Third Party Assurance

*ISACA & itSMF IT Governance Conference*
*Dublin, 11th October 2013*

[Mathieu.gorge@vigitrust.com](mailto:Mathieu.gorge@vigitrust.com)

[www.vigitrust.com](http://www.vigitrust.com)
Today’s Presentation

• Setting the Scene
• Why should anyone care about Third Party Assurance?
• Focus on legal & industry frameworks requiring third party assurance
• 2013-2015 Outlook
• Q&A
About VigiTrust

**About VigiTrust**

Compliance as a Service

The 5 Pillars of Security Framework™
Physical Security; People Security; Data Security; IT Security; Crisis Management

**1**
SECURITY TRAINING & eLEARNING
Online training for management and staff

**2**
COMPLIANCE, READINESS & VALIDATION
Comprehensive online programs to achieve and maintain compliance

**3**
SECURITY & GRC SERVICES
Professional services to enable and support your compliance process
# Existing eLearning Portfolio

## eSEC Portfolio US – Existing
- HIPAA
- NERC-CIP 101
- MA 201
- Understanding Data Breach Notification Requirements

## eSEC Portfolio EMEA – Existing
- Data Protection Fundamentals
- Credit Card Security
- Introduction to PCI DSS
- Banking & Fraud
- Green IT & Security
- ISO IT & SDLC
- Security During M&A Process

## eSEC Portfolio Generic Training - Existing
- Info Security 101
- Mobility & Security
- Security of Social Networks
- Cloud Computing & Security 101
- Physical Security for Good Logical Security

## eSEC Portfolio Technical Training - Existing
- Secure Coding for PCI DSS
- Introduction to Secure Printing
- Log Management & Security
- Wireless Security
Mathieu Gorge
CEO & Founder, VigiTrust

VigiTrust
Compliance as a Service

European PCI DSS Roadshow

EastWest Institute
Forging Collective Action for a Safer and Better World

ISSA Web Conferences

ENISA
European Network and Information Security Agency

ISACA

ISACA
Central UK Chapter

ISACA
New York Metropolitan Chapter

SearchSecurity.co.UK

ComputerWeekly.com

Baseline
Driving Business Success With Technology

American National Standards Institute
(Disclaimer: Outside Reviewer)
1st prize a pair of Barclays Premier League Football tickets

- 1st prize a pair of Barclays Premier League Football tickets
- 2nd prize a pair of ATP tickets (Association of Tennis Professionals)
- 3rd prize one of eight £50 Visa prepaid cards

See prize draw terms and conditions below. No purchase required.

Complete survey

If you have 10 minutes to spare, we’d love to hear about your experience of the Payment Card Industry Data Security Standard (PCI DSS).

With all the media attention on cybercrime and cybersecurity, protecting sensitive information is becoming increasingly crucial for everyone. For those who accept card payments, compliance to the PCI Data Security Standard is vital but the subject matter can be complicated and confusing to small organisations.

To address this challenge, Barclaycard and Visa Europe, in association with security experts VigiTrust, are launching a survey dedicated to small merchants and allowing them to voice their opinion on how PCI DSS impacts their business. Your responses to this survey will remain completely confidential, and all results will be aggregated.

The survey should take no longer than 10 minutes to complete. To thank you for your time, you will be entered into a draw for the chance to win one of the above prizes.
Definitions – Third Party Assurance in 2013 & Beyond

• Going Back to Basics
  – Third Parties
    • Suppliers (any type: IT, legal, finance, goods/services)
    • Partners
    • Internal suppliers or group partners
  – Assurance
    • Is the code secure?
    • Is the architecture secure?
    • Is the data that the app is transmitting, storing or processing at risk?
  – Two sides of the same coin
    • Your organization is another’s third party
    • Can you demonstrate your business does not put another one at risk – security/compliance
  – 2013
    • Most organizations outsource some IT
    • Some organizations are less “tangible” in that they use BPO
    • Advent of Cloud Computing
  – And beyond
    • Because threats evolve and the traditional business ecosystem keeps involving third parties
      – Some trusted
      – Some partially trusted
      – Some untrusted but necessary to do business

(c) VigiTrust 2003-2013
Definitions – Third Party Assurance from an Accounting Perspective

• Definitions & Key Terms
  – “The International Standard for Assurance Engagements No. 3402 (ISAE 3402), formerly SAS 70, is an attestation standard issued by the International Auditing and Assurance Standards Board (IAASB). Its aim is to produce a formal report on the design, implementation and operating effectiveness of controls within a service organisation”.
  – What is the ISAE 3402? ISAE:
    • “is a formal report on the design, implementation and effectiveness of controls within a service organisation, usually covering a period of six months or longer
    • is primarily used to support the financial audit process of entities that use external service organisations
    • contains an independent accountant’s opinion and management assertion on the design, implementation and effectiveness of controls within a service organisation for the audit period
    • contains a description of the service organisation’s control environment, its control objectives and the key controls put in place to achieve these objectives
    • contains tests of operating effectiveness performed by the independent accountant, and the results of those tests (type II)
    • contains control considerations that should be employed at entities that use the service organisation
    • is intended for use by the service organisation, its customers and the independent accountants of its customers”


