RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

NOW MATTERS

SESSION ID: PDAC-R04

# THE TOP 9 FACTORS FOR EFFECTIVE DATA PROTECTION CONTROLS

**Ciske van Oosten**

Global Intelligence Senior Manager
Verizon Enterprise Solutions

# Proprietary Statement

This document and any attached materials are the sole property of Verizon and are not to be used by you other than to evaluate Verizon's service.

This document and any attached materials are not to be disseminated, distributed or otherwise conveyed throughout your organization to employees without a need for this information or to any third parties without the express written permission of Verizon.

# Content

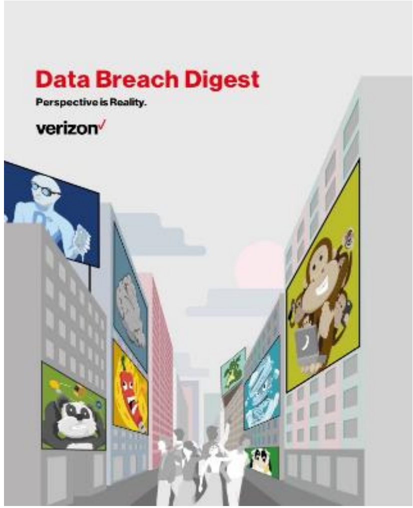
1. **Data protection threats** – long term trends
2. **Data security compliance** – the value of compliance
3. **Security control failures** – what fails, and how?
4. **Control effectiveness** and sustainability
5. **The top 9 factors** for effective data protection controls

# Forensic Data Breach Investigations & Analyses

## Threat. Defined as.

**Actor:** Who did it?
**Action:** How did they do it?
**Asset:** What was affected?
**Attribute:** How was it affected?

Verizon started data breach investigations in **2004** and started reporting on them in **2008**



Data Breach Digest
Perspective is Reality.
verizon

2017 Data Breach Investigations Report
10th Edition
verizon

# Data Protection & Compliance Research

Verizon has published five **Payment Security Reports** since 2010 with #6 due this year.

Our Compliance industry analysis goes as far back as 2002.

VERIZON 2010 PAYMENT CARD INDUSTRY COMPLIANCE REPORT

2010

VERIZON 2011 PAYMENT CARD INDUSTRY COMPLIANCE REPORT

2011

Verizon 2014 PCI Compliance Report

2014

Verizon 2015 PCI COMPLIANCE REPORT

2015

2017 Payment Security Report

2017

2018

# PCI Data Security Standards

Over 10 years, while objectives and key requirements have not changed, we've seen some increases in total control requirements and significant increase in test procedures.

| PCI DSS | Version 1.1 | Version 3.2 |
|---|---|---|
| Year | 2006 | 2016 |
| Number of pages | 50 | 139 |
| Control Objectives | 6 | 6 |
| Key Requirements | 12 | 12 |
| Total Controls | 64 | 78 |
| Total Requirements | 206 | 251 |
| Test Procedures | 251 | 417 |

# Who Is Getting Breached? (PCI)

**Question:** In what month are payment card data breaches most likely to occur?

**Answer:** October (14%), followed by March (12%) and January (10%).

**Confirmed payment card data breaches by industry:**

| | |
|---|---|
| **Retail** | 41.2% |
| **Hospitality & Travel** | 38.5% |
| **Financial Services** | 11.5% |
| **IT Services** | 2.7% |
| **Other** | 6.2% |

*Verizon PFI global caseload 2010 to 2016.*

**Highest percent of breaches based on organization size** (# of employees):

| | | |
|---|---|---|
| **Small** | (11 to 100) | 42.1% |
| **Medium** | (101 to 1000) | 20.2% |
| | (1001 to 10,000) | 11.8% |

