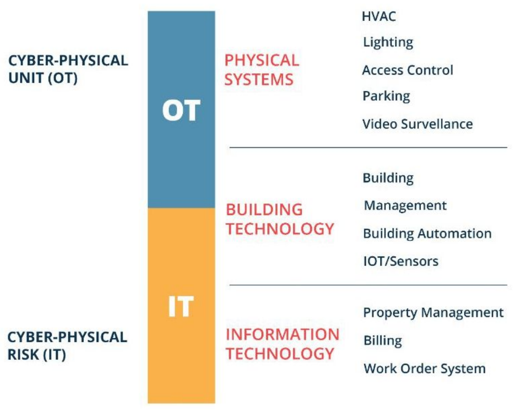


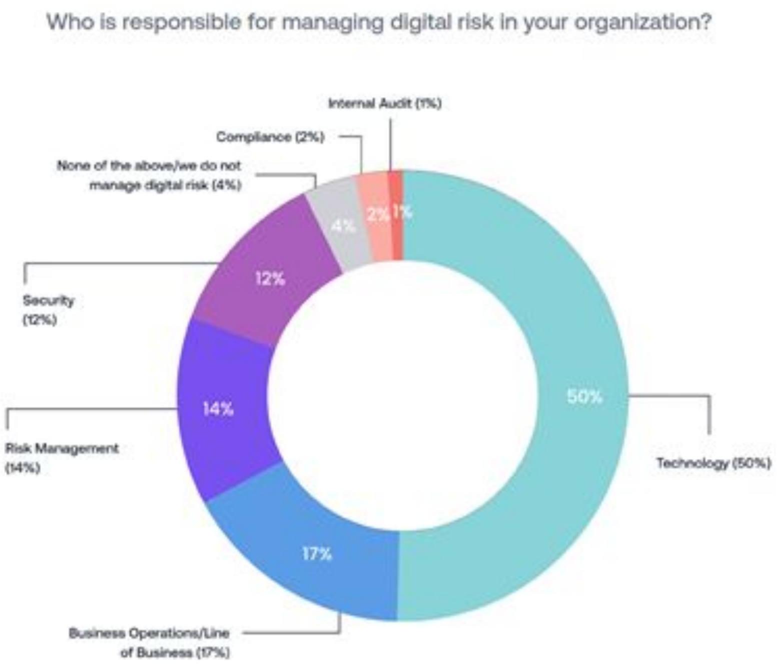
Figure: OT and IT convergence (Source: Building Cyber Security)

