



® SISA and CPISI logo are the Registered Trademarks of SISA Information Security

Risk Assessment for PCI 2.0 Requirement 12.1.2 using SMART-RA

Presented by Dharshan Shanthamurthy, SISA Information Security.

SISA Background



- ❖ SISA : **Information Security Specialists**
- ❖ Three Competency Centers namely **Consulting, Training and Products**. Fifteen Intellectual Property Rights in Information Security Space.
- ❖ Headquartered in India with subsidiaries in Delaware-USA, Kuala Lumpur-Malaysia, Manila-Philippines and Bahrain.
- ❖ Customer Footprint in over **21 Countries** spread across Banks, Information Technology, Insurance, Telecom and Retail.
- ❖ Recognized by CERT-India as specialist Information Security firm.

Competency Matrix



Consulting

- PCI QSA Validation Services (PCI-DSS)
- PCI ASV Scanning Services (PCI-DSS)
- PA QSA Validation Services (PA-DSS)
- PCI Assurance Services (SAQ)
- Risk Assessment (IS-RA)
- Privacy and Standards Compliance (ISO 27001, GLBA, HIPAA, DPA, COBIT/FISMA, BS 25999)
- Application Pen Test and Code Review
- Network VA and Pen Test
- Forensics



Training

- OCTAVE (SEI-CMU) Security Risk Assessment Workshop
- Information Security Risk Assessment workshop (CSRA)
- PCI DSS Implementation Workshop (CPISI)
- ISO 27001 Implementation Workshop
- Business Continuity Management Workshop
- Secure Coding in Dot-Net
- Awareness Sessions



Products

- SMART-RA.COM
- MANAGEPCI.COM
- DDT (Data Discovery Tool)
- SISASMART IT-GRC
- SISASMART Audit Management Tool
- SISASMART Survey Management

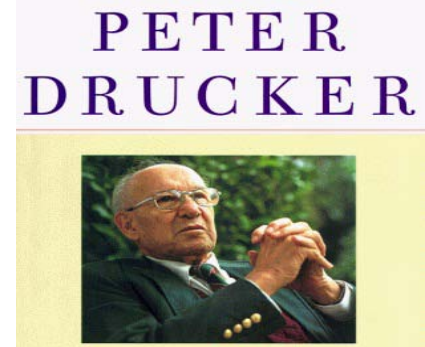
Over 100 Workshops.....



Definition

Risk assessment is the **cornerstone** of any information security program, and it is the **fastest** way to gain a complete understanding of an **organization's** security profile – its **strengths** and **weaknesses**, its **vulnerabilities** and **exposures**.

**“IF YOU CAN’T MEASURE IT
...YOU CAN’T MANAGE IT!”**



Need for IS-RA

- PCI DSS
- ISO 27001 (ISMS)
- HIPAA
- GLBA
- IT Act
- OECD
- FISMA
- FISAP
-

Countries	Equivalent Standard
 Australia	AS/NZS ISO/IEC 27002:2006
 New Zealand	
 Brazil	ISO/IEC NBR 17799/2007 - 27002
 Chile	NCH2777 ISO/IEC 17799/2000
 Czech Republic	ČSN ISO/IEC 27002:2006
 Denmark	DS484:2005
 Estonia	EVS-ISO/IEC 17799:2003, 2005 version in translation
 Japan	JIS Q 27002
 Lithuania	LST ISO/IEC 27002:2009 (adopted ISO/IEC 27002:2005, ISO/IEC 17799:2005)
 Netherlands	NEN-ISO/IEC 17799:2002 nl, 2005 version in translation
 Poland	PN-ISO/IEC 17799:2007, based on ISO/IEC 17799:2005
 Peru	NTP-ISO/IEC 17799:2007
 South Africa	SANS 17799:2005
 Spain	UNE 71501
 Sweden	SS 627799
 Turkey	TS ISO/IEC 27002
 United Kingdom	BS ISO/IEC 27002:2005
 Uruguay	UNIT/ISO 17799:2005
 Russia	ГОСТ/Р ИСО МЭК 17799-2005
 China	GB/T 22081-2008

Risk Assessment in PCI 2.0-

Requirement 12.1.2

- Requirement 12.1.2 emphasizes the need for a structured and formal risk assessment methodology.

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

Requirement 12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment. (Examples of risk assessment methodologies include but are not limited to **OCTAVE, ISO 27005 and NIST SP 800-30.**)”

Challenges in Risk Assessment

Challenge	Consequence
Lack of a Structured, Organized and approved risk assessment methodology.	<ul style="list-style-type: none">•Risk Assessment is conducted in a chaotic, haphazard and incorrect manner.•Comprehensive coverage of assets, threats and controls is lost.
Lack of Automation.	<ul style="list-style-type: none">•Human involvement is increased.•Scope of error rises.
Unwarranted complexity.	<ul style="list-style-type: none">•More time is spent on understanding the risk assessment methodology than in implementing it.•Training spend increases in terms of time and money.
Inadequate reporting functionality.	Senior management is not happy.
Ineffective measurement metrics.	Risk Assessment becomes inaccurate or insufficient.