# Fourteen Years Of Payment Card Compromises

## Investigated by Verizon

**Question:**
How many organizations were PCI DSS compliant at the time of their data compromise?

# Difference Between DSS-validated and Data-compromised Organizations

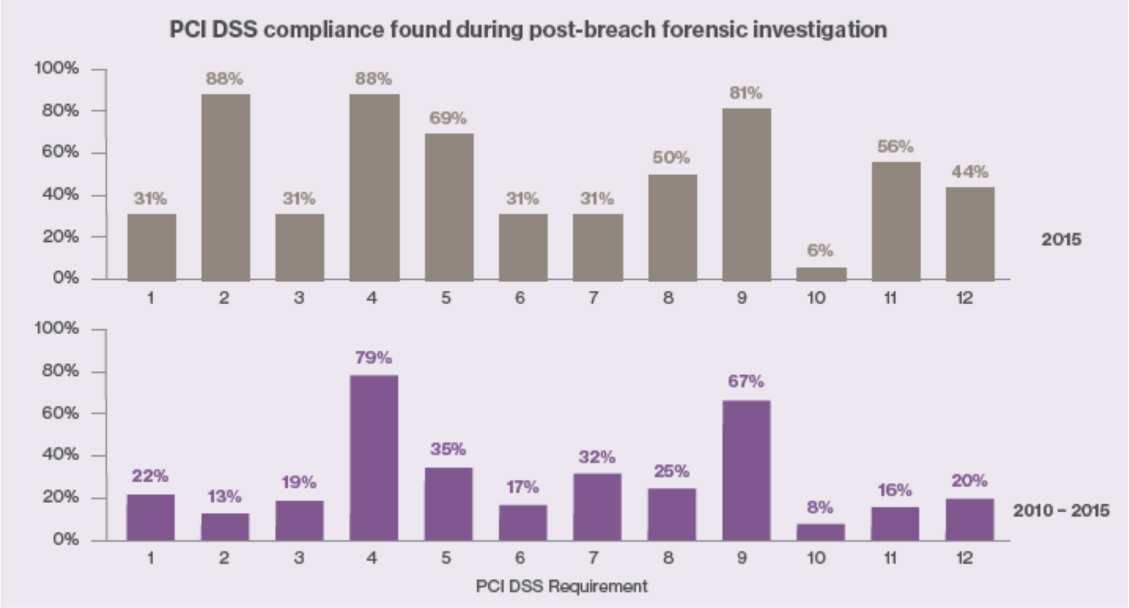
Organizations experiencing confirmed payment card data breaches consistently demonstrate significantly lower compliance with 11 of the 12 PCI DSS key security requirements.

| | |
|---|---|
| **2015:** | **42p.p** delta |
| **2016:** | **64p.p** delta |

# PCI Data Security Standards

Compromised organizations have substantially lower compliance, whether measured over a one-year or six-year period.

% organizations compliant per DSS Key Requirement - at time of breach:



ᴾFI compliance, 2010 – 2015. Data includes "partial yes" responses (not indicative of full compliance with PCI DSS).

*Source: Verizon 2017 Payment Security Report*

# Card Compromise and Non-compliance

**91%** of breached organizations did not provide evidence that they validated PCI DSS compliance and they were determined compliant prior to the breach.

How many organizations provided evidence that they at least validated their PCI DSS compliance prior to the breach?

**63%** confirmed to be substantially non-compliant prior to, and at time of the breach.

?

**28%** unknown – no evidence of an operational compliance program and no compliance validation.

*Based on 288 confirmed payment card data breach cases investigated between 2010 and 2016.*

## A familiar discussion

***Investigator***
*" Payment card data was compromised from your systems."*

***Client***
*" We did all we could to protect the data!"*

***Investigator***
*" You are PCI DSS compliant right? "*

***Client***
*" Yes, sure! "*

***Investigator***
*" Did you validate PCI DSS compliance? Do you have a PCI DSS Report on Compliance (RoC) and attestation (AoC)? "*

***Client***
*" Well …. "*

# QSA Horror Story

## Terrifyingly short

**Question:** How long would you make your password if storing primary account numbers (PANs) in clear text?

During one assessment, a QSA found an admin account with access to 70 million PANs protected by the weakest password we've ever seen - **a single character**!

The operator's defense was that it was a "special character".

**#lame_excuse**

# Control Failure Taxonomy

1. **Actions of people**
   Action, or lack of action, taken by people either deliberately or accidentally that impact cyber security.

2. **Systems and technology failures**
   Failure of hardware, software, and information systems.

3. **Failed internal processes**
   Problems in internal business processes that impact the ability to implement, manage, and sustain cyber security.

4. **External events**
   Issues outside the control of the organization (disasters, legal issues, and service provider dependencies).

