VIGITRUST

Integrated Risk Management SaaS Provider

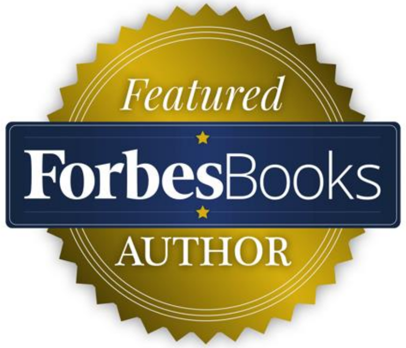
Should we focus on Risk rather than Compliance

Of Risk Apetite, Culture of Cyber accountability and Data Management

mathieu.gorge@vigitrust.com

https://ie.linkedin.com/in/mgorge

IRM Expertise



FINANCE MONTHLY GAME CHANGERS AWARDS 2019

CEO TODAY GLOBAL AWARDS 2019

AI acquisition international Cyber Security awards

VigiTrust - the Republic of Ireland

Best Information Security Compliance Management Platform 2020

The Cyber Elephant in the Boardroom

Published by ForbesBooks
November 24th 2020

Available on Amazon, Nook and Apple

Integrated Risk Management Portal - IRM

VIGIONE

Multi-Award Winning

Used in 120+ countries

- Map Policies & Procedures and Controls to Regulations and Standards
- Facilitate Information Gathering
- Generate up-to-date, customizable, automated Reporting & Analysis
- Maintain security & compliance levels
- Implement security and adapt to the evolving regulatory environment
- Upscale and adapt to your organization's needs