Smart Buildings – IT & OT

Corporate Governance Institute

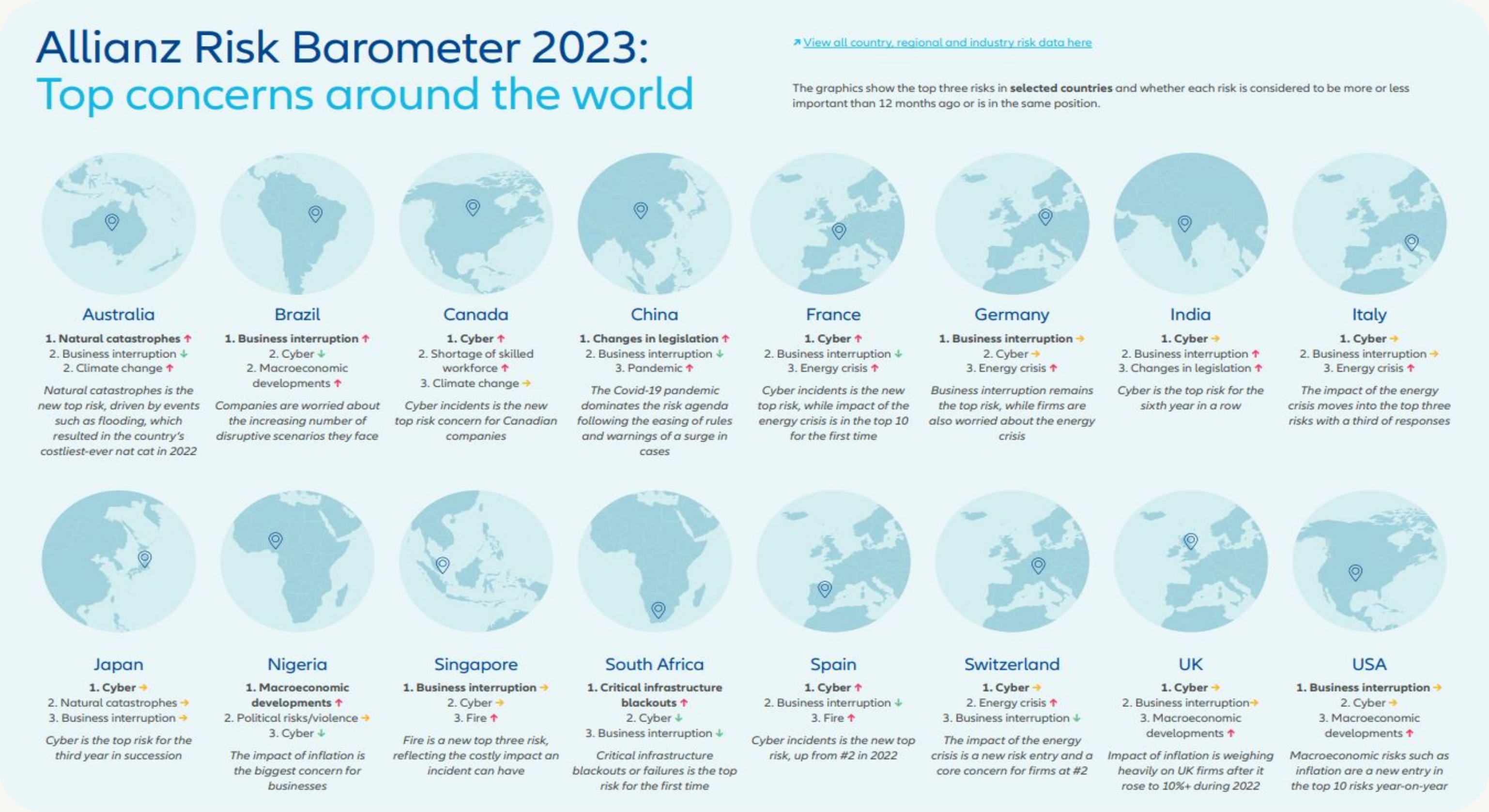
As Digital Risk Expands, There is Often a Fragmented Response

- As digital business grows, so does third-party ecosystems (e.g. vendors, suppliers, partners)
- Most organizations have invested in digital technologies without prioritizing the supply chain
- While digital risk is manifested across the organization (and supply chain) it is often treated as an IT Risk Management problem


Who is responsible for managing digital risk in your organization?

Corporate Governance Institute

Digital risk is top of mind globally



Allianz Risk Barometer 2023: Top concerns around the world

↗ View all country, regional and industry risk data here

The graphics show the top three risks in **selected countries** and whether each risk is considered to be more or less important than 12 months ago or is in the same position.

Australia

1. **Natural catastrophes ↑**
2. Business interruption ↓
2. Climate change ↑

Natural catastrophes is the new top risk, driven by events such as flooding, which resulted in the country's costliest-ever nat cat in 2022

Brazil

1. **Business interruption ↑**
2. Cyber ↓
2. Macroeconomic developments ↑

Companies are worried about the increasing number of disruptive scenarios they face

Canada

1. **Cyber ↑**
2. Shortage of skilled workforce ↑
3. Climate change →

Cyber incidents is the new top risk concern for Canadian companies

China

1. **Changes in legislation ↑**
2. Business interruption ↓
3. Pandemic ↑

The Covid-19 pandemic dominates the risk agenda following the easing of rules and warnings of a surge in cases