Meet Requirement 12.1.2 with SMART



Acknowledging the importance of risk assessment, SISA has developed SMART – Security Management and Risk Assessment Tool.

Features

SMART is adherent to OCTAVE, ISO 27005 and NIST SP 800-30.

Multi Purpose Tool: SMART enables compliance with ISO 27001, PCI DSS, HIPAA, FISMA, FISAP and GLBA.

Extensible and Scalable: SMART can be deployed effectively for organizations of varied size and complexity and on multiple environments.

Fully Automated: SMART is the first product of its kind that provides automated implementation of Information Security compliance.

Asset Information

Page
Safety
Tools

SMART Launch

General Information

Risk Assessment

Asset Information

Define Threats

Threat Profiles

Action Register

Administration

Reports

Dashboard

Logout

ASSET INFORMATION

* Asset Name : Card Information

* Asset Owner : Card Operations

* Asset Description : Card Information includes credit card, debit card and the charge card information which is stored at various locations for eg in the applicationdatabases (Phoenix and CMS) and includes the card holder name , expiry date , and sensitive authentication data like CVV and

Building	Address	ZipCode	City	Country	Select	Action
IT Center 1			Bangalore		<input type="checkbox"/>	Add Del
IT Center 2			Bangalore		<input type="checkbox"/>	Add Del
IT Center 4			Mumbai		<input type="checkbox"/>	Add Del
IT Center 3			Chennai		<input checked="" type="checkbox"/>	Add Del

Threats



User Name: smart-mr
Company Name: Demo Technologies
Role: MR

SMART Launch

[Dashboard](#)

[Logout](#)

- General Information
- Risk Assessment**
 - [Asset Information](#)
 - [Define Threats](#)**
 - [Threat Profiles](#)
 - [Action Register](#)
- Administration
- Reports

AREA OF CONCERNS

* Threat Name : InternetApplication logs capture PAN info

Threat Probability : High

* Threat :
Description : If logging is enabled the PAN information gets captured in the application logs

* Threat Outcome :
☐ Loss of Integrity
☒ Loss of Confidentiality
☐ Loss of Availability

* Threat Access : Network

* Threat Actor : Human Insider

Threat Motive : Deliberate

Asset Name	Asset Locations	Select	Action
Card Information	Chennai-IT Center 3	<input type="checkbox"/>	Add Del
Card Information	Chennai-IT Center 3	<input type="checkbox"/>	Add Del
Card Information	Mumbai-IT Center 4	<input type="checkbox"/>	Add Del
Card Related Information	Mumbai-IT Center 4	<input type="checkbox"/>	Add Del
Cardholder Data	Bangalore-IT Center 1	<input type="checkbox"/>	Add Del

Save

Cancel

Threat Profile







User Name: smart-mr
Company Name: Demo Technologies
Role: MR

SMART Launch

Dashboard

Logout

- General Information
- Risk Assessment
 - Asset Information
 - Define Threats
 - Threat Profiles**
 - Action Register
- Administration
- Reports

Location	Assets	Threat Outcome	Impact	Probability	Risk	Risk Treatment Plan	Action Item
--ALL Locations--	Cardholder Data	Loss of Confidentiality	High	High	High	<input checked="" type="checkbox"/> Treat <input type="checkbox"/> Transfer <input type="checkbox"/> Terminate <input type="checkbox"/> Tolerate	
		Loss of Integrity	Medium	High	High	<input checked="" type="checkbox"/> Treat <input checked="" type="checkbox"/> Transfer <input type="checkbox"/> Terminate <input type="checkbox"/> Tolerate	
		Loss of Integrity	Please select	High			
		Loss of Confidentiality	Medium	Medium	Medium	<input checked="" type="checkbox"/> Treat <input type="checkbox"/> Transfer <input type="checkbox"/> Terminate <input type="checkbox"/> Tolerate	
		Loss of Confidentiality	High	High	High	<input checked="" type="checkbox"/> Treat <input type="checkbox"/> Transfer <input type="checkbox"/> Terminate <input type="checkbox"/> Tolerate	

Benefits

- SMART will reduce compliance time for your organization by 50%.
- SMART implements only the necessary controls for a threat. This significantly cuts your compliance costs.
- SMART is automated to the extent that documentation and human involvement are significantly reduced.
- SMART is designed with the vision of empowering zero background knowledge in implementing compliance.

Thank You

Dharshan Shanthamurthy,

CISA, CISSP, PCI QSA, ISO 27001 LA, CEH, FCA, ISA, OCTAVE Authorized Trainer/Advisor, PA-QSA, Dip (ASP.NET)

E-mail: dhharshan.shanthamurthy@sisa.in

Phone: +91-99451 22551

URL: www.sisa.in