PCI Version 2.0 and Risk Management

Doug Landoll, CISSP, CISA, QSA, MBA
Practice Director
Risk and Compliance Management

ACCUVANT
Alignment • Clarity • Confidence

Payment Card Industry Data Security Standard

- Objective: Protect cardholder data (CHD) wherever it resides
- Application: All card brand merchants and service providers who store, process, or transmit CHD

Risk Management

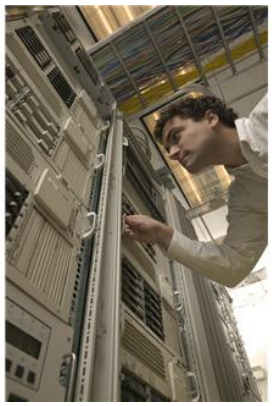
Risk Management

- *identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control t probability and/or impact of unfortunate events or to maxim the realization of opportunities.*

~Hubbard, Douglas (2009). *The Failure of Risk Management: Why It's B... and How to Fix It*. John Wiley & Sons. p. 46.

Another Way of Looking at Risk

Hardware / SW



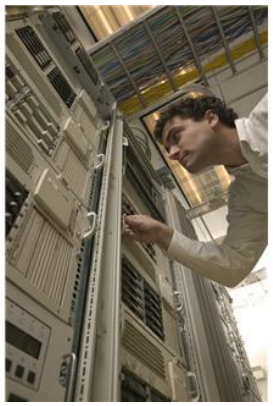
- Funding

- Staff

Given your limited resources are you confident that your initiatives are addressing the largest risks to your organization's assets?

Limited Resources to Address Risk

Hardware / SW



- Funding

- Staff

How do you demonstrate that to your management?

ACCUVANT

PCI DSS v2.0 Changes Re: Risk

- Old Way (Controls Based)
  - Historically, the DSS was prescriptive in its controls. Merchants and service providers were told what and how to fulfill the control requirements
- New Way (Risk Based)
  - Some control elements can/must be address based on risk.
  - More documentation and process.
  - Controls required closer to business objectives.

DSS v2.0 Risk Application

DSS v2.0 contains a number of areas using a risk-based approach:

- 6.1 – Patch Management
- 6.2 – Vulnerability Criticality Ranking
- 11.1 – Wireless Access Point Testing
- 11.4 – IDS/IPS Placement
- 12.1 – Required Annual Risk Assessment
- 12.8.3 – Service Provider Management

Requirement 6.1 (System Patching)

6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.

Note: *An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

Requirement 6.1 Effect

Impact: Organizations have the ability to prioritize patching efforts according to their own risk-based assessment of existing exposures.

Benefit: Work is more easily prioritized and scheduled, easing the overall impact upon personnel and affected systems.

Required Proof: The organization must be able to show a consistent methodology that was used to evaluate each patch for criticality and prioritization. This methodology must follow the "threat → control → vulnerability → impact → likelihood → risk valuation" approach.

Requirement 6.2 (Maintain Config Stds).

6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.

Notes: *Risk rankings should be based on industry best practices. For example, criteria for ranking "High" risk vulnerabilities may include a CVSS base score of 4.0 or above, and/or a vendor-supplied patch classified by the vendor as "critical," and/or a vulnerability affecting a critical system component.*

The ranking of vulnerabilities as defined in 6.2.a is considered a best practice until June 30, 2012, after

Requirement 6.2 Effect

Impact: Organizations have the ability to evaluate identified vulnerabilities according to their own risk-based assessment of existing exposures.

Benefit: Required remediation activities are reduced by proving that the criticality of the identified vulnerability is lessened through the existence of compensating controls.

Required Proof: The organization must evaluate each vulnerability, taking into account both existing external rankings and mitigating internal factors. This evaluation must be documented and follow the "threat → control → vulnerability → impact → likelihood → risk valuation" approach.

Requirement 11.1 (Security Testing)

11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.

Note: *Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.*

Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.