France

1. **Cyber ↑**
2. Business interruption ↓
3. Energy crisis ↑

Cyber incidents is the new top risk, while impact of the energy crisis is in the top 10 for the first time

Germany

1. **Business interruption →**
2. Cyber →
3. Energy crisis ↑

Business interruption remains the top risk, while firms are also worried about the energy crisis

India

1. **Cyber →**
2. Business interruption ↑
3. Changes in legislation ↑

Cyber is the top risk for the sixth year in a row

Italy

1. **Cyber →**
2. Business interruption →
3. Energy crisis ↑

The impact of the energy crisis moves into the top three risks with a third of responses

Japan

1. **Cyber →**
2. Natural catastrophes →
3. Business interruption →

Cyber is the top risk for the third year in succession

Nigeria

1. **Macroeconomic developments ↑**
2. Political risks/violence →
3. Cyber ↓

The impact of inflation is the biggest concern for businesses

Singapore

1. **Business interruption →**
2. Cyber →
3. Fire ↑

Fire is a new top three risk, reflecting the costly impact an incident can have

South Africa

1. **Critical infrastructure blackouts ↑**
2. Cyber ↓
3. Business interruption ↓

Critical infrastructure blackouts or failures is the top risk for the first time

Spain

1. **Cyber ↑**
2. Business interruption ↓
3. Fire ↑

Cyber incidents is the new top risk, up from #2 in 2022

Switzerland

1. **Cyber →**
2. Energy crisis ↑
3. Business interruption ↓

The impact of the energy crisis is a new risk entry and a core concern for firms at #2

UK

1. **Cyber →**
2. Business interruption→
3. Macroeconomic developments ↑

Impact of inflation is weighing heavily on UK firms after it rose to 10%+ during 2022

USA

1. **Business interruption →**
2. Cyber →
3. Macroeconomic developments ↑

Macroeconomic risks such as inflation are a new entry in the top 10 risks year-on-year

Corporate
Governance
Institute

A Holistic Approach to Cyber Risk

Holistic Risk Management

Comprehensive and Holistic Views of Risk

- Leaders gain a full view of how their organization’s risks have an impact on objectives, strategies, and business operations.
- Successful IRM programs take into account events that might take place outside of the identified risks, and in doing so contributes to a healthy analysis of the landscape and management’s position in all areas of their industry.
- In addition to integrating operational, enterprise, and cybersecurity risk management functions, a mature IRM program could also integrate ESG risk management and reporting into the umbrella, getting ahead of pending regulatory requirements.

1. Risk Appetite Awareness
2. Better Data
3. Project Prioritization
4. Finding Efficiencies
5. Cost Savings
6. Third Party Trust
7. Disaster Preparedness and Resilience

Corporate
Governance
Institute

Questions the Board should ask Regarding Third Parties

Physical:

- Are third parties vetted with background checks?
- Are there IP security and privacy requirements included in all 3rd party contracts?

Behavioral:

- Has the organization’s information security policy been actively communicated to all relevant external parties?
- Are privacy awareness training obligations extended to the organizations subcontractors or third parties?

Technical:

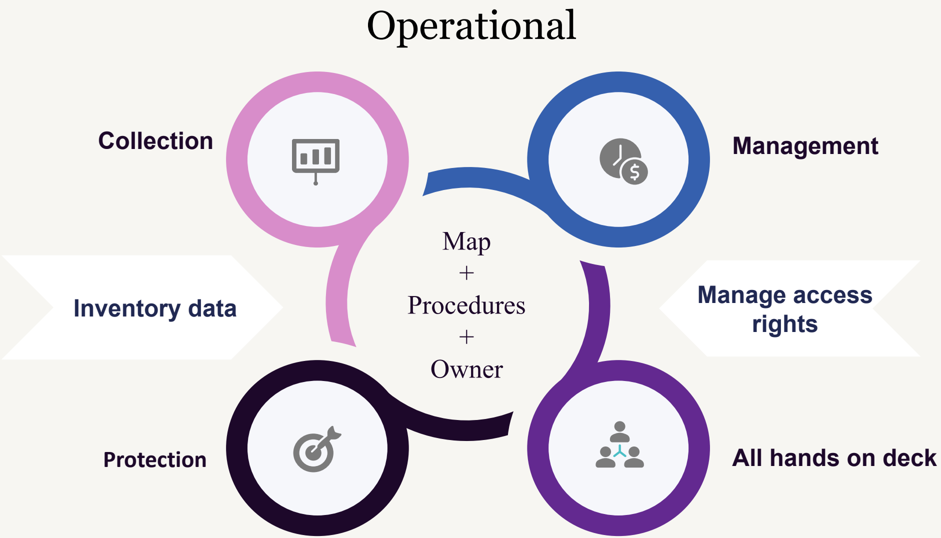
- Are there IP security and privacy requirements included in all 3rd party contracts?
- Is there a vendor risk management program addressing the security of data, that may be accessed, processed, communicated to, or managed by external parties?

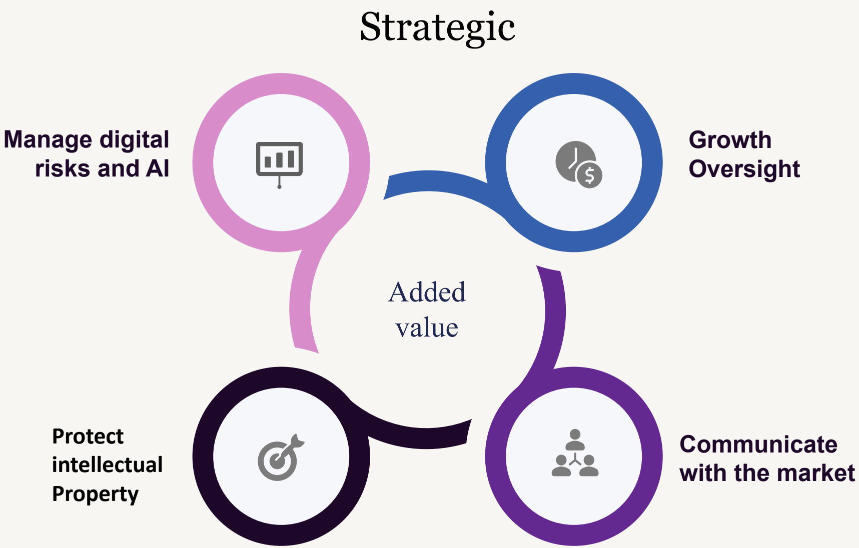
Corporate
Governance
Institute

Is the board aware of what third-party contractors do with data provided them by the organization?

Corporate Governance Institute

Questions the Board should ask Regarding Data Governance




Strategic
Manage digital risks and AI
Growth Oversight
Added value
Protect intellectual Property
Communicate with the market

The accuracy of your data is a major driver of risk mapping and resource allocation.

Corporate Governance Institute

Questions the Board should ask Regarding Data Governance

Physical:

- Are you aware of your organization’s backup policy/procedure?
- Have you met the facility manager and do you know what data is being collected?

