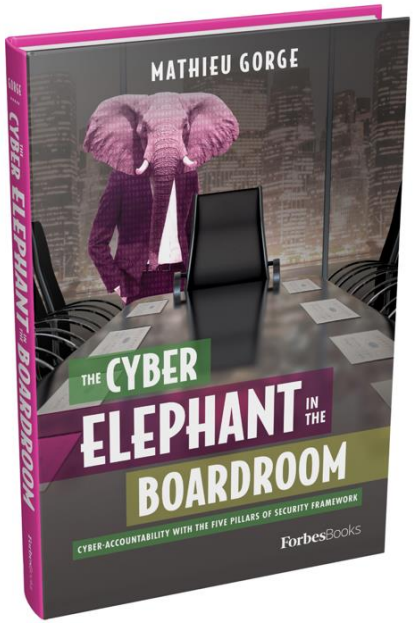


VIGITRUST

Integrated Risk Management SaaS Provider

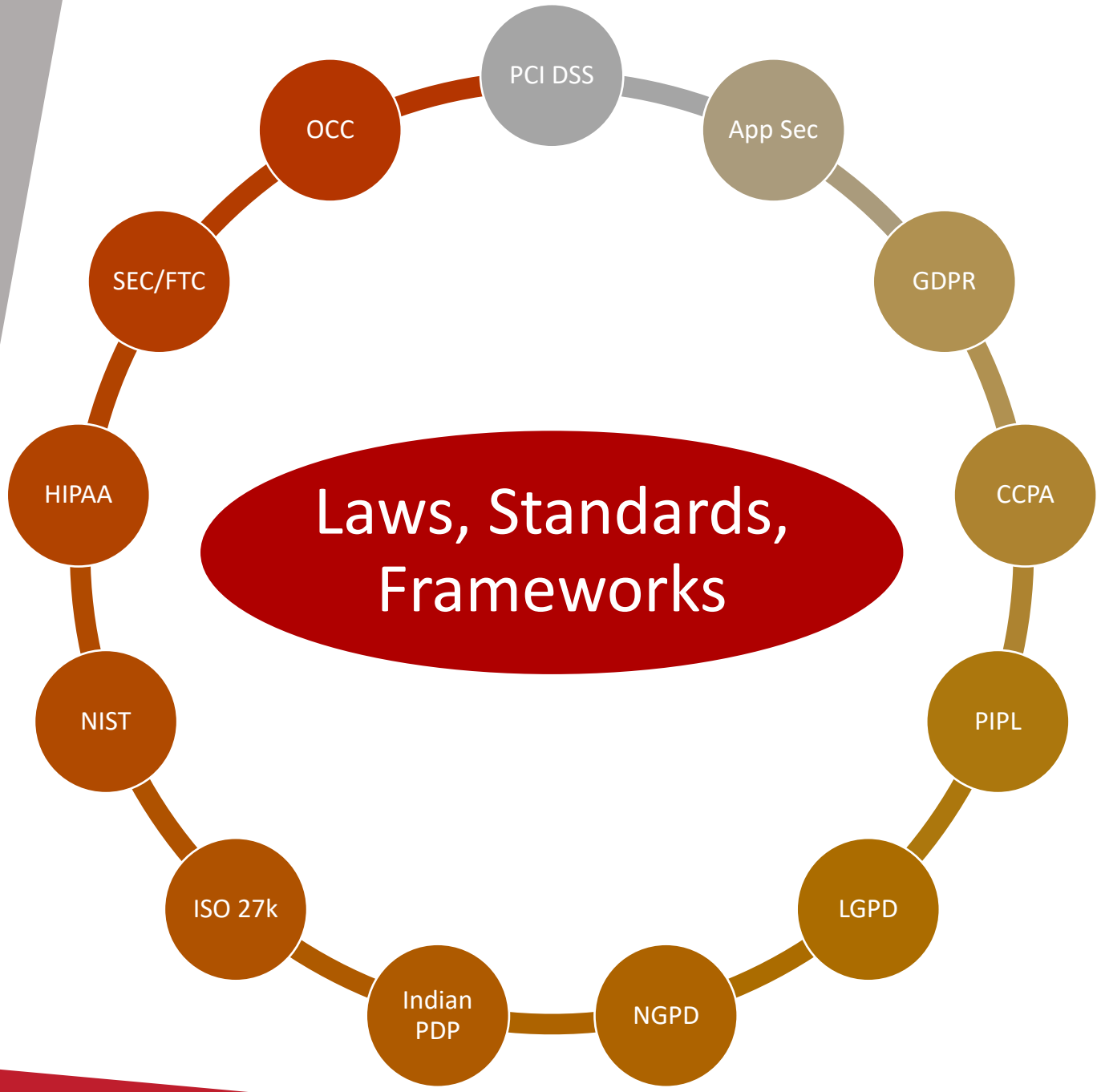
PCI DSS for Small Merchants

Of risk appetite, culture of cyber accountability and data management

mathieu.gorge@vigitrust.com

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

Global Risk Landscape



Global Compliance Landscape – 2022

A complex web of often conflicting requirements

Payments Industry – PCI History

Lifecycle of a Credit Card Transaction

Credit Card Transactions

Five Brands	Banks	Payment Service Providers	Merchants	Customers
MasterCard Worldwide DISCOVER FINANCIAL SERVICES AMERICAN EXPRESS VISA JCB	 	 	 	 

Payments Industry – a Definition

Payment security entails **managing** and **securing payment data** across an organization's full order **lifecycle**, from the point of **payment acceptance**, through **fraud management**, fulfilment, customer service, funding and **financial reconciliation**, and transaction **record storage**.

The presence of payment data at any of these points, whether on organization systems, networks or visible to staff, **exposes the organization to risk**.

The presence of payment data …. exposes the organization to risk.

Therefore you need to fully understand your own ecosystem and payments data flow

Challenges for Small Merchants

Small Merchants Attributes

a. 1 or few MiDs
b. 1 or few Acquirers/PSPs
c. Little knowledge of payment technology architecture & security
d. Not focused on compliance
e. Franchisees or subsidiaries

Small Merchants Security & Compliance Challenges

a. Little or no technical knowledge
b. Little or no IT staff – reliance on 3rd parties
c. Little knowledge of payment technology architecture & security
d. Not focused on compliance
e. No knowledge of PCI Compliance
f. Old Acquiring contracts
g. Consequences of hacks not understood

One cheeky question: can we really expect all small merchants to understand

1. Scoping
2. Securing payment data
3. Payment acceptance
4. Fraud management
5. Financial reconciliation
6. Payments storage records
7. P2PE

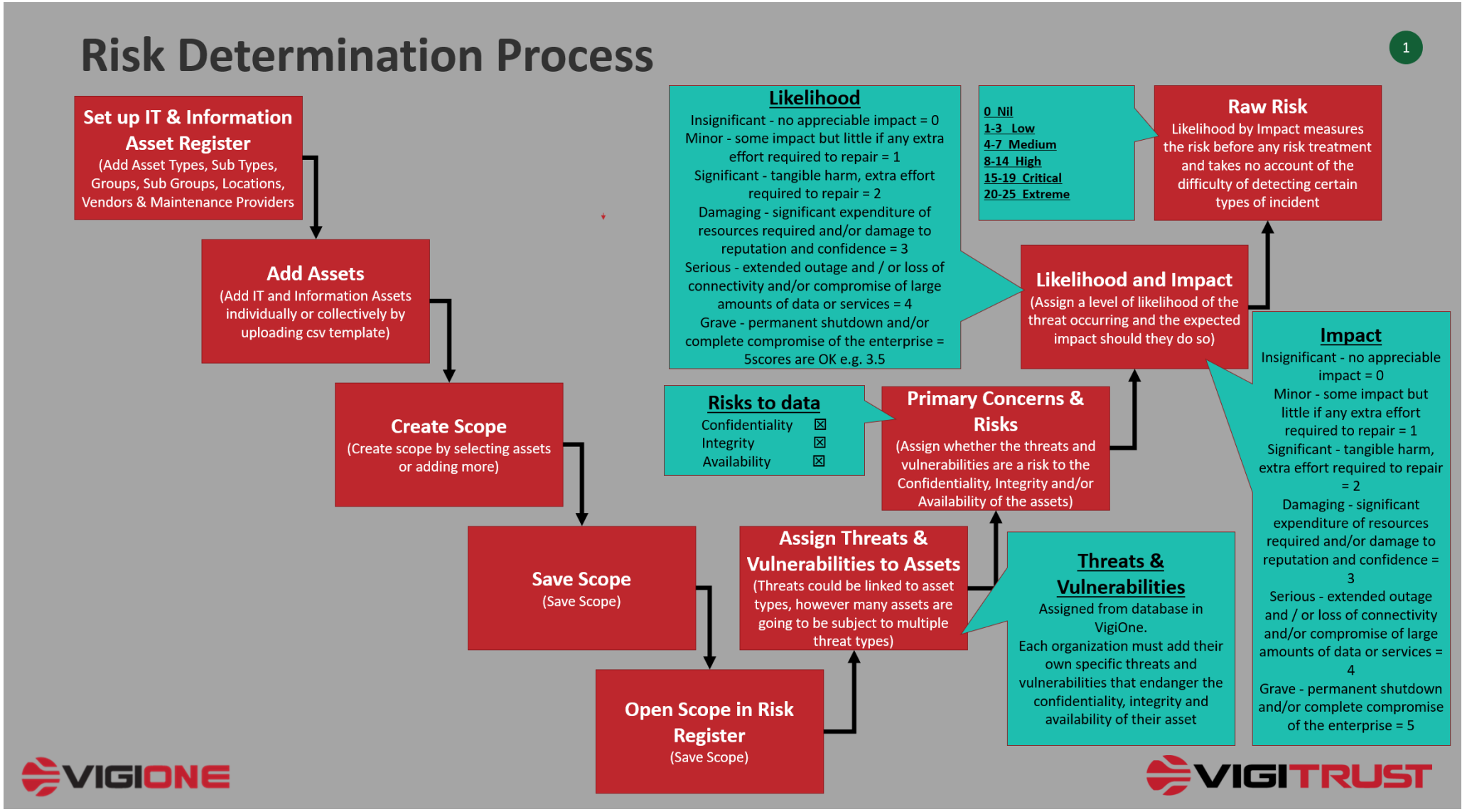
They need advice from payments security & compliance subject matter experts!

PCI SSC – Board & Small merchants

Small Merchants Voice?

a. Acquiring banks
b. Payments Council
c. Large enterprises with 100's or 1,000's of franchisees or subsidiaries

Tower of Babel - How Risk Professionals talk



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

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 !

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

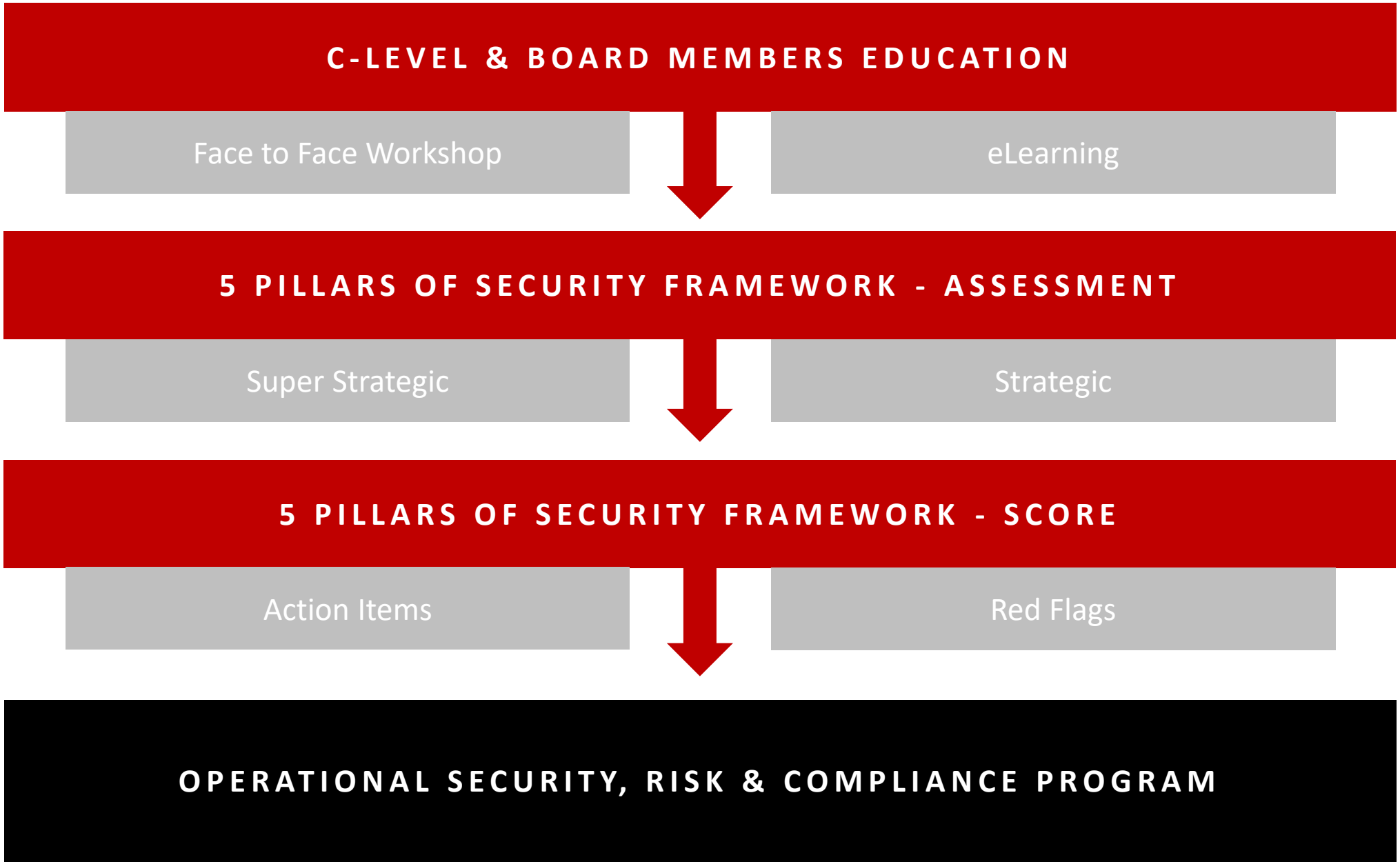
- Networks
- Remote Sites
- Remote Users
- Application Security
- Website
- Intranet

IT Team & Manager

CRISIS MANAGEMENT

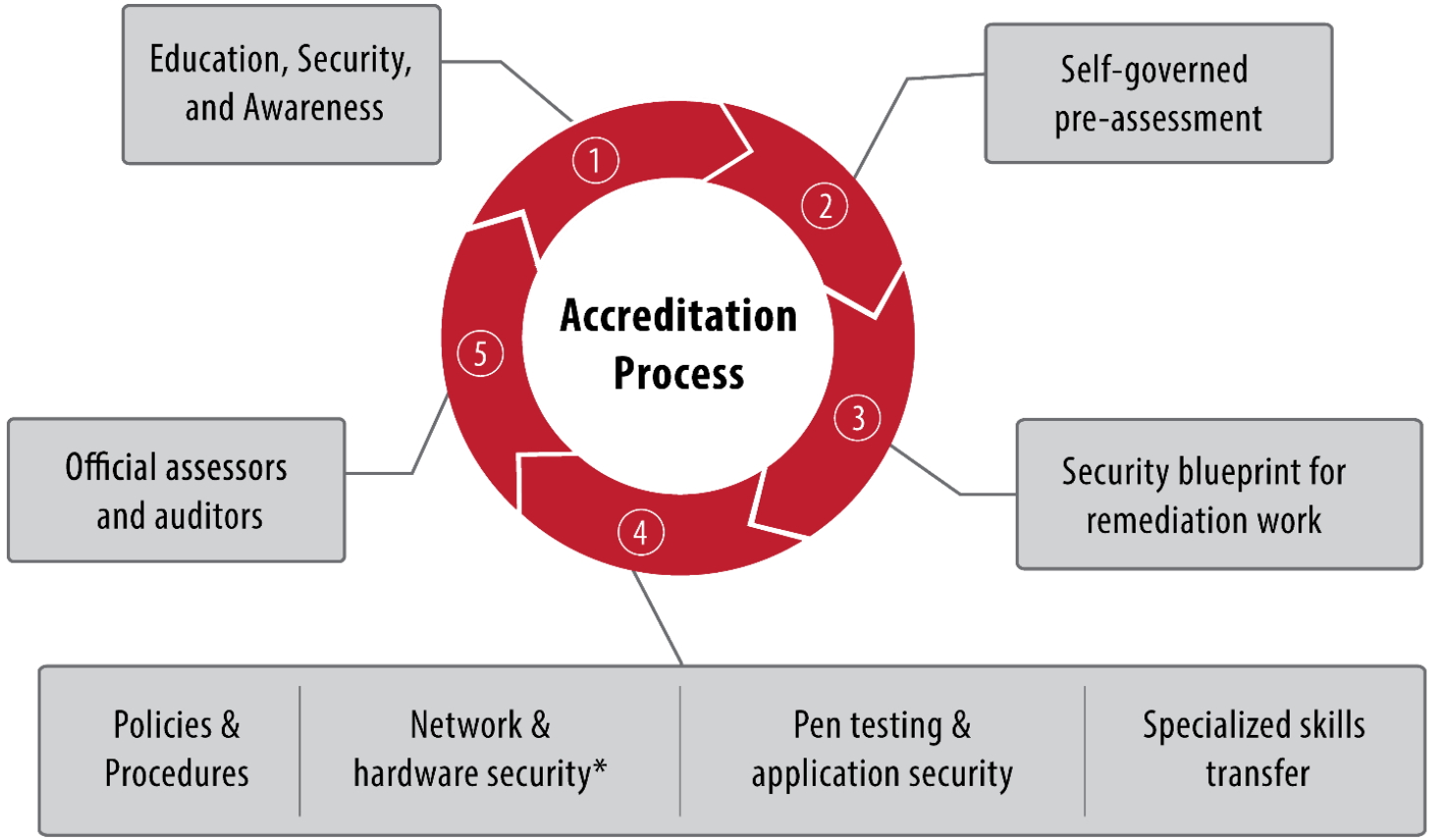
- Documentation & Work Procedures
- Emergency Response Plans
- Business Continuity Plans
- Disaster Recovery Plans

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

Some easy steps towards continuous compliance

- SOX
- ISO 27000 SERIES
- EU DATA PROTECTION
- PCI DSS
- HIPAA



*Delivered by our partners

CASE STUDY

PCI DSS Programs for Small Merchants: Making PCI DSS "Business As Usual" in large, multinational, distributed environments

THE MERCHANT

ACCOR

Accor is the largest hotel operator with a network of 5,000 hotels in 110 countries distributed through a hotel portfolio of 39 hospitality brands from luxury to economy.

Accor also has new businesses in private rental, co-working, concierge services, dining & events and digital solutions, with 300,000 employees whose commitment and passion is helping Accor reinvent hospitality.

For more information visit:
http://www.group.accor.com

THE SOLUTION

VIGITRUST

VigiTrust is an award-winning provider of SaaS Governance Risk Compliance (GRC) solutions with users in over 120 countries. VigiTrust enables large organizations, their subsidiaries, franchise operations and wider enterprise networks, to achieve and maintain compliance with legal and industry security frameworks including PCI DSS, GDPR and HIPAA. This is done through the provision of education, compliance validation and compliance management solutions.

For more information visit:
http://VigiTrust.com

How Accor and VigiTrust help thousands of hotels achieve and maintain compliance with PCI DSS

Let's hear from the merchant and the partner provider.

What PCI DSS program management challenges do you face?

Accor: Accor comprises more than 39 brands of hotels of all types and sizes in over 110 countries. The group includes owned and managed hotels and franchisees. At the Accor Group, compliance efforts are spread across different teams and business units including security/ compliance, country offices, local management and other lines of business. Coordinating these efforts is challenging, and central to this is the need to educate merchants, get them onboard with the PCI Data Security Standard (PCI DSS) and simplify their compliance efforts as much as possible.

What kind of PCI DSS compliance program was needed?

Accor: Facing the challenges Accor had with PCI DSS compliance on scale, we knew we needed a comprehensive multinational, multidimensional, and multicultural PCI DSS program to support our network of hotels. We needed a program that would have value-add to help our merchants achieve and maintain compliance. Secure payments throughout the merchant organization is the end game - for hotels this includes reception, restaurants, bars, gyms, spas, shops. It was also important for us to use the PCI DSS compliance program as a foundation for other compliance and risk assessment programs to maximize on successes achieved through the original program.

What does 'value-add' mean when it comes to a PCI DSS compliance program?

VigiTrust: The real value added for merchants is access to plain-English business-driven security advice so they can easily implement and maintain good security practices. This is done through VigiOne, an award winning Integrated Risk Management (IRM) SaaS solution. Providing education through eLearning and access to user friendly, procedures helps merchants understand why payment security is important and what's involved. Additionally, easy access to all PCI DSS SAQs, policies & procedures and training is provided on VigiOne.

Why did Accor choose VigiTrust?

Accor: Working with the right partner is essential to the success of our PCI DSS program.

The relationship with VigiTrust spans nearly a decade. We first met VigiTrust at their PCI European Roadshow in June 2011. They impressed us by highlighting the need to demystify PCI DSS for target audiences, prompting us to think about how we could customize a PCI DSS program for the hospitality industry. Their PCI Compliance program tailored for the hospitality industry, now available on VigiOne, has been evolving with ours over the years. We first engaged VigiTrust in 2012 for PCI DSS eLearning for 15,000 users. We further customized this for our hospitality needs over the years, leading up to a full, two-part customized program released in 2013 and incorporated PCI Risk assessment and Vendor Risk Management questionnaires into the platform.

From the outset, we found VigiTrust to be a flexible partner that could adapt to our needs and work with us to develop tailor-made PCI DSS training solution by Accor hotels.

PCI Security Standards Council

What makes a good future safe and scalable PCI DSS portal?

VigiTrust: A PCI DSS portal must make it straightforward for merchants to prepare for, validate and maintain their compliance levels. From an enterprise perspective, portals are mission critical tools allowing them to report not only on completion, but also on exceptions allowing PCI program managers to help merchants struggling to understand and implement good security required to achieve compliance. Additionally, portals must provide dynamic reports on compliance status across the whole portfolio as well as allow for the production of reports required by acquiring banks and card schemes.

What about continuous compliance and BAU?

Accor: Making PCI DSS compliance Business as usual is a must. From a compliance management perspective, organizations need access to real time PCI compliance status and have the ability to dynamically monitor their small merchant's portfolio compliance levels. Of course, regular static pre-defined reporting also helps but the real value is the ability to have access to compliance snapshots on demand. Accor uses a mix of pre-defined reports including an overall "Meteo/Weather" report as well as the ability to use VigiOne to zoom in on selected merchants as required and on demand.

What Key Performance Indicators (KPIs) have Accor implemented through VigiOne to monitor PCI DSS compliance across its portfolio of merchants?

Accor: Accor really wanted to promote objectives and KPIs related to PCI DSS compliance throughout the organization. This includes monitoring progress against PCI DSS program steps, identify top performers, follow new hotel onboarding, identify non-compliant properties, manage renewal dates.

What collaboration features do organizations need in a good PCI DSS portal to manage large portfolio of merchants?

VigiTrust: Accor really benefits from the fact VigiOne allows for the reproduction of the Accor worldwide organization (per hubs, brands, management type) such that the overall PCI DSS team can collaboratively help small merchants. VigiTrust for its part is also working with Accor on the platform to provide support whilst multiple QSAs working with Accor in various hubs are connected to VigiOne to do preparation work, assist with compliance work, document site visits to conduct gap analysis, manage evidence collection and remediation work and conduct full QSA Assessments

Can you explain the concept behind One Portal - Multiple Regulations and why it matters to small merchants & PCI DSS compliance?

VigiTrust: Small merchants need to comply with PCI DSS but they also need to comply with local and international data security mandates, for instance GDPR. Accor is building on the PCI program it built and extended its VigiOne implementation to cover GDPR, Risk Assessments and VRM (Vendor Risk Management). On their portal Accor and their QSAs have access to all merchants SAQs (multilingual), SAQ D Service Provider and ROCs. In terms of GDPR, users can do processing mapping, PIAs (Privacy Impact Assessments), Data Subject Access Request and Data Breach Response Plan. Additionally, Accor and VigiTrust released risk assessments & readiness questionnaires and GDPR and VRM readiness questionnaire on the same platform: one platform, multiple regulations.

PCI DSS - SECURITY POLICIES FOR HOTEL FRONT DESK / RECEPTION

ACCOR

Data Retention & Cleansing	• I only keep information required for the operation • I delete sensitive data as soon as I receive authorisation • I only store cardholder data in PCI compliant software or in a locked cabinet and shred it according to our Data Retention Policy
CVV (Credit Card Verification code)	• I do not store CVVs, either on paper or electronically • I never write down CVVs • I remove CVVs from e-mails using the Action => Edit option • I print Adobe Acrobat PDF files and make CVVs unreadable
SecurePAYbyLink	• I use SecurePAYbyLink for all TARS*-non-supported booking requests *(*TARS=The Accor Reservation System)* • I never ask for a copy/scan of a payment card to guarantee a reservation
Email & Fax	• I deal with fax right upon receipt and shred immediately • Alternatively, I lock faxes into the Reservations cabinet
ID & Passwords	• I do not share my ID and passwords for critical systems • I only use "strong" passwords • I never write down passwords on paper
USB Keys	• I never connect visitors USB keys to devices on the hotel network • Instead, I direct visitors to the Business Center/ WebCorner
Visitors Log	• I register visitors in the appropriate log at the Front Desk • I register myself in the appropriate log when accessing restricted areas such as Computer Room and Archive Room
EPT (Electronic Payment Terminal)	• I inspect my EPTs daily and keep them stored in a safe location • When working on night shift, I inspect all EPTs daily and record the audit into the Zero Pinpoint Inventory tool
IRP & SIR (Incident Response Plan & Security Incident Response)	• I am aware about my responsibility regarding cardholder data and about the importance of confidentiality • I know how to detect a system security incident and I immediately react on it
Shredder	• I destroy cardholder data using a shredder to make it unrecoverable when it is no longer needed for business or legal reasons
Security Policy	• I am aware about our company security policy and best practices and comply with them at all times
Security Awareness Training	• I validate my annual certification assessment annually
Merchant Tickets/ Receipts	• I store merchant tickets/receipts in a locked cabinet/ drawer

Payment Card Industry Security Standards Council, LLC
www.pcisecuritystandards.org

December 2020

PCI Security Standards Council

PCI Compliance – Tools + Advisors

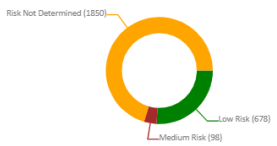
Regional Manager: Mathieu Gorge
Region: Access to all region
Country: France, Germany , United States, Australia , Belgium , Ivory Coast, Egypt, United Kingdom, Hungary , Netherlands, Korea(South)- Republic, Austria, Poland , Senegal, Switzerland, Indonesia, Qatar, French Polynesia, Ireland, United Arab Emirates, Portugal, Saudi Arabia, Cameroon, Spain, Greece, Canada, Italy, Chad, Luxembourg, Thailand, Mauritius, Russia, Algeria, Vietnam, China, Romania, New Zealand, Benin , Laos, Morocco, Lebanon , Nigeria, South Africa, Cambodia, Czech Republic, Mexico , Hong-Kong, Slovakia, Bahrain , Singapore, Lithuania, Togo, Monaco, Equatorial Guinea, Japan, Fiji, Kuwait, Turkey, Tunisia, India, Guatemala, Philippines, Jordan, Malaysia, Macao, Oman , Taiwan Republic of China, Madagascar, Ukraine, Armenia, Uruguay, Bulgaria, Kazakhstan, Myanmar, Panama, Georgia, Democratic Republic of Congo , Macedonia, Israel, Maldives, Angola, Ghana, Kenya, Azerbaidjan

Managers Comment: Edit
test comment

VIGITRUST

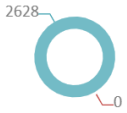
Vigione Dashboard 2022 February
Source May 2019

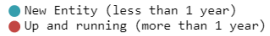
PCI Risk Assessment



User Certification

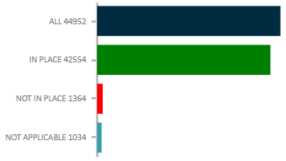
Entity Status



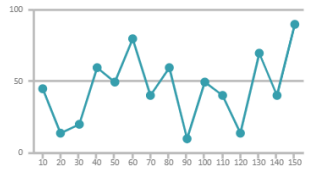


Best of the best: 197
Elearning done: 880
Policies and procedures done: 401
SAQ done: 2011

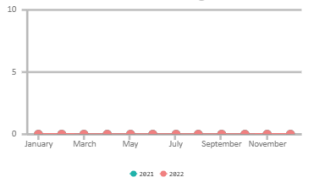
Policies & Procedures



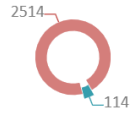
Line Chart

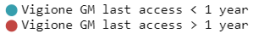


Users Training



Vigione GM Last Access

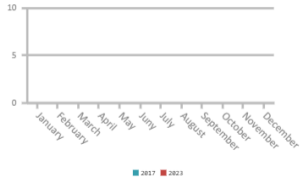




Certified Users

All users: 44389
Certified: 33259
Not certified: 11130

Entity Licence Renewal

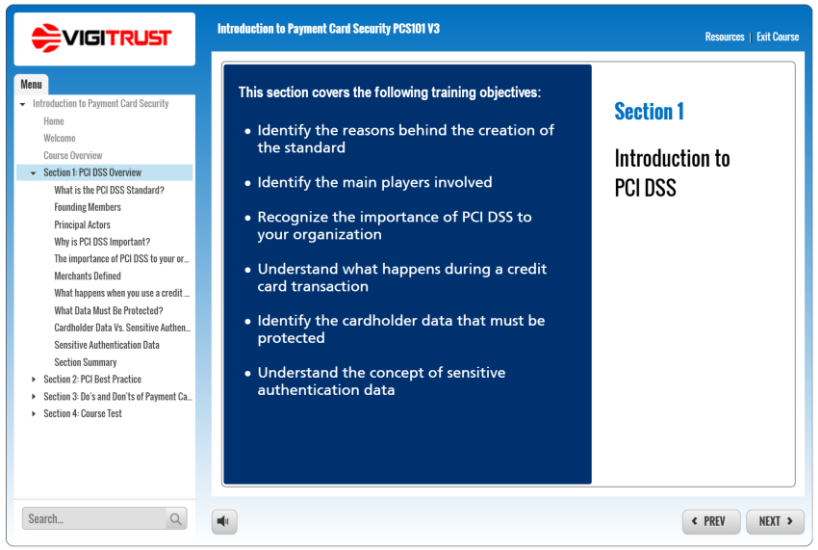


Policies and Procedures

In place: 42554
Not in place: 1364
Not applicable: 1034

Risk Assessment

High risk: 2
Medium Risk: 98
Low Risk: 678
To be determined: 1850



Empowering CEOs, CxOs, Boards and Senior Security & compliance Pros to talk about Cyber risk and cyber accountability in a collaborative and judgement free way!

Global Advisory Board - Topics

How are topics selected for GAB?

1. Suggested by GAB Chair & Global Leadership Team
2. Proposed by Chartered Advisors
3. Proposed by GAB speakers

Global Advisory Board - Membership

VIGITRUST
Global Advisory Board

Community Members

Official Community Membership Recognition
Invites to open events
Basic access to Global Advisory Board Material

VIGITRUST
Global Advisory Board

Chartered Advisors

Official Chartered Adisors Membership Recognition and Social Media Opportunities
Invites to all Global Advisory Board events
Full access to Global Advisory Board Material
Full Access to Chartered Advisors Portal:

- VigiTrust Research
- Other members research
- Other members details (opt-in only)

Speaking opportunities (keynote, panel)
Agenda & topics contribution
Global Membership Team opportunities

VIGITRUST

Integrated Risk Management SaaS Provider

PCI DSS for Small Merchants

Of risk appetite, culture of cyber accountability
and data management

We are looking for placement students, graduates and experienced security & compliance professionals ☺

mathieu.gorge@vigitrust.com

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

FINANCE MONTHLY GAME CHANGERS AWARDS 2019

Featured ForbesBooks AUTHOR

AI Cyber Security awards

VigiTrust - the Republic of Ireland
Best Information Security Compliance Management Platform 2020

LAWYER INTERNATIONAL LEGAL 100 2021 WINNER
MATHIEU GORGE
VIGITRUST
Best IT Security & Risk Management Business Leader - USA