Requirement 11.1 Effect

Impact: Organizations can perform non-technical wireless access point detection. This is especially critical with merchants with numerous similar facilities.

Benefit: Where this option can be performed, the expense required to implement wireless scanning or intrusion detection systems can be saved.

Required Proof: The choice to use this method carries an increased risk due to the decision to rely upon manual controls and the guiding policies should demonstrate the risk-based decision making process that was used to approve this solution.

Requirement 11.4 (IDS/IPS)

11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises.

Requirement 11.4 Effect

Impact: Previous versions of the DSS required the IDS/IPS systems to monitor "all traffic in the cardholder data environment." The new version requires that the "perimeter … as well as at critical points inside of the cardholder data environment" be monitored.

Benefit: Areas deemed to be non-critical are not required to be monitored by IDS/IPS sensors, lessening the costs for hardware, software, storage, and monitoring.

Required Proof: The organization must use and be able to demonstrate the evidence of risk-based evaluation of CDE elements to identify which portions are not "critical" and thus required to be monitored by IDS/IPS.

Requirement 12.1 (Security Policy)

12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:

- 12.1.2 Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment

Requirement 12.1 Effect

Impact: Previous versions of the DSS required an annual risk assessment. The requirement now defines examples of acceptable risk assessment frameworks.

Benefit: By implementing an identified framework, the evaluated entity is able to better defend implemented process and controls, minimizing the opportunity for their approach to be deemed insufficient by a QSA.

Required Proof: The organization must choose and implement an approved risk assessment methodology. The foundational controls of this methodology should be used to address all risk-based decision making used to address the DSS.

Requirement 12.8.3 (SP Due Diligence)

12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.

Requirement 12.8.3 Effect

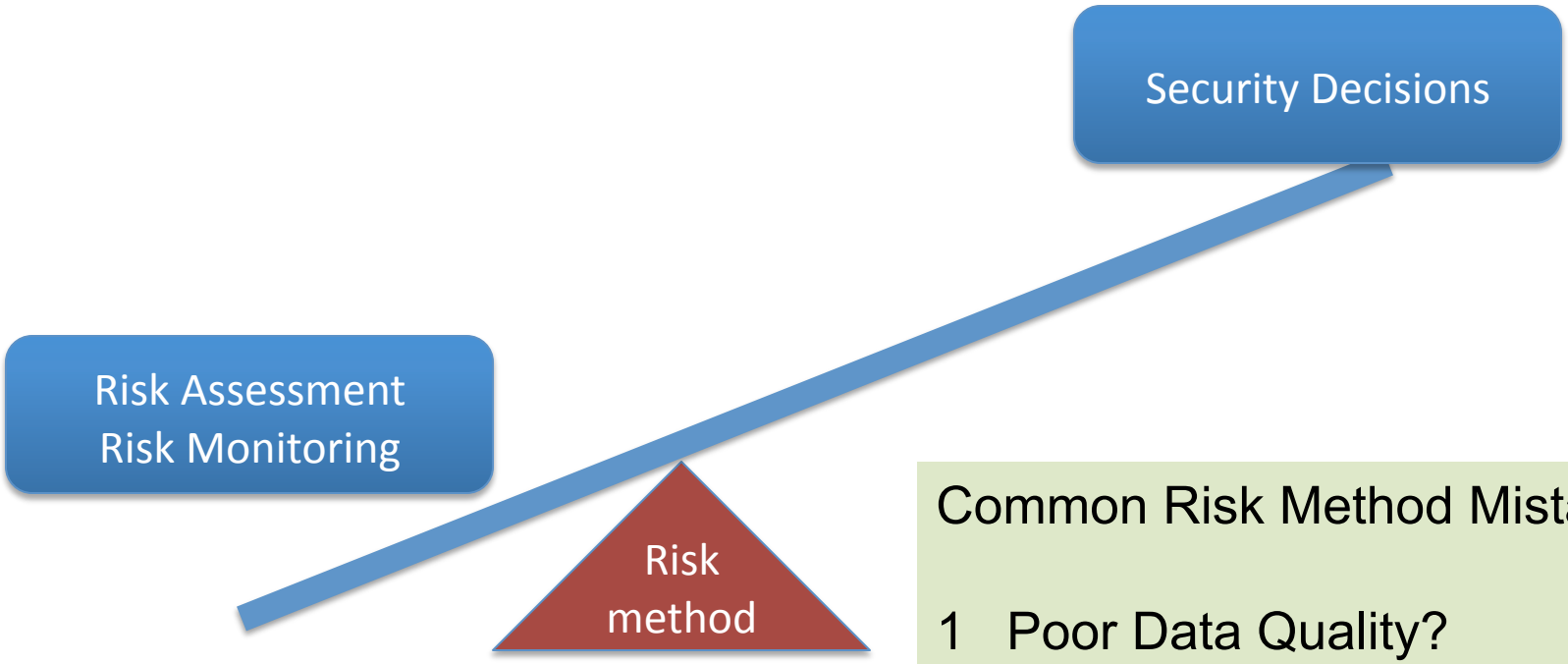
Impact: The selected risk assessment methodology can be used to frame the service provider management due diligence program.