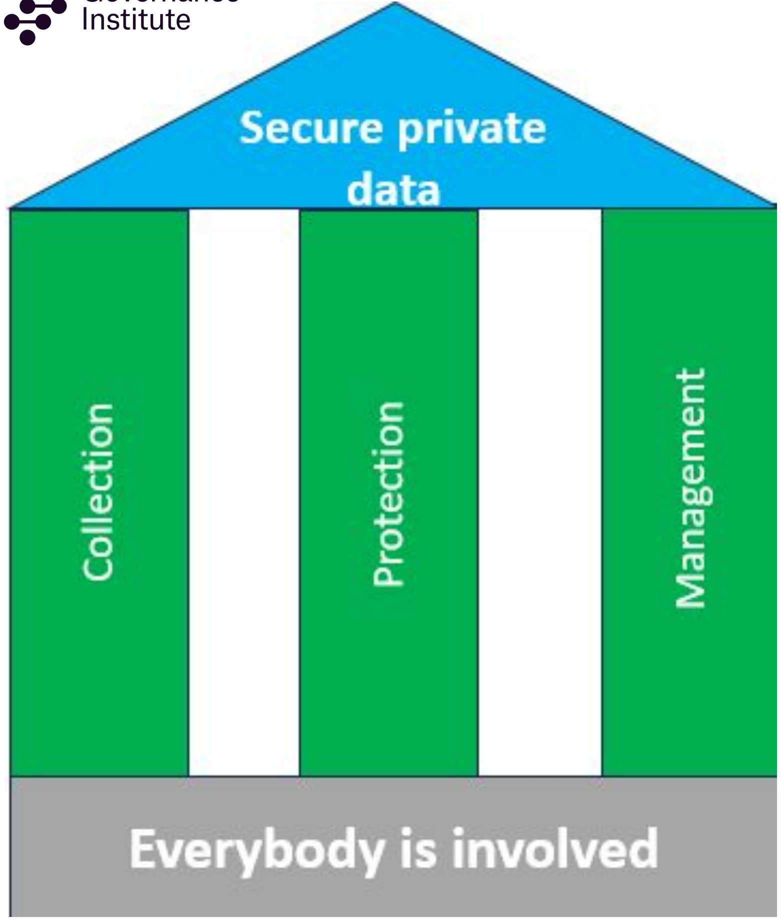
Behavioral:

- Do you know what training is provided to whom?
- Is there a Data Protection Officer (DPO)? And have you met them?

Technical:

- Is there a secure platform for board members to share information?
- How is AI being used in the organization?

Corporate
Governance
Institute



Strong Data Governance is a good place to start for business continuity and crisis management

Questions the Board should ask Regarding Business Continuity

- For most organizations, the question of a data breach is not if, but when.
- Regulators and insurance companies are compressing reporting requirements turnarounds.
- Thus, it is critical that organizations proactively plan for how they will respond to a data breach.

Questions the Board should ask Regarding Business Continuity

Physical:

- Is there an approved Business Continuity plan for the organization? Is it tested regularly and does the Board get an update on the results of the tests?
- Is there an approved Disaster Recovery Plan for the business? Is it tested regularly and does the Board get an update on the results of the tests?