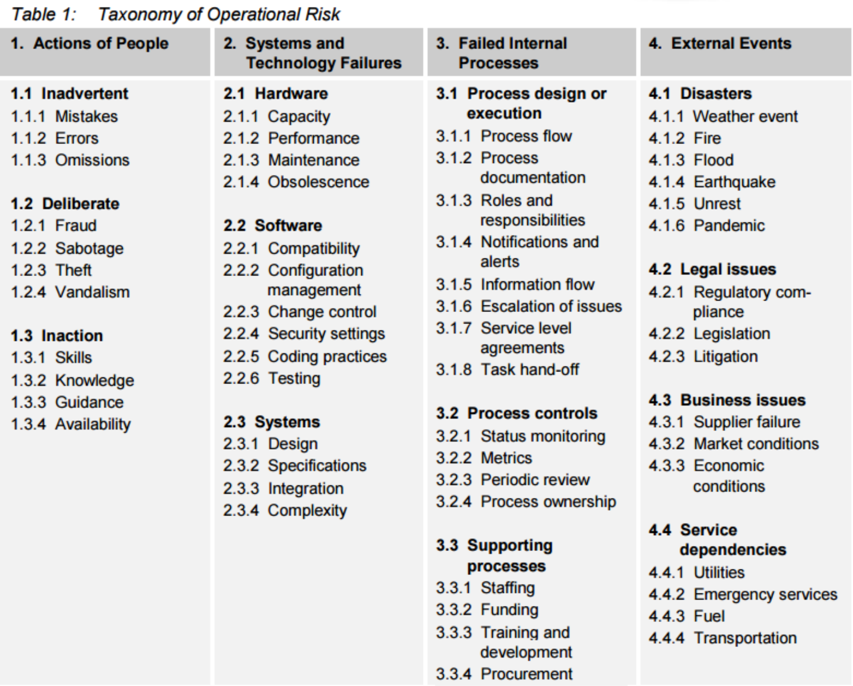


*Table 1: Taxonomy of Operational Risk*

| 1. Actions of People | 2. Systems and Technology Failures | 3. Failed Internal Processes | 4. External Events |
|---|---|---|---|
| **1.1 Inadvertent**<br>1.1.1 Mistakes<br>1.1.2 Errors<br>1.1.3 Omissions<br><br>**1.2 Deliberate**<br>1.2.1 Fraud<br>1.2.2 Sabotage<br>1.2.3 Theft<br>1.2.4 Vandalism<br><br>**1.3 Inaction**<br>1.3.1 Skills<br>1.3.2 Knowledge<br>1.3.3 Guidance<br>1.3.4 Availability | **2.1 Hardware**<br>2.1.1 Capacity<br>2.1.2 Performance<br>2.1.3 Maintenance<br>2.1.4 Obsolescence<br><br>**2.2 Software**<br>2.2.1 Compatibility<br>2.2.2 Configuration management<br>2.2.3 Change control<br>2.2.4 Security settings<br>2.2.5 Coding practices<br>2.2.6 Testing<br><br>**2.3 Systems**<br>2.3.1 Design<br>2.3.2 Specifications<br>2.3.3 Integration<br>2.3.4 Complexity | **3.1 Process design or execution**<br>3.1.1 Process flow<br>3.1.2 Process documentation<br>3.1.3 Roles and responsibilities<br>3.1.4 Notifications and alerts<br>3.1.5 Information flow<br>3.1.6 Escalation of issues<br>3.1.7 Service level agreements<br>3.1.8 Task hand-off<br><br>**3.2 Process controls**<br>3.2.1 Status monitoring<br>3.2.2 Metrics<br>3.2.3 Periodic review<br>3.2.4 Process ownership<br><br>**3.3 Supporting processes**<br>3.3.1 Staffing<br>3.3.2 Funding<br>3.3.3 Training and development<br>3.3.4 Procurement | **4.1 Disasters**<br>4.1.1 Weather event<br>4.1.2 Fire<br>4.1.3 Flood<br>4.1.4 Earthquake<br>4.1.5 Unrest<br>4.1.6 Pandemic<br><br>**4.2 Legal issues**<br>4.2.1 Regulatory compliance<br>4.2.2 Legislation<br>4.2.3 Litigation<br><br>**4.3 Business issues**<br>4.3.1 Supplier failure<br>4.3.2 Market conditions<br>4.3.3 Economic conditions<br><br>**4.4 Service dependencies**<br>4.4.1 Utilities<br>4.4.2 Emergency services<br>4.4.3 Fuel<br>4.4.4 Transportation |