Benefit: While this requirement is not new, it can benefit from the use of an approved methodology used to support existing processes and minimize the likelihood that the service provider management program will be identified as insufficient by a reviewing QSA.

Required Proof: The organization must use the controls established by their chosen methodology to identify, classify, treat, and manage the risks incurred by engaging a service provider.

Aligning Strategy with Business

- Risk – basis of all security decisions



Common Risk Method Mistakes

1 Poor Data Quality?
2 Spreadsheets & Pen Tests?
3 Invalid Equations?

ACCUVANT

Referenced Methods

- Requirements 12.1 Acceptable Methods
  - Not Limited to…
  - OCTAVE
  - ISO 27005
  - NISP SP 800-30

Current SRA Guidance

How <u>exactly</u> do we assess mechanisms?

- *"[Ensure that] the organization's hiring and termination practices for staff take information security issues into account."*
- *"[Assess whether] the organization uniformly enforces its security policies."*
- *"Run Vulnerability Evaluation Tools on Selected Infrastructure Components"*
  - *"[ensure you have the] correct tool...[and the] latest version..."*

ACCUVANT

ISO 31000 Advice

The organization should identify sources of risk, areas of impacts, events and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that might enhance, prevent, degrade or delay the achievement of the objectives. It is also important to identify the risks associated with not pursuing an opportunity. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis. Identification should include risks whether or not their source is under control of the organization.

The organization should apply risk identification tools and techniques which are suited to its objectives and capabilities, and to the risks faced.

Relevant and up-to-date information is important in identifying risks. This should include suitable background information where possible. People with appropriate knowledge should be involved in identifying risks. After identifying what might happen, it is necessary to consider possible causes and scenarios that show what consequences can occur. All significant causes should be considered.