(c) VigiTrust 2003-2013
Definitions – Third Party Assurance from non financial perspectives

- Business Process Outsourcing
- Supply chain risk management
- Contract compliance
- Cloud computing
- Digitization of Business Processes
- Privacy and security
- Regulatory compliance and reporting
- Asset & IP Risk Management
- Green IT

- Suppliers of Key 3\textsuperscript{rd} Party Applications?
- Application Security should be an integral part of 3\textsuperscript{rd} Party Assurance Strategy

• 98% of applications presented at least one application security risk, while the average application registered 22.4 risks
• Authentication and Session Management risks affect 93% of applications and comprise 34% of application vulnerabilities, by far the most prevalent application security risk
• Compared to automated tools, manual code review and penetration testing identify significantly more serious authentication, access control, and encryption risks
• Secure coding training and eLearning cause a significant improvement in prevalence and severity of the risks discovered in applications
• Application security risk profiles are remarkably similar across different industry sectors
• Yet, applications are rarely part of the 3rd Party Assurance process!

(c) VigiTrust 2003-2013
OWASP Top 10 - 2013
The Ten Most Critical Web Application Security Risks
Understanding Database Risks Cloud Risk for 3rd Party Assurance

- **Technology Risk – Stating the Obvious**
  - Virtual Servers
  - Database / Storage
  - The Internet

- **Infrastructure Risks**
  - Choosing a private cloud infrastructure means that network security is effectively under your control – Risk is “mitigated”
  - With a public cloud infrastructure, the operational responsibility for security rests with the provider, legal responsibility is with you
  - Implication: you plan to process, transmit or store sensitive data, you need to clearly understand your service providers stance on the following:
    - Transparency
    - Privacy
    - Compliance
    - Trans-border information flow

(c) VigiTrust 2003-2013
Understanding Transparency

- Cloud Providers must be capable of demonstrating the existence of effective and robust security controls, assuring that customer data is properly secured against unauthorized access, change and destruction.

- The key questions that should be asked when choosing a service provider include:

  - How will my data be protected?
  - Which (provider) employees will have access to customer information?
  - How is customer information segregated?
  - What controls are in place to detect and prevent security breaches?
    - Technical Controls
    - Policies & Procedures
    - User Awareness
  - Is the Cloud Provider helping or hindering with PII/DPA & industry compliance (e.g. PCI DSS)
Cloud Storage Considerations

- **Storage as a Service = Storage in the Cloud**
  - Your organizations data is stored in the Cloud whether you are aware of it or not

- **Data Classification is key for Cloud, understanding your risk surface & performing assurance audits**
  - Do you have a data classification policy stating what can make it to the Cloud and what cannot?
  - Are you encrypting data the right way – remember PCI DSS
    - If you don’t need it don’t store it
    - If you need it – encrypt it according to Requirement 3.4 – good benchmark for storage technical security
    - Consider tokenizing more than payment data
  - Ensure data is tagged so you can retrieve it easily
    - DR considerations
    - E-Discovery requests
      - What about data held in the Cloud – do you know which is in the Cloud and where? Can you access it?

(c) VigiTrust 2003-2013
Focon us 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.

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

YEAR 1
1. Standards Published
   October
2. Standards Effective
   January 1
3. Market Implementation
   All Year
4. Feedback Begins
   November
5. Old Standards Retired
   December 31
6. Feedback Review
   April–August
7. Draft Revisions
   November–April
8. Final Review
   May–July

YEAR 2

YEAR 3

COMMUNITY MEETINGS
September–October

(c) VigiTrust 2003-2013
Why Application Security Matters for the Payments Industry

Lifecycle of a Credit Card Transaction

Credit Card Transactions

Five Brands
- MasterCard Worldwide
- Discover Financial Services
- American Express
- VISA
- JCB

Banks

Payment Service Providers

Merchants

Customers
PCI DSS Structure

1. **Build & Maintain a Secure Network**
   - Install & maintain a firewall configuration to protect data
   - Do NOT use vendor supplied defaults for passwords or other security parameter

2. **Protect Cardholder data**
   - Protect stored data
   - Encrypt the transmission of cardholder data

3. **Maintain a Vulnerability Management Programme**
   - Use & regularly update anti-virus software
   - Develop & maintain secure systems & applications

4. **Implement strong Access Control Measures**
   - Restrict access to data by business need-to-know
   - Assign a unique ID to each person with computer access
   - Restrict physical access to cardholder data

5. **Regularly monitor & Test Networks**
   - Track & monitor ALL access to network resources & cardholder data
   - Regularly test security systems & processes

6. **Maintain an Information Security Policy**
   - Maintain a policy that addresses information security
Understanding PCI DSS Controls

- **Available through**
  - Risk based approach
    - Internal or 12 Requirements Approach
  - Prioritized approach

- **PCI DSS Controls can be categorized as follows**
  - Technical Controls
  - Policies & Procedures
  - User Awareness & Training