ASESSMENTS

eLEARNING

DOCUMENTATION

PROJECT MANAGEMENT

IP SCANNING

REPORTS

DASHBOARD

Global Risk Landscape

Strategic
Geopolitical

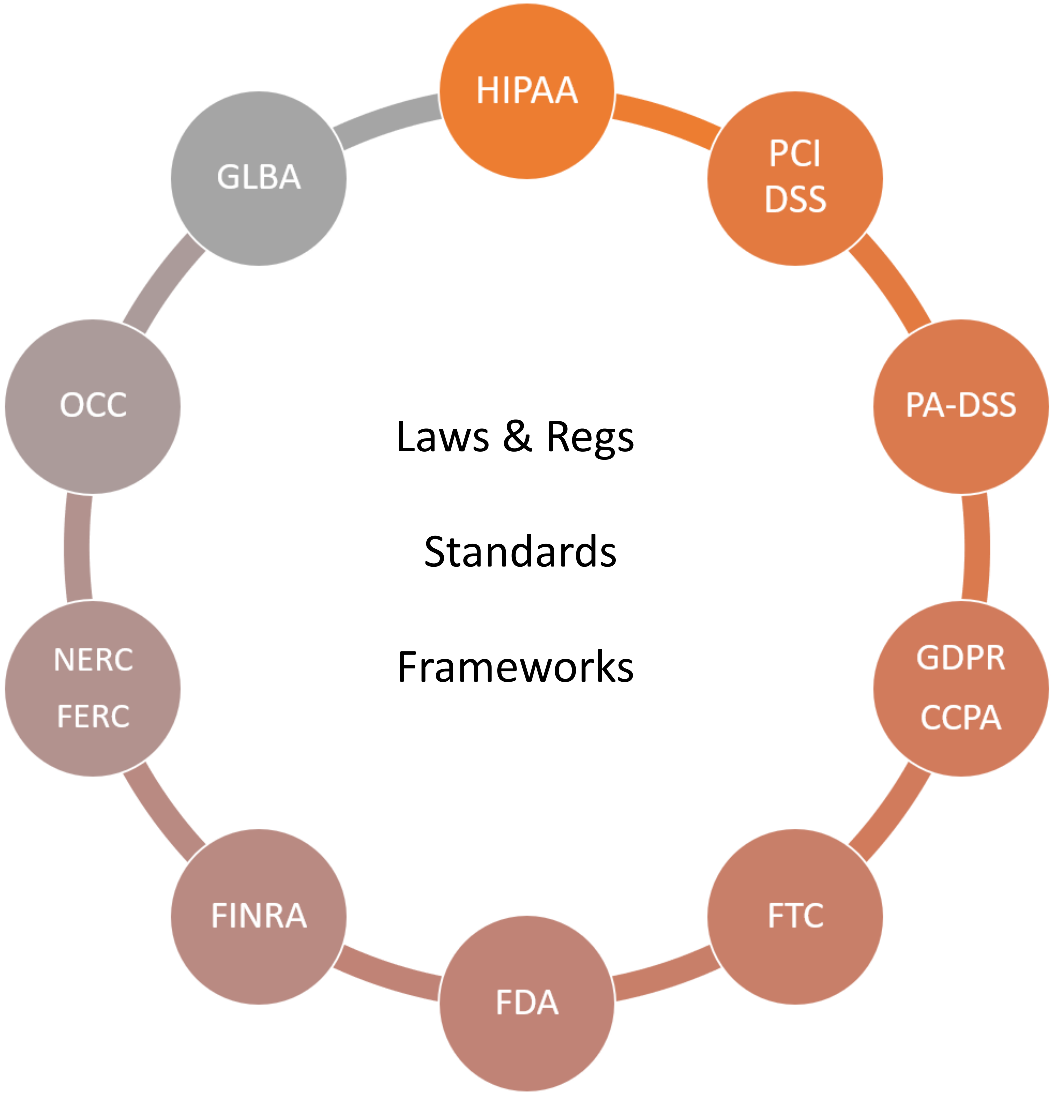
Cyber
IP / ICT
DR / BC

RISK AREA

Financial
Operational
Contractual

Reputational
Brand Management
Quality

Global Compliance Landscape



The irony of it all…PCI DSS

- PCI DSS v3.2.1 (2018)
  - “Risk” is found 208 times
  - “Risk assessment” is found 10 times
  - Not performing risk assessments on the CDE, vendors or payment apps is a non-conformity

PCI Security Standards Council

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel.

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, “personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are “resident” on the entity’s site or otherwise have access to the cardholder data environment.

PCI DSS Requirements	Testing Procedures	Guidance
12.1 Establish, publish, maintain, and disseminate a security policy.	**12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners).	A company's information security policy creates the roadmap for implementing security measures to protect its most valuable assets. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.
12.1.1 Review the security policy at least annually and update the policy when the environment changes.	**12.1.1** Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.	Security threats and protection methods evolve rapidly. Without updating the security policy to reflect relevant changes, new protection measures to fight against these threats are not addressed.
12.2 Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk. *Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.*	**12.2.a** Verify that an annual risk-assessment process is documented that: • Identifies critical assets, threats, and vulnerabilities • Results in a formal, documented analysis of risk **12.2.b** Review risk-assessment documentation to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment.	A risk assessment enables an organization to identify threats and associated vulnerabilities with the potential to negatively impact their business. Examples of different risk considerations include cybercrime, web attacks, and POS malware. Resources can then be effectively allocated to implement controls that reduce the likelihood and/or the potential impact of the threat being realized. Performing risk assessments at least annually and upon significant changes allows the organization to keep up to date with organizational changes and evolving threats, trends, and technologies.

The irony of it all…ISO 27001

ANNEX A.18:1 COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS.

This control has the main objective to oblige the legal and regulatory requirements as per the business needs. A combined group of procedural, information, personnel, information communications technology, and physical security measures identifies the information assets against a range of security threats. Any organization looking to achieve ISO 27001:2013 Certification must get familiarize themselves with the statutory and regulatory legislation.

ANNEX. A:18.1.1 IDENTIFICATION OF APPLICABLE LEGISLATION & CONTRACTUAL REQUIREMENTS

To avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security and of any security requirements.

ANNEX. A:18.1.4 PRIVACY & PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION

Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable.

Cyber Accountability – PCI DSS Viewpoint

Table 1. Common PCI DSS Roles and Responsibilities

Roles and Teams	Examples of PCI DSS Responsibilities
Executive Sponsors, Leader, Owner	• Authority to provide direction and budget. • Accountable for the risk and/or delivery of PCI DSS compliance.
Compliance Managers	Manages ongoing compliance efforts and the completion of PCI DSS validation documents such as Attestations of Compliance and Self-Assessment.
Information Security Team	Responsible for the security controls applied across the business. This includes overall accountability for: • Information security • Policy • Acceptable-use guidelines • Awareness • Incident response
Business Unit Managers	• Ensures business unit payment card controls are enforced. • Assists in removing payment card information from processes. • Helps make processes compliant.
Audit, Risk Management Team	Guides risk assessment and governance responsibilities.
Information Technology Team	The staff or outsourced third party providing and operating the organization's computer network(s). IT Administrator/s are vital to identify due to their span of responsibility.
Third-Party Service Providers	Outsourced processes, technology, staffing, or purchased PCI DSS solutions.
All Staff (Organization)	Understanding of their responsibilities to protect cardholder data.
QSAs/ISAs	Subject-matter experts in PCI DSS compliance.