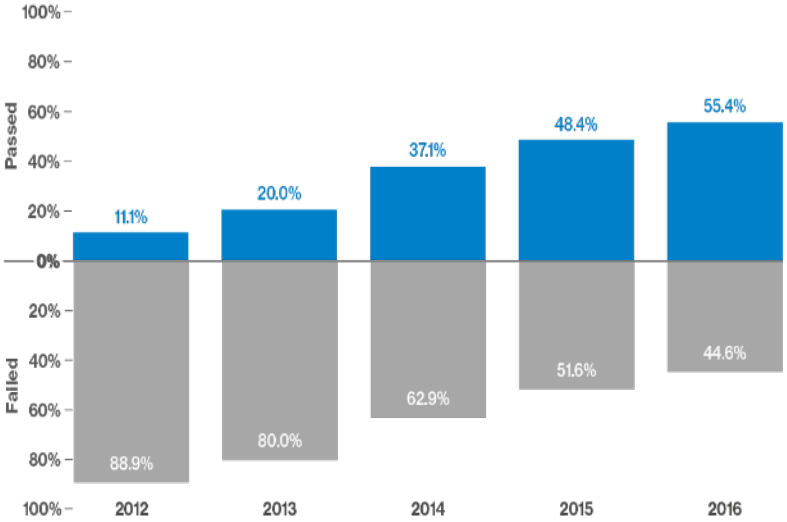
*Source: CMU/SEI "A Taxonomy of Operational Cyber Security Risks Version 2" by James J. Cebula et al. , May 2014. https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_91026.pdf*

# Control Sustainability

**In 2016, for the first time more than half of companies were compliant at interim PCI DSS assessment.**

Since 2012, full compliance has continued an upward progression, but many still fail to maintain compliance.

So where are the problems?



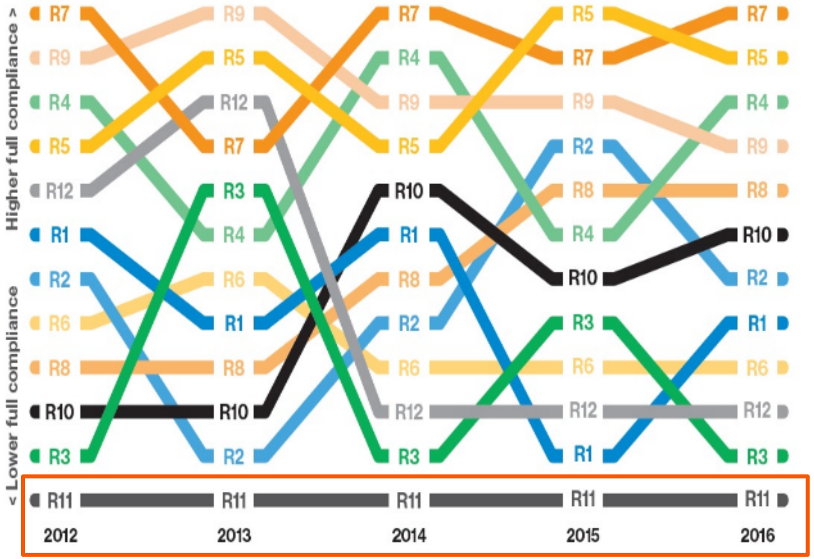
*Source: Verizon 2017 Payment Security Report*

# Full Compliance

## Trend Analysis by Requirement

Percentage of organizations achieving full compliance improved across all 12 Key Requirements from 2012 to 2016.

