S21sec

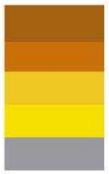
La seguridad digital del futuro, hoy

CISCO

*[Auditing PCI-DSS]

Antonio Ramos,
Consultancy Director
Lisboa, 3th April 2008

CONTENTS



- Company presentation: **S21sec**
- Requirements established by PCI DSS.
- Compliance with PCI DSS:
  - Financial Entities.
  - Merchants.
  - Service Providers.
- Scope.
- Auditing Process.
- PCI DSS Service Compliance.

CISCO S21sec

S21SEC, COMPUTER SECURITY SERVICES

- Spanish company exclusively dedicated to Information Security.
  - **“Mission: Prevent and manage the risk to organisations and people in their digital lives.”**

- **Clients:**
  - Present in 25 of the IBEX 35 companies.
  - 20% of European Eurostoxx 50 index.
  - 90% of Spanish financial sector.
  - Public Administrations bodies and institutions.
  - Main telecommunications companies.
  - E-commerce, utilities and construction companies.
  - Major national airlines and transport & logistics companies.
  - Defence and Security Forces.
  - Health Sector.

7 offices in Spain
3 international offices

The largest Digital Security team in Spain: 200 specialists

CISA – Certified Information Systems Auditor

CISSP – Certified Information Systems Security Professional

GIAC – Global Information Assurance Certification

CISM – Certified Information Security Manager

Microsoft

An Integral Management model for 24x7 Security

WHAT MAKES US DIFFERENT

S21sec labs

La seguridad digital del futuro, hoy

Committed to innovation from the start. First R+D+i centre in Europe

PCI Security Standards Council

AENOR ER Empresa Registrada UNE-EN ISO 9001

IQNet

AENOR ER Gestión I+D+i UNE 166002

AENOR ER Seguridad Información UNE 71502

AENOR ER Capacidad Software 1 ISO/IEC 15504

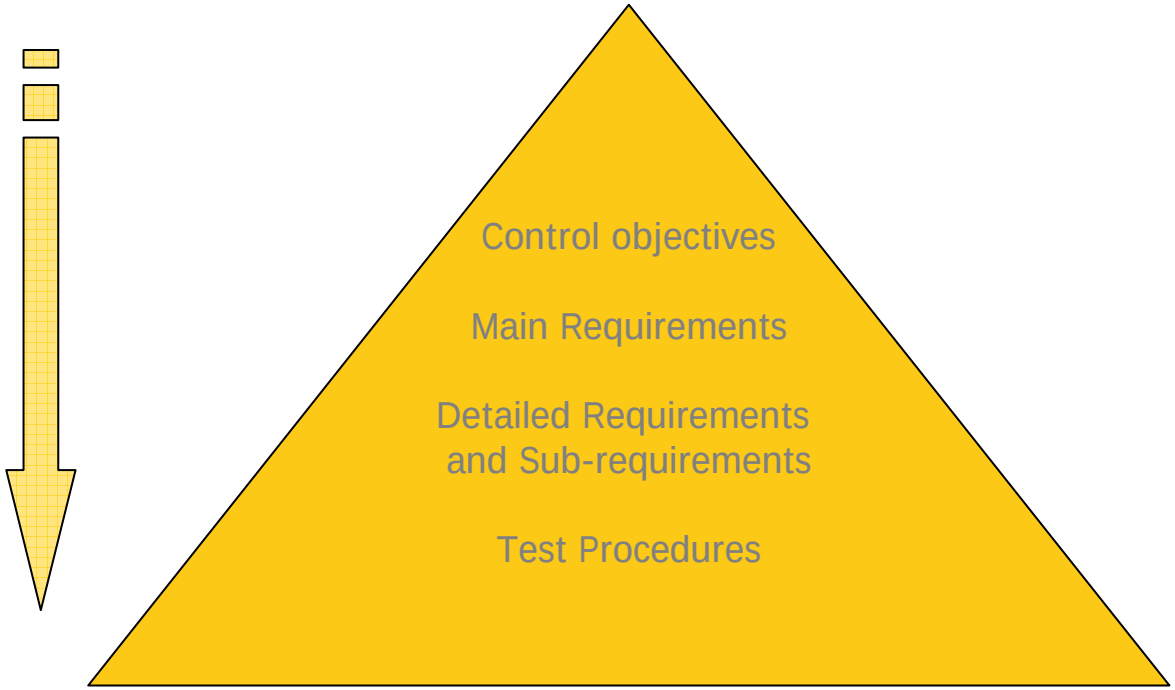
And into the future, with quality and certificates