Accountability
Compliance/Governance

Cyber Accountability – GDPR

Accountability obligation

Accountability is a common principle for organisations across many disciplines; the principle embodies that organisations live up to expectations for instance in the delivery of their products and their behaviour towards those they interact with. The General Data Protection Regulation (GDPR) integrates accountability as a principle which requires that organisations put in place appropriate technical and organisational measures and be able to demonstrate what they did and its effectiveness when requested.

Organisations, and not data protection authorities, must demonstrate that they are compliant with the law. Such measures include:

- Adequate documentation on what personal data is processed;
- How, to what purpose, and how long data will be processed for;
- Documented processes and procedures aiming at tackling data protection issues at an early state when building information systems or responding to a data breach; and
- The presence of a Data Protection Officer (if required) who is integrated in the organisation planning and operations etc.

Make an inventory of all personal data you hold and examine it under the following headings:

- Why are you holding it?
- How did you obtain it?
- Why was it originally gathered?
- How long will you retain it?
- How secure is it, both in terms of encryption and accessibility?
- Do you ever share it with third parties and on what basis might you do so?

This is the first step towards compliance with the GDPR's accountability principle, which requires organisations to demonstrate (and, in most cases, document) the ways in which they comply with data protection principles when transacting business. The inventory will also enable organisations to amend incorrect data or track third-party disclosures in the future, which is something that they may be required to do.

You should also reference our guidance on Data Protection Officers, Data Protection Impact Assessments and the Risk-based Approach to processing activities to see whether any of the criteria laid down there are of relevance to your processing activities.

Source:

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Predictions

- More of the same, read my 2020 Predictions ☺
- Phishing attacks will keep rising
- More ransomware attacks
- More sophisticated CEO – C-Suite attacks
- Attacks will get personal
    - Social Media
    - Personal Home Infrastructure
- Attacks on Critical Infrastructure
    - Health Systems
    - Banking
    - Transportation systems
- Compliance audits will be more frequent
- More GDPR fines
- More CCPA type regs on the way in the US
- More GDPR type regs worldwide
- Brexit Issues related to Data Protection

- Other than that…nothing to worry about ☺

Journal of Cyber Policy

HOME ARTICLES NEWS RESOURCES GUEST POSTS ABOUT US

Home » Articles and Opinion » Featured » Predictions 2021: Privacy and Compliance

PREDICTIONS 2021: PRIVACY AND COMPLIANCE

January 4, 2021 Hugh Taylor Off Articles and Opinion, Featured,

What should we expect in the worlds of privacy and compliance in 2021? Industry experts weigh in:

More consumers will submit data subject to access requests (DSARs)

"Now that the California Consumer Protection Act (CCPA) is in place, we will likely see an increase in customers submitting data subject access requests (DSARs). However, numbers will vary tremendously from company to company. Generally speaking, individuals either don't know or don't care that they can ask for this information until something brings it to their attention. For example, the publicity surrounding a ransomware attack might make them think, 'I'm a customer of that company. I want to know what they've got on me!'" – Rick Hedeman, Sr. Director of Business Development at 1touch.io

More CCPA-type regulations

"The new US administration will continue the work done by the previous two administrations on privacy regulations and enforcement. This will start with ensuring higher security and transparency for anything related to voting but will be much wider. We can expect more CCPA-type regulations and stricter privacy regulations. What is still not clear is whether there will be an effort to bring a federal PII regulation to the US, such as GDPR in the EU. If so, any bill will most likely be met with initial pushback as it would mean that the stricter states may need to loosen mandates whilst less strict ones will need to increase PII controls and have a way to implement them." – Mathieu Gorge, CEO of VigiTrust and author of the new book *The Cyber-Elephant in the Boardroom*

READ OUR NEW REPORT:

Cybersecurity Ratings and Stock Performance

Search...