**Security Testing (R11)** retained its traditional place at the bottom of the list in terms of full compliance (71.9%)

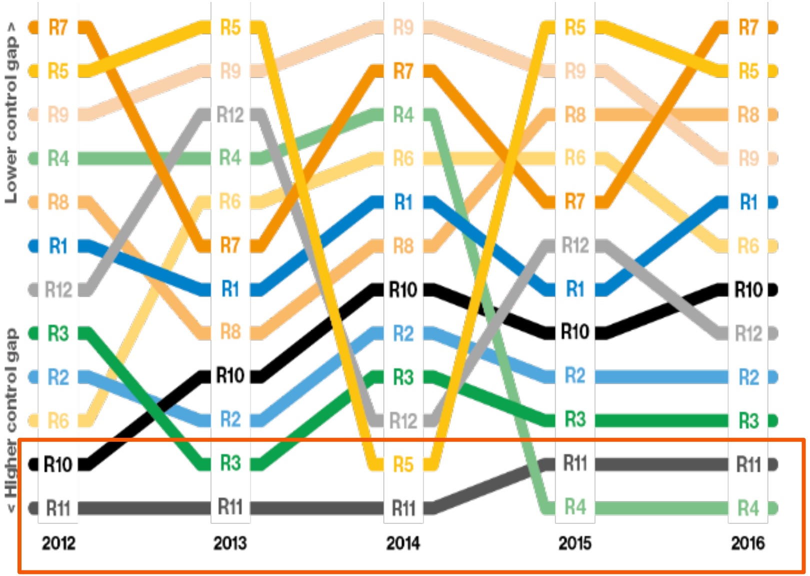


*Source: Verizon 2017 Payment Security Report*

# Control Gap

## Trend Analysis by Requirement

Five out of six of the worst performers are the same now as they were in 2013.



*Source: Verizon 2017 Payment Security Report*

# Control Effectiveness

## Best Practices for Maintaining PCI DSS

1. **Standardized control frameworks**
   *Integrate controls into a larger set.*

2. **Manual control reviews**

3. **Security control volatility**
   *How frequently a control is likely to change over time.*

4. **Security control weaknesses**
   *Controls with identified weaknesses should be monitored more frequently until remedied.*

5. **Identify control failure causes**

6. **Performance metrics**
   *Develop metrics to measure success.*

7. **Commitment**
   *Maintaining compliance.*

*Source: PCI SSC - Best Practices for Maintaining PCI DSS Compliance Special Interest Group PCI Security Standards Council - August 2014*

# Why Do Organizations Get Breached And Data Compromised?

“Security breaches and data compromises occur because one or more controls are missing, not fully operational, or the control was operating as designed, but was knowingly or unknowingly ineffective.”

*Source: Verizon 2017 Payment Security Report*

**It’s <u>not</u> a knowledge or technology problem.**

**It’s a proficiency problem.**

# Detecting Low Proficiency

**Ask the right questions:**

- Which controls are effective? (and not merely “in place”)
- Which controls fail? When and how?
- What is the impact when a control fails?
- How soon do you detect control failure?
- How quickly do you restore failed controls?
- Was the root cause of failure remedied?

**Top performers** proactively track the failure rate of their security controls.

**Mediocre performers** follow a “break / fix" model year-after-year.

**Low performers** wait for an assessor to point out the control failures.

# The top nine factors for achieving sustainable control effectiveness

9

- Control Environment
- Control Design
- Control Risk
- Control Robustness
- Control Resilience
- Lifecycle Management
- Performance Measurement
- Maturity Measurement
- Self-Assessment

# Nine Factors

1. Design and maintain a control environment
2. Design and integrate security controls
3. Measure the control risk of each control
4. Enhance control robustness
5. Enhance control resilience
6. Maintain control lifecycle management
7. Performance management
8. Maturity measurement
9. Control self-assessment

Control Environment

Control Design

Control Risk

Control Robustness

Control Resilience

Lifecycle Management

Performance Measurement

Maturity Measurement

Self-Assessment

# F1: Control Environment

An effective control environment is:

“an environment in which **competent** people understand their **responsibilities**, the **limits** of their authority, and are **knowledgeable**, mindful and **committed** to doing  what is right and doing it the right way.”

*Source: Sanjay Anand  “Sarbanes-Oxley Guide for Finance and Information Technology Professionals”, page 49, chapter three “Control Environment”, published by John Wiley & Sons.*

- Control Environment
- Control Design
- Control Risk
- Control Robustness
- Control Resilience
- Lifecycle Management
- Performance Measurement
- Maturity Measurement
- Self-Assessment

# Capacity, Capability, Competence, Commitment

- **Capacity**
  Required number of resources; people, process and technology.  You cannot measure, manage, and improve that which you do not have.

- **Capability**
  Ability to direct and apply resources to perform data protection tasks  and the processes to support them.

- **Competence**
  Having the skills, knowledge and experience to establish and maintain an operational control environment. This requires a level of maturity in business process management to achieve quality (repeatability and consistency) in each step of the control lifecycle.

- **Commitment**
  Assurance that management and employees will consistently adhere to data protection and compliance programs.