BUSINESS LINES

- SERVICES
  - Technical assessment
  - Consultancy
  - Digital Surveillance
  - Fraud and intelligence
  - Managed Security
  - Training
- PRODUCTS
  - SIEM
  - Vulnerabilities database

REQUIREMENTS SET BY PCI DSS

- The PCI DSS standard is structured around the four levels which are described in the graph below.
- The level of detail increases as we work down.

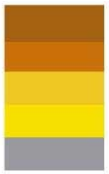


REQUIREMENTS SET BY PCI DSS

- The Control Objectives set in PCI DSS are given below:

A. Build and maintain a secure network.
B. Protect cardholder data.
C. Maintain a vulnerability management program.
D. Implement strong access control measures.
E. Regularly Monitor and test networks.
F. Maintain an Information Security Policy.

PCI DSS COMPLIANCE : FINANCIAL ENTITIES



- All Visa or MasterCard members must comply with PCI DSS. They are responsible for security within their own systems.
- Issuer or adquiring members are not required to validate their compliance, except that they are also acting as service providers.
- The purchasing banks are in charge of guaranteeing:
  - PCI DSS compliance from their businesses.
  - PCI DSS compliance from all their service providers through which they or their merchants, process or transmit information on card payments.
- In the case of Visa and MasterCard, the adquiring bank will take on any responsibility which could be incurred from non compliance with card brand compliance programs.

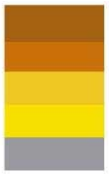
CISCO S21sec

PCI DSS COMPLIANCE: MERCHANTS

- All merchants which accept card payments must comply with PCI DSS, but only certain merchants must validate their compliance, depending on their volume of transactions.
- Visa and MasterCard classify maerchants which accept card payments into four levels, depending on the number of transactions they carry out on a yearly basis.

Category	Description	Validation requirements
Level 1	▪ Any merchant processing over 6,000,000 VISA or MasterCard transactions per year (regardless of the acceptance channel). ▪ Any merchant that has suffered an attack that resulted in an account data compromise in the past year. ▪ Any merchant identified by another payment card brand as a Level 1	▪ Annual on-site Security Audit (carried out by a Qualified Security Assessor - QSA). ▪ Quarterly network scans (carried out by an Approved Scanning Vendor - ASV)
Level 2	▪ Any merchant processing between 1,000,000 and 6,000,000 Visa or MasterCard transactions per year (regardless of the acceptance channel).	▪ Annual Self-assessment questionnaire (carried out by the merchant) ▪ Quarterly network scans (carried out by an Approved Scanning Vendor - ASV)
Level 3	▪ Any merchant processing between 20,000 and 1,000,000 VISA or MasterCard transactions over the Internet per year.	
Level 4	▪ Any merchant processing less than 20,000 transactions over the Internet per year. ▪ Remaining merchants processing up to 1,000,000 VISA or Mastercard transactions per year.	▪ Annual Self-assessment questionnaire (carried out by the merchant) ▪ Quarterly network scans (carried out by an Approved Scanning Vendor - ASV)

PCI DSS COMPLIANCE: SERVICE PROVIDERS



- All card brands require service providers to comply with PCI DSS requirements.
- Validation and compliance requirements vary depending on the different card brands.
- Visa and MasterCard: They classify service providers according to the volume of transactions and/or type of service provider.
- American Express, Discover and JCB: They do not classify service providers according to the volume of transactions. All service providers must comply with PCI DSS.