- **Controls may include several control points**
  - Mix of the above e.g. technical control + policy

- **Some controls are inherently requiring recurring tasks, e.g.**:
  - Quarterly Scans
  - Log Analysis
  - Yearly training

- **What about controls relating to Third Party Assurance**
  - 3rd Party Assurance identified as one of the Key Change Drivers
  - Requirement 12.8
  - Third Party Assurance SIG
  - Logging & auditing controls throughout the standard

(c) VigiTrust 2003-2013
Required Documentation

- Diagrams and Data Flows
  - Ecosystem Diagrams
  - Data Flow Diagrams
  - Network Diagrams
- Asset Inventory
- Acceptable Usage Policy for staff
- Access Control Policy
- Firewall Rules and Business Justification for Rules
- AV, Anti-Spam and Intrusion Detection-Prevention Policy
- **Hardening, Log and Patch Management Policy**
- Back-Up and Media Storage Policy
- **Security Assessment, Application Security & Vulnerability Management Policy**
- Incident Response Plan
- **Management of Third Parties Policy**
Changes to Data Protection in the EU

• Not a directive but a single regulation in the EU
  – Harmonization at European level...but with challenges

• Applies to companies based outside in the EU if personal data is handled abroad by companies that are active in the EU and offer services to EU citizens

• Right to be forgotten

• Controllers responsibilities
  – Policies & procedures
  – Staff Training

• Data processing impact assessment
  – If any data is likely to present risks to individuals

• Security
  – Both processor and controllers must put security measures in place

• Data Breach Notification
  – Within 24 hours of noticing the breach

• Data Portability (service providers) & Data Transfers

• Data Protection Officers
ISO 2700 series – Risk Assurance & Security Perspectives

• Based on the ISMS
• 4 Levels of documentation work
  – Policies
  – Procedures
  – Work Instructions
  – Records Documents

• Where is Risk Assurance Mentioned & How:
  – Communication & Operations Management (10)
    • Protection Against Malicious & Mobile Code
    • Security & Network Services
    • Audit Logging
  – Access Control (11)
    • Application & Information Access Control
  – Information Systems Acquisition, Development & Maintenance (12)
    • Cryptographic controls
    • Security In development & support
  – Information Security Incident Management (13)
    • Reporting & Management of Security events, weaknesses & incidents
  – Compliance (15)
    • Legal Requirements & Audit Considerations
Security & GRC Process

Regulatory, Legal & Corporate Governance Frameworks

1. **Education, Security & Awareness**
2. **Self-Governed Pre-Assessment**
3. **Security Blueprint for Remediation Work**
4. **Policies & Procedures**
   - Network & Hardware Security
   - Pen-Testing & Application Security
   - Specialized Skills Transfer
5. **Official Assessors & Auditors**

- **SOX**
- ISO 27000 series
- EU Data Protection
- PCI DSS
- HIPAA
- Others

(c) VigiTrust 2003-2013
Understanding Your Ecosystem

Key
- High Security Zone: CC
- Data Suppliers
- Acme: Main Hubs
- Partners requiring database access

Internet
(Including ISPs)

ACME
EU HQ

ACME LA

ACME NYC

ACME UK

ACME France

Partner 1

EU Lawyers for ACME

EU Accountants For ACME
Chief Security Officer
Project leader for all Security Related Matters

5 Pillars of Security Framework™

PHYSICAL SECURITY
- Access to Building
- Physical Assets
- IT Hardware
- Vehicle Fleet

PEOPLE SECURITY
- Permanent & Contract Staff
- Partners
- 3rd Party Employees
- Visitors
- Special Events Security

DATA SECURITY
- Trade Secrets
- Employee Data
- Database
- Customer Data

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

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

Operations Manager, Security Staff
HR, Security Staff
HR, IT Team & Manager
IT Team & Manager
Operations Manager, IT Team, HR

Best Practice Security Framework for Enterprise
Corporate Culture & Risk Management – The overall Picture

Corporate Values

Corporate Ecosystem

Risk Management & Safeguards

Residual Risk Surface which needs to be managed by your Organization

Risk Management Strategy for Internal and/or external Risk Management Teams

DPA, PCI DSS & ISO 27001 compliance
Best Practices for Third Party Assurance

• Own your Ecosystem by:
  – Performing an asset inventory, network & application architecture review
  – Mapping out ecosystem actors & data flow – including 3rd parties!

• Data Management & Classification
  – Ensure you have up to date data flow diagrams
  – Classify all data that comes from or goes to 3rd parties
  – Protect client’s personal data and all sensitive data at rest, in transit and in use

• Use Compliance as a driver for 3rd party assurance
  – Good guidelines – basic benchmark
  – Not the end game though – security & good governance is the goal
  – Make it business as usual – continuous process

• Mathieu’s Crystal ball...3rd Party Assurance is here to stay!

(c) VigiTrust 2003-2013
Third Party Assurance

ISACA & itSMF IT Governance Conference
Dublin, 11th October 2013

Mathieu.gorge@vigitrust.com

www.vigitrust.com