**Data protection with consistency:**
**doing the right things,**
**in the right manner and**
**at the right time.**

# F2: Control Design

**Documented control profiles:**

1. **Objective:** define the control objective
2. **Owner:**  assigned ownership and responsibilities
3. **Function:** management, procedural, technical etc.
4. **Purpose:** preventative, detective, corrective, directive
5. **Architecture:** system-specific, common, hybrid
6. **Risk:** control to risk matrix / mapping
7. **Implementation:** specifications, scope, dependencies
8. **Operation:** specifications, scope, processes, dependencies
9. **Maintenance:** specifications, scope, processes
10. **Governance:** related policies, standards and frameworks

Control Environment

Control Design

Control Risk

Control Robustness

Control Resilience

Lifecycle Management

Performance Measurement

Maturity Measurement

Self-Assessment

# The Control Landscape

## Control Architecture Allocations:

- **System-Specific Controls**
  Controls that provide a security capability for a particular information system only
- **Common Controls**
  Controls that provide  a security capability for multiple information systems
- **Hybrid controls**
  Controls that have both system-specific and common characteristics

# Control Design Guidance

**Built-in Effectiveness**
Controls should achieve effectiveness by design while operating according to the limitations of their design and control environment.

**Dependencies**
Controls are supported by people, processes and technology, and are dependent or interdependent upon other controls.

**Control Maturity**
Newly-introduced security controls are rarely mature in terms of design and operation. Design should cater to growth over time.

# Control Deficiencies

**Deficiency in design exists when:**

a. a control necessary to meet the control objective is missing, or

b. an existing control is not properly designed so that, even if the control operates as designed, the control objective would not be met.

**Deficiency in operation exists when**

a. a properly designed control does not operate as designed, or

b. when a person performing the control does not possess the  necessary competence or authority to perform the control effectively.

*Source: PCAOB Public Accounting Oversight Board Auditing Standard No. 5 available online at https://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_5_Appendix_A.aspx*

# F3: Control Risk

**The likelihood and impact of control failure, due to absence or failure of control design or operation.**

- Typically caused by controls losing effectiveness over time.
- Continuously measure and monitor:
    - *Inherent risk x Residual risk x Detection risk*

> *“ Controls are effective only as long as they mitigate risk to an acceptable risk tolerance. They are often sustainable merely by luck—certainly not by design. ”*
>
> ~ Verizon 2017 Payment Security Report

Control Environment

Control Design

Control Risk

Control Robustness

Control Resilience

Lifecycle Management

Performance Measurement

Maturity Measurement

Self-Assessment

# F4: Control Robustness

Capacity of a control, and/or the control environment, to absorb disturbance and still retain its basic structure and viability without the need for intervention.

- Control Environment
- Control Design
- Control Risk
- Control Robustness
- Control Resilience
- Lifecycle Management
- Performance Measurement
- Maturity Measurement
- Self-Assessment

# F5: Control Resilience

**Goals.**

- **Anticipate:** Maintain a state of informed preparedness.
- **Withstand:** Continue essential functions despite attacks.
- **Recover:** Restore functions to fullest extent possible.
- **Evolve:** Change functions to minimize future adverse effects.

*Source: MITRE, "Cyber Resiliency Basics" by Rosalie McQuaid, November 15, 2013*
*https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/cyber-resiliency-basics*

Control Environment

Control Design

Control Risk

Control Robustness

Control Resilience

Lifecycle Management

Performance Measurement

Maturity Measurement

Self-Assessment

# F6: Lifecycle Management

1. Conception
2. Design and Build
3. Testing
4. Introduction and Deployment
5. Operation and Monitoring
6. Growth and Evolution
7. Maintenance and Improvement
8. Maturity
9. Decline and Retirement

- Control Environment
- Control Design
- Control Risk
- Control Robustness
- Control Resilience
- Lifecycle Management
- Performance Measurement
- Maturity Measurement
- Self-Assessment

# F7: Performance Measurement

1. Establish **performance standards** for each component of the control environment.
2. Maintain performance measurement program on:
   a. Control environment
   b. Control design, risk, robustness, resilience
   c. Control lifecycle management
   d. Defined metrics
3. Provide ongoing feedback, guidance on corrective actions.

- Control Environment
- Control Design
- Control Risk
- Control Robustness
- Control Resilience
- Lifecycle Management
- Performance Measurement
- Maturity Measurement
- Self-Assessment

# F8: Maturity Measurement

1. **Measuring Control Design:**
   How well it should work in theory

2. **Measuring Control Implementation:**
   How well it actually performs in practice

3. **Measuring Control Monitoring:**
   How we know that it's still working

4. **Measuring Control Evaluation:**
   How frequently we evaluate effectiveness & efficiency

5. **Scoring Control Effectiveness** :
   DIME Model: "Design, Implementation, Monitoring, Evaluation"

Control Environment

Control Design

Control Risk

Control Robustness

Control Resilience

Lifecycle Management

Performance Measurement

Maturity Measurement

Self-Assessment

# Control Effectiveness: Maturity

| Control effectiveness | Guide |
|---|---|
| **Fully effective** | Nothing more to be done except review and monitor the existing controls. |
| **Substantially effective** | Most controls are designed correctly but more work to be done on design, validation. |
| **Partially effective** | Some controls are designed correctly and operate effectively, but many need work to ensure they address root causes and/or contributing factors. |
| **Largely ineffective** | Significant control gaps exist, or controls do not operate effectively at all. |
| **None or totally ineffective** | Management has no confidence that any degree of control is being achieved. |

# F8: Maturity Measurement

## How To - Example:

### 5. Scoring Control Effectiveness (No Weighting)

Apply DIME:

**D**esign = 2 (3)
**I**mplementation = 3 (3)
**M**onitoring = 2 (3)
**E**valuation = 1 (3)
TOTAL = 8 (12) = 0.75 (75% total effectiveness)

NOTE: If either Design, or Implementation is zero then total score becomes zero

- Control Environment
- Control Design
- Control Risk
- Control Robustness
- Control Resilience
- Lifecycle Management
- Performance Measurement
- Maturity Measurement
- Self-Assessment

*Source: John Mitchell - Measuring Control Effectiveness*
*GRC 2.0 -Breaking Down The Silos, ISACA Ireland Conference –3rd October 2014*
*available at http://www.isaca.org/chapters5/Ireland/Documents/2014%20Presentations/easuring%20Control%20Effectiveness%20-%20John%20Mitchell.pdf*

# F9: Control Self-Assessment

- Establish self-assessment program.
- Standardize assessment methods.
- Develop and maintain assessment procedures.
- Build internal assessment competency to measure, monitor and **proactively** manage factors.
- Self-assess your Capacity, Capability, Competence, and Commitment.

Control Environment

Control Design

Control Risk

Control Robustness

Control Resilience

Lifecycle Management

Performance Measurement

Maturity Measurement

Self-Assessment

# Apply What You Have Learned Today

1. Commit to competence!

2. Achieve control environment sustainability by design – not by luck!

3. Map and measure control risk.

4. Manage controls throughout their lifecycle.

5. Develop and maintain a control effectiveness self-evaluation program.

**You cannot prevent security breaches and data compromises by maintaining a set of ineffective controls.**

# Apply What You Have Learned Today

## Lessons learned:

- ***Measure twice, cut once.*** You seldom get a 2nd change at preventing data breaches.
- **Develop your in-house proficiency.** Confidence and predictable outcomes are achieved through knowledge, skill, and experience.
- Do not place mission critical tasks in the hands of unqualified resources.

# Books: Security Management

| | YEAR | TITLE | AUTHOR | PUBLISHER | PAGES | ISBN |
|---|---|---|---|---|---|---|
| 1 | 2003 | The Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program | Gerald Kovacich | Butterworth-Heinemann | 361 | 9780750676564 |
| 2 | 2003 | Principles and Practice of Information Security | Linda Volonino & Stephen Robinson | Pearson | 256 | 9780131840270 |
| 3 | 2004 | A Practical Guide to Managing Information Security | Steve Purser | Artech House | 259 | 9781580537025 |
| 4 | 2004 | Executive Guide to Information Security: Threats, Challenges, and Solutions | Mark Egan, Tim Mather | Addison-Wesley | 288 | 9780321304513 |
| 5 | 2008 | IT Compliance and Controls: Best Practices for Implementation | James J. DeLuccia | Wiley | 274 | 9780470145012 |
| 6 | 2009 | Beautiful Security: Leading Security Experts Explain How They Think | Andy Oram, John Viega | O'Reilly Media | 304 | 9780596527488 |
| 7 | 2013 | CISO and Now What? | Michael Oberlaender | Createspace | 102 | 9781480237414 |
| 8 | 2013 | Executive's Guide to COSO Internal Controls: Understanding and Implementing the New Framework | Robert Moeller | Wiley | 304 | 9781118626412 |
| 9 | 2015 | Internal Control Audit and Compliance: Documentation and Testing Under the New COSO Framework | Lynford Graham | Wiley | 416 | 9781118996218 |
| 10 | 2015 | Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats | Scott Donaldson, Stanley Siegel, Chris Williams, Abdu Aslam | Apress | 536 | 9781430260820 |
| 11 | 2016 | Security Controls Evaluation, Testing, and Assessment Handbook | Leighton Johnson | Syngress | 678 | 9780128023242 |
| 12 | 2016 | Psychology of Information Security: Resolving Conflicts Between Security Compliance and Human Behaviour | Leron Zinatullin | IT Governance Ltd | 128 | 9781849287890 |
| 13 | 2016 | CISO Desk Reference Guide: A Practical Guide for CISO’s | Bill Bonney, Gary Hayslip, Matt Stamper | CISODRG | 366 | 9780997744118 |

# Books: Risk Management

| | YEAR | TITLE | AUTHOR | PUBLISHER | PAGES | ISBN |
|---|---|---|---|---|---|---|
| 1 | 1999 | Risk Management for Security Professionals | Carl A. Roper | Butterworth-Heinemann | 304 | 9780750671132 |
| 2 | 2001 | Information Security Risk Analysis | Thomas R. Peltier | Auerbach | 281 | 9780849308802 |
| 3 | 2002 | Managing Information Security Risks: The OCTAVE | Christopher Alberts & Audrey Dorofee | Addison-Wesley | 512 | 9780321118868 |
| 4 | 2005 | Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments, The | Douglas Landoll | Auerbach | 473 | 9780849329982 |
| 5 | 2006 | A Practical Guide to Security Assessments | Sudhanshu Kairab | Auerbach | 498 | 9780849317064 |
| 6 | 2009 | The Failure of Risk Management: Why It's Broken and How to Fix It | Douglas W. Hubbard | Wiley | 281 | 9780470387955 |
| 7 | 2011 | Security Risk Management: Building an Information Security Risk Management Program from the Ground Up | Evan Wheeler | Syngress | 340 | 9781597496155 |
| 8 | 2012 | Information Security Risk Assessment Toolkit: Practical Assessments Through Data Collection and Data Analysis | Mark Talabis & Jason Martin | Syngress | 258 | 9781597497350 |
| 9 | 2014 | Measuring and Managing Information Risk: A Fair Approach | Jack Freund & Jack Jones | Butterworth-Heinemann | 408 | 9780124202313 |
| 10 | 2016 | IT Security Risk Control Management: An Audit Preparation Plan | Raymond Pompon | Apress | 311 | 9781484221396 |

# Books: Security Measurement & Metrics

| | YEAR | TITLE | AUTHOR | PUBLISHER | PAGES | ISBN |
|---|---|---|---|---|---|---|
| 1 | 2005 | The Chief Information Security Officer's Toolkit: Security Program Metrics | Fred Cohen | Fred Cohen & Associates | 228 | 9781878109354 |
| 2 | 2007 | Security Metrics: Replacing Fear, Uncertainty, and Doubt | Andrew Jaquith | Addison-Wesley | 336 | 9780321349989 |
| 3 | 2007 | How to Measure Anything: Finding the Value of "Intangibles" in Business | Douglas Hubbard | John Wiley | 287 | 9780470110126 |
| 4 | 2007 | Complete Guide to Security and Privacy Metrics - Measuring regulatory compliance, operational resilience, and ROI | Debra S. Herrmann | Auerbach | 824 | 9780849354021 |
| 5 | 2009 | Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement | W. Krag Brotby | CRC Press | 223 | 9781420052855 |
| 6 | 2011 | Security Metrics, a Beginner's Guide | Caroline Wong | McGraw-Hill | 397 | 9780071744003 |
| 7 | 2013 | Pragmatic Information Security Metrics | W. Krag Brotby & Gary Hinson | Auerbach | 512 | 9781439881521 |
| 8 | 2014 | Measures and Metrics in Corporate Security | George Campbell | Elsevier | 145 | 9780128006887 |
| 9 | 2015 | Measuring and Communicating Security's Value: A Compendium of Metrics for Enterprise Protection | George Campbell | Elsevier | 226 | 9780128028414 |
| 10 | 2016 | How to Measure Anything in Cybersecurity Risk | Douglas Hubbard, & Richard Seiersen | Wiley | 304 | 9781119085294 |

# Thank you.

Read the 2017 Payment Security Report
to get the full picture.

**VerizonEnterprise.com/PaymentSecurity**

Ciske van Oosten
email: ciske.vanoosten@verizon.com

2017 Payment Security Report

Revealing the challenges in sustaining payment card security

verizon