ACCUVANT

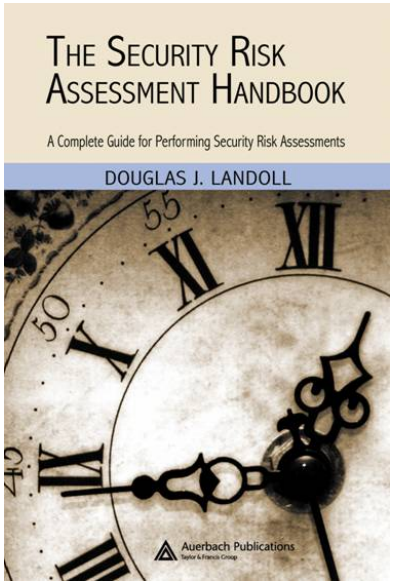
Data Quality Cube: Avoiding GIGO

ACCUVANT

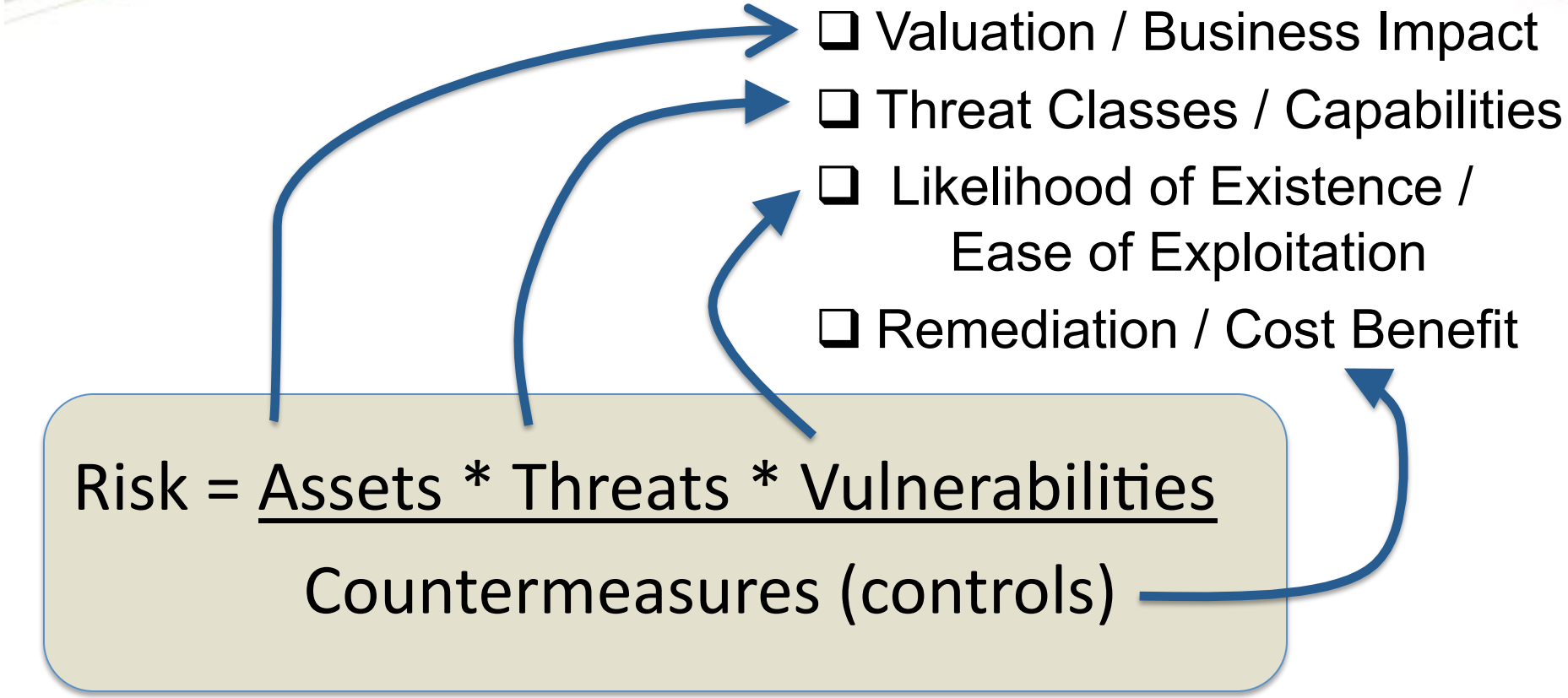
Multiple Data Points: RIIOT Approach to Data Gathering

- Introduced in “Security Risk Assessment Handbook”
- Organizes the task of data gathering on all controls.
- Identifies the 5 methods to data gathering

- Review Documents
- Interview Key Staff
- Inspect Controls
- Observe Behavior
- Test Controls



Risk: Risk Equation



Not Risk Assessments

- Vulnerability Scan
- Penetration Test

- Security Audit
- Compliance Audit

Invalid Equations: Advanced

4 x ★★★★ = 1 ★★★★ ?