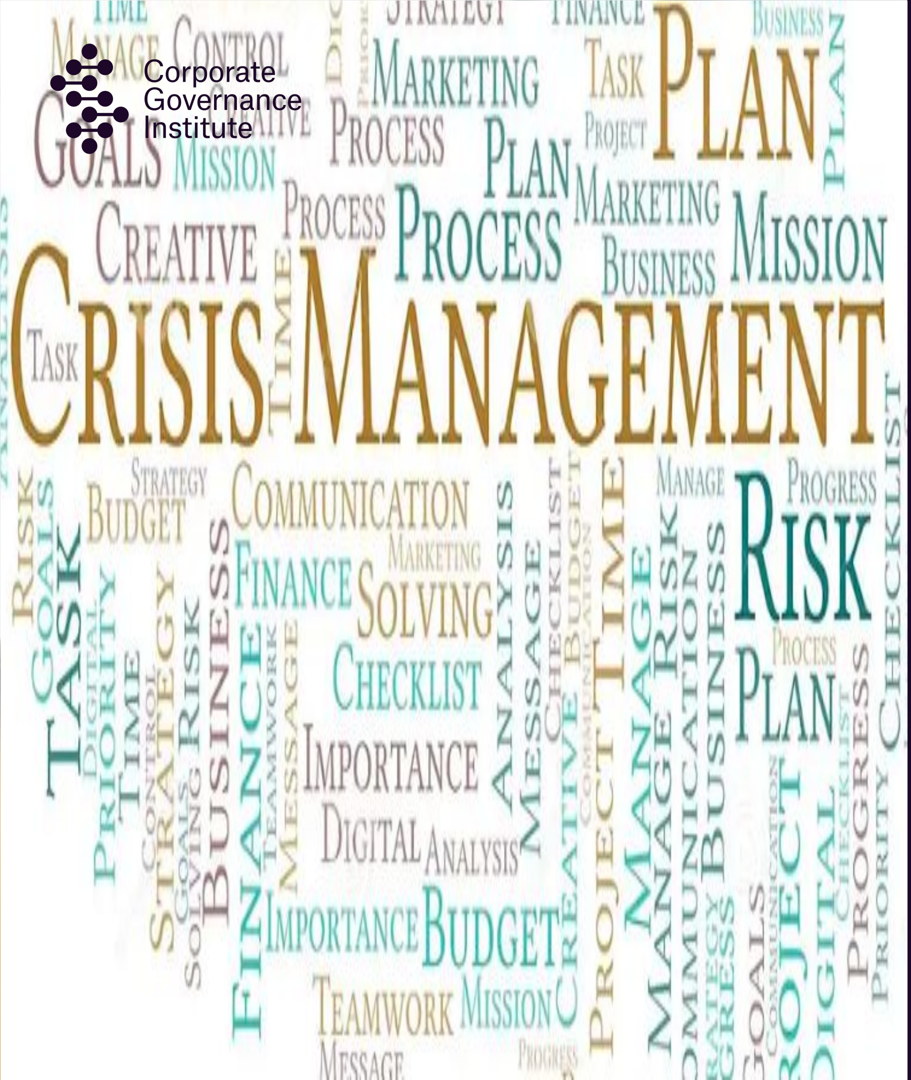
Behavioral:

- Is there a business-aligned Risk Governance Program that has been approved by management?
- Are cyber risks included in the Organization risk map?