PCI DSS COMPLIANCE: SERVICE PROVIDERS

- Levels Defined and Validation Requirements.
  - VISA

Category	Description	Validation Requirements
Level 1	All VisaNet processors, payment gateways and Internet payment service providers (regardless of transactions volume).	▪ Annual On-site Security Audit (carried out by a Qualified Security Assessor - QSA). ▪ Quarterly network scans (carried out by an Approved Scanning Vendor - ASV).
Level 2	Any service provider that is not in Level 1 and stores, processes or transmits more than 1,000,000 VISA accounts / transactions annually.	
Level 3	Any service provider that is not Level 1 and stores, processes or transmits less than 1,000,000 VISA accounts / transactions annually.	▪ Annual Self-assessment questionnaire (carried out by the service provider). ▪ Quarterly network scans (carried out by an Approved Scanning Vendor - ASV).

PCI DSS COMPLIANCE: SERVICE PROVIDERS

- MasterCard

Category	Description	Validation Requirements
Level 1	▪ All TPPs (Service Providers -Third Party Processors) ▪ All DSEs (Data Storage Entities) which store account information for Level 1 or Level 2 Businesses.	▪ On-site Security Audit (carried out by a Qualified Security Assessor - QSA). ▪ Quarterly network scans (carried out by an Approved Scanning Vendor - ASV).
Level 2	▪ All DSEs which store account information for Level 3 Businesses.	
Level 3	▪ The remaining DSEs which are not included in Levels 1 and 2.	▪ Quarterly network scans (carried out by an Approved Scanning Vendor - ASV).

SCOPE OF PCI DSS

- Who must comply with PCI DSS?
  - Financial entities (who only have to validate their compliance in the event that they act as service providers).
  - Service providers which store, process and/or transmit information on cardholders.
  - Merchants which store, process and/or transmit information on cardholders.

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

** These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS; however, does not apply if PANs are not stored, processed, or transmitted.*

*** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).*

cisco S21sec

SCOPE OF PCI DSS

- The scope of PCI DSS includes all systems which store, process or transmit information on credit or debit cards.

- The cardholders' environment is the part of the network which processes cardholders' data or sensitive authentication data. This includes all system components:
  - Servers: web, database, authentication, mail, proxy, NTP, DNS...
  - Applications
  - Network devices: firewalls, switches, routers, wireless access points, network appliances...

- When third parties are involved in processing, each *service provider* is responsible for their own compliance (aside from contractual obligations).

- PCI DSS is therefore applied to the different channels for transmitting card data (Physical TPV, Virtual TPV,...)

SCOPE OF PCI DSS

- Defining the scope is a critical moment in the audit process.
  - Adequate network segmentation, which isolates systems which store, process or transmit cardholder data from the rest of the network may reduce the scope of the audit.
  - The QSA must verify that the segmentation is adequate to reduce the scope of the audit.

- The scope of annual onsite reviews includes:
  - All external connections into the merchant network, such as employee remote access, third party access for processing and maintenance or payment card company.
  - All connections to and from the authorization and settlement environment.
  - Any data repository outside the authorization and settlement environments which stores more than 500,000 account numbers (NOTE: Not falling within the scope does not mean that it must not comply with the standard).
  - The Point of Sales systems (POS – *Point of Sales*), if there is any type of external access to the business location by any means (Internet, virtual private network, dial-in, broadband, or publicly accessible machines such as kiosks).

AUDITING PROCESS

AUDITING PROCESS

- Scope validation

- Sampling
  - Sampling techniques can be used to run audit procedures.
  - The sample must be a representative selection of all of the types of system components and include a variety of operating systems, functions and applications into the scope.
  - When selecting samples of merchants' stores or for franchised merchants:
    - If there are standardised processes, the size of the sample can be reduced.
    - If there are several types of processes, the sample must include processes for each of them.
    - If there are no standardised processes, the sample must be larger to be able to assure whether each location understands and implements PCI DSS requirements properly.

- Compensating controls
  - They must be considered when an entity cannot comply with the technical specification for a requirement but mitigates the associated risk sufficiently.
  - Effectiveness depends on