ACCUVANT

Invalid Equations: Advanced

- Ordinal Numbers
  - Order but not scale or quantity
  - Ex: 1st place, 2nd place, H, M, L
  - Conclusion: Mathematical operations are invalid
- Cardinal Numbers
  - Order and Scale (size)
  - Ex: $3M, 4 times/yr, 1200 employees, 25 breaches
  - Mathematical operations are valid

ACCUVANT

Invalid Equations: Advanced

System exposure	+	System content	+	System criticality	+	Compromise impact	=	Combined risk score
1-4		1-4		1-4		1-4		4-16

Design Flaw	+	Bad Practice	+	No Mitigating controls	+	Sensitive data	+	Risk of Accidental Exploit	+	Risk of Intentional Exploit	=	Risk Level
1-5		1-5		1-5		1-5		1-5		1-5		6-30

- Invalid Approaches
  1) Mathematical operations with ordinal numbers
  2) "Kitchen sink" approach

ACCUVANT

Qualitative or Quantitative?

- SRA Objective
  1) Determine priority of security initiatives
  2) Demonstrate economic benefit

ACCUVANT

Qualitative Risk Assessment

- Requirements
  1) Quality Data
  2) Solid Approach
     - Proper Scope
     - Calibrated Estimations
- Pros
  - Prioritization of security initiatives
- Cons
  - Inadequate to demonstrate economic benefits

ACCUVANT

Quantitative Risk Assessment

- Requirements
  1) Quality Data
  2) Solid Approach
     - Proper Scope
     - Calibrated Estimations
- Pros
  - Prioritization of security initiatives
  - Adequate to demonstrate economic benefits

ACCUVANT

Proper Scope

- Limitation in What We Assess
  - Failure to measure what appears to be difficult
    - Ex. Intangibles (reputation, morale)
    - Leads to measuring what is easy and many times less valuable data
  - Advice
    - Easier to measure than you think
    - More data than you think
    - Its been done before

ACCUVANT

Contact Information

Doug Landoll,

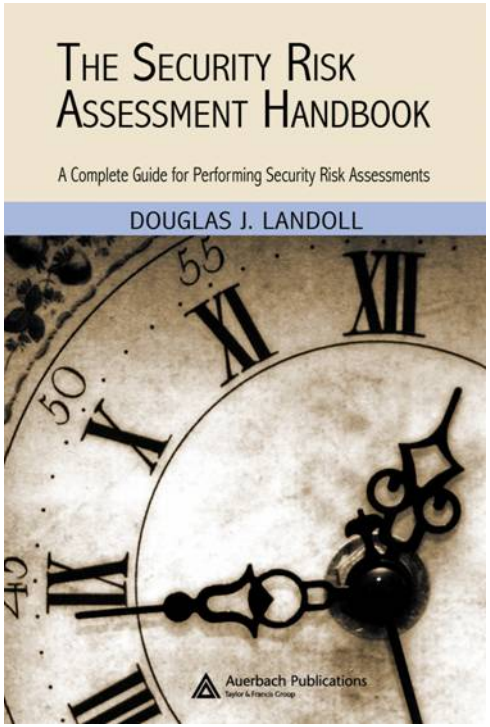
CISSP, CISA, QSA, MBA

Practice Director

Risk and Compliance Management

dlandoll@accuvant.com

(512) 297-2000 office



ACCUVANT

Back Up Slides

Calibrated Estimations

- Inaccurate Measurements
  - Illusion of communication and knowledge
  - "Gut Feel" is wrong – Overconfidence
    - 90% Confidence Interval
      - Havard MBA's **40%**
      - Computer Company Engineers **17%**
  - Advice – Calibration Training
    - 90% Confidence Interval
      - Accuvant RCM Consultants Before **48%**
      - Accuvant RCM Consultants After **84%**

ACCUVANT