Technical:

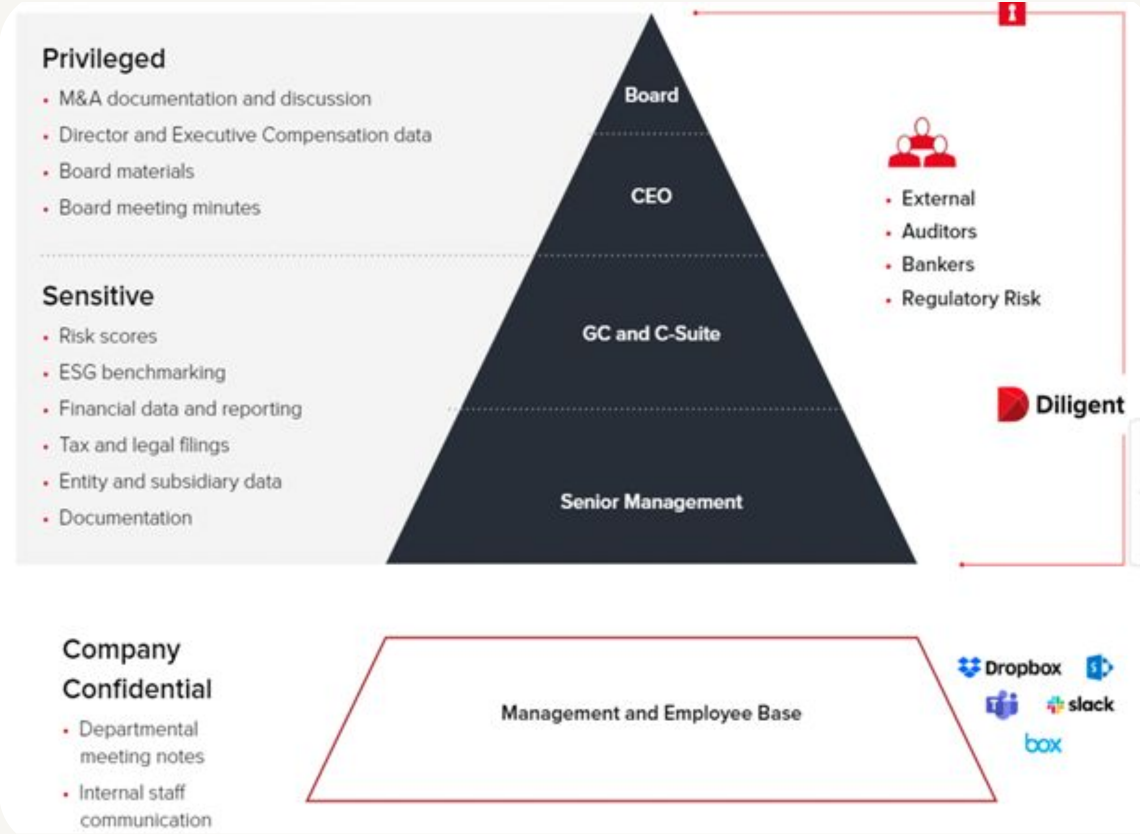
- Does the organization perform regular data backups?
- Is the Board made aware of the physical location of the cloud backup?

Corporate Governance Institute



Business Continuity and Disaster Recovery are complementary components of a robust Crisis Oversight Program

Heightened Sensitivity Requires Heightened Security



Privileged

- M&A documentation and discussion
- Director and Executive Compensation data
- Board materials
- Board meeting minutes

Sensitive

- Risk scores
- ESG benchmarking
- Financial data and reporting
- Tax and legal filings
- Entity and subsidiary data
- Documentation

Company Confidential

- Departmental meeting notes
- Internal staff communication

- External
- Auditors
- Bankers
- Regulatory Risk

Corporate
Governance
Institute

Take Aways

1 Cyber resilience is an enterprise risk but also an opportunity.

2 Track silos.

3 Mind the data: Your responsibility extends throughout the supply and value chain.

4 Be aware and be prepared. Know what to ask.

Corporate
Governance
Institute

Thank you

Noelleb@cyberready.net
michael@cyberready.net
www.cyberready.net

info@thecorporategovernanceinstitute.com
www.thecorporategovernanceinstitute.com

Questions?

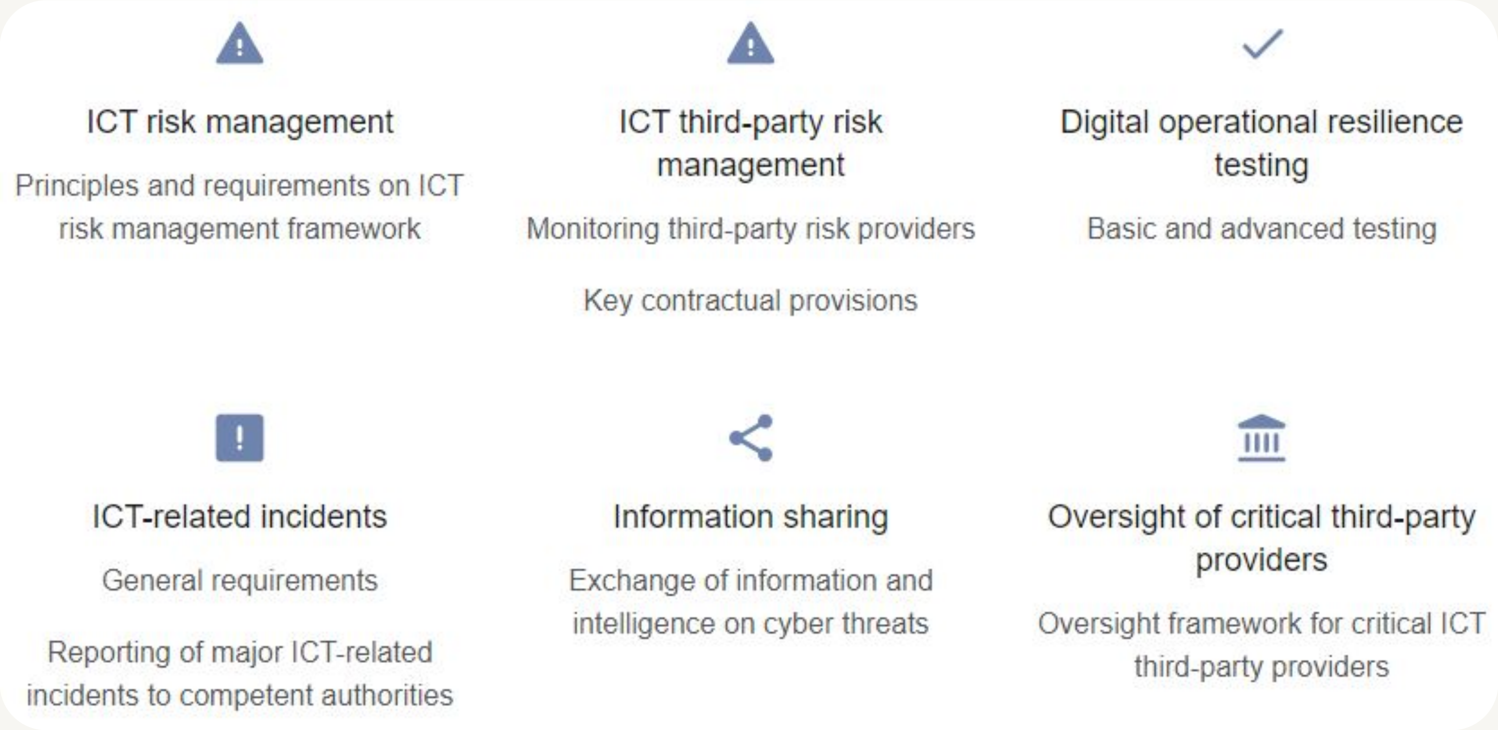
What is DORA?

DORA stands for The Digital Operational Resilience Act. It is an EU regulation that entered into force on 16 January 2023 and will apply as of 17 January 2025.

- **What is its purpose?**
  - The purpose of DORA is to strengthen the IT security of financial entities such as banks, insurance companies and investment firms and ensure that the financial sector in Europe is able to stay resilient in the event of a severe operational disruption.

- **Why is DORA needed?**
  - The financial sector is increasingly dependent on technology and on tech companies to deliver financial services, making them vulnerable to cyber-attacks. When not managed properly, these risks can lead to disruptions of financial services offered across borders. This in turn, can have an impact on other companies, sectors and even on the rest of the economy.

What does DORA Cover?



ICT risk management

Principles and requirements on ICT risk management framework

ICT third-party risk management

Monitoring third-party risk providers

Key contractual provisions

Digital operational resilience testing

Basic and advanced testing

ICT-related incidents

General requirements

Reporting of major ICT-related incidents to competent authorities

Information sharing

Exchange of information and intelligence on cyber threats

Oversight of critical third-party providers

Oversight framework for critical ICT third-party providers

Source: EIOPA - European Insurance and Occupational Pensions Authority, https://eiopa.europa.eu/

How to Prepare for DORA

1. Inquire about the data security vetting of all third parties,especially ICT partners
2. Require regular live, not just table top -, continuity plan exercises
3. Get debriefed on results
4. Require a presentation of the crisis response unit, and make sure there is an escalation process
5. Ask to see an incident reporting template

Corporate Governance Institute

Useful Readings

1 https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

2 https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214

3 https://www.iso.org/standard/27001;https://www.iso.org/standard/88412.html

4 https://www.aon.com/en/insights/articles/cyber-insurance-market-trends-and-outlook

5 https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

6 https://artificialintelligenceact.eu