Search

TAGS

1 · AI in cybersecurity · automotive · cloud security · consumer cybersecurity · COVID-19 · cybercrime · elections · financial services cybersecurity

USA TODAY

ZOOM FILTERS Add a filter

SETTING iPhone photo tips

APPLE WATCH Tips to use

News Sports Entertainment Life Money Tech Travel Opinion

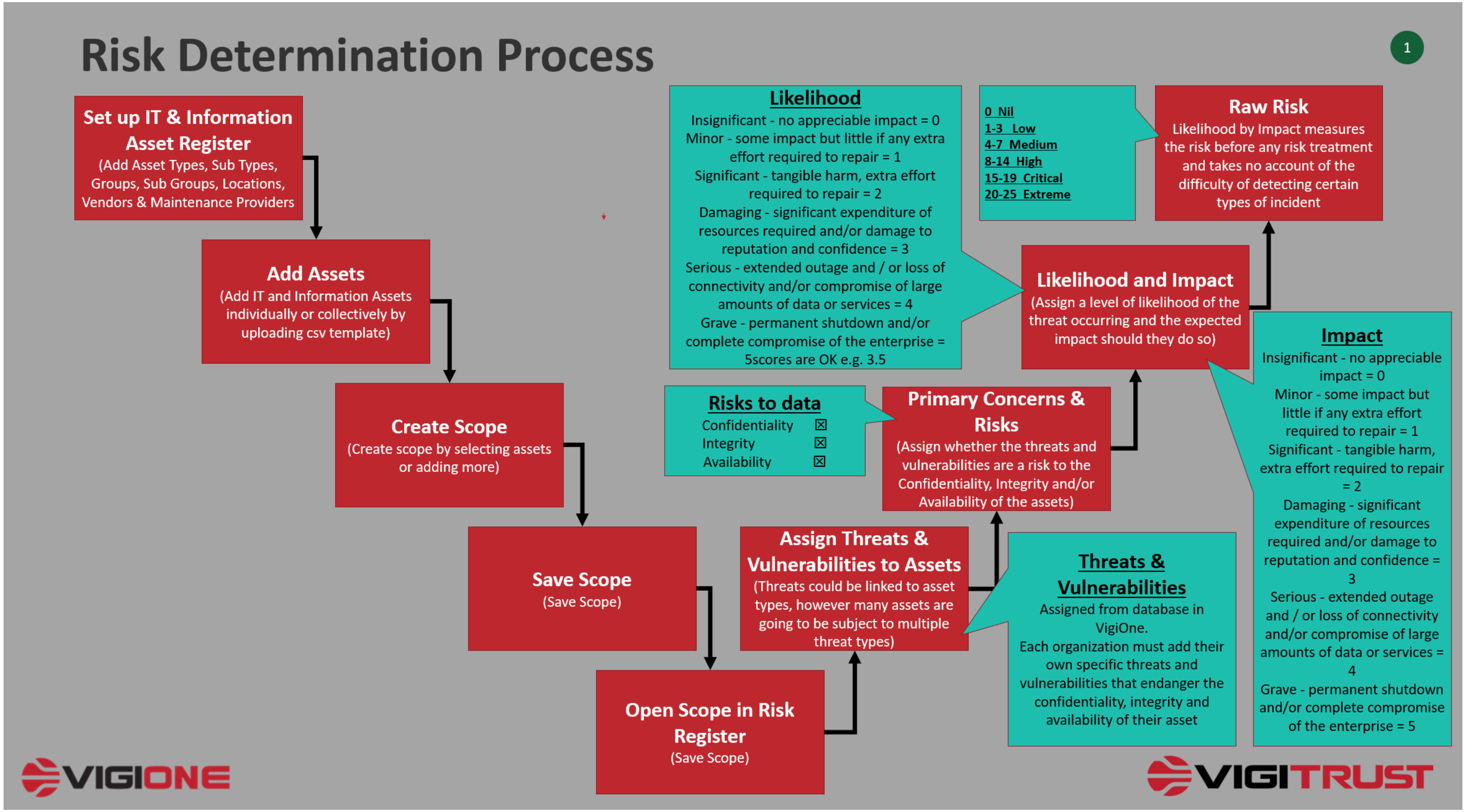
TECH

What you need to know about the FireEye hack: Cybersecurity attack against US government

Nathan Bomey and Kevin Johnson USA TODAY

Published 2:08 p.m. ET Dec. 14, 2020 | Updated 6:59 a.m. ET Dec. 18, 2020

How Risk Professionals talk about Risk



How do CEOs, CxOs, Boards talk about Cyber risk and cyber accoutability

Copyright 2005 by Randy Glasbergen. www.glasbergen.com

DENIAL

Cyber ? – It doesn't apply to me, ask my managers and lines of business !

ANGER

It isn't fair – we're trying to grow a business and create jobs here. Back off with your cyber nonsense !

BARGAINING

I'll do some of it – it'll be sort of compliance "a la carte" just to fend off regulators and governing bodies. That should do the job!

DEPRESSION

I'll never get there – it's not just laws & standards, but also documentation, technical investment, ongoing monitoring. I just can't!

ACCEPTANCE

It'll be okay! – it's not rocket science, we're doing a good bit already and we can now bridge the gap and stay ahead !

Data Security Technology as a Business Enabler

You can't protect what you're not aware of!
So what data do you have, where is it, how do you protect it?

- Asset Discovery and Asset Management Tools
- Data Discovery Tool
  - Generic date discovery tools
  - PII specific tool
    - Personal ID info
    - Banking info
    - Credit Card Holder Data
    - PHI – Personal Health Information
- Data Classification Tools
- Data Mapping
- Data Masking
- Tokenization
- Functional Separation

- Data Encryption
  - In Transit
  - At rest
  - In Use
- Data Back-up
- Data Recovery
- Data Erasure Technology

PHYSICAL SECURITY

- Access to building
- Physical Assets
- IT Hardware
- Vehicle Fleet

Operations Manager, Security Staff

PEOPLE SECURITY

- Permanent & Contract Staff
- Partners
- 3rd Part Employees
- Visitors
- Special Events Security

HR, Security Staff

DATA SECURITY

- Trade Secrets
- Employee Data
- Database
- Customer Data

HR, IT Team & Manager

INFRASTRUCTURE SECURITY

- Networks
- Remote Sites
- Remote Users
- Application Security
- Website
- Intranet

IT Team & Manager

CRISIS MANAGEMENT

- Documentation & Work Procedures
- Emergency Response Plans
- Business Continuity Plans
- Disaster Recovery Plans

Operation Manager, IT Team, HR

C-LEVEL & BOARD MEMBERS EDUCATION

- Face to Face Workshop
- eLearning

5 PILLARS OF SECURITY FRAMEWORK - ASSESSMENT

- Super Strategic
- Strategic

5 PILLARS OF SECURITY FRAMEWORK - SCORE

- Action Items
- Red Flags

OPERATIONAL SECURITY, RISK & COMPLIANCE PROGRAM

The Cyber Elephant in the Boardroom

GUEST CHAPTER CONTRIBUTORS

James Grundvig
Author and Tech Journalist
Breaching the C-Suite (CEOx, CxOs and Boards)

Nina Shulepina
Banking Compliance Professional
Member Of The VigiTrust Global Advisory Board
Protecting Data as the New Currency

Cathy Smith
Founder, Women in Tech NJ & NY
The Intersection of Cybersecurity and Business Digitization

Marco Antonio Soriano
Chief Investment Officer, Soriano Family Office
Handbook for C-Level and Board Members

Bob Gardner
Partner, New World Technology Partners
Managing the Cyber Risk Impact of Capital and Valuation

Nicolas Vigier
CxO Advisor – Cyberstrategy, Coalfire
Cyber Risk Impact on the Board

Ed Adams
CEO, Security Innovation
Software – Catalyst for Today's Digital Business

Marie-Christine Vittet
VP Compliance, Accor
To Comply with PCI DSS and keep Cardholder Data Secure

Cecile Martin
Partner, Ogletree Deakins International LLP
Cybersecurity Risk in Human Resources

Thibaud Lexerois
Attorney, Ogletree Deakins International LLP
Cybersecurity Risk in Human Resources

Alexander Abramov
Past President, ISACA New York Metropolitain Chapter
Education for Key Decision Makers

Integrated Risk Management SaaS Provider

Should we focus on Risk rather than Compliance

Of Risk Appetite, Culture of Cyber accountability and Data Management

mathieu.gorge@vigitrust.com

https://ie.linkedin.com/in/mgorge

VigiTrust - the Republic of Ireland

Best Information Security Compliance Management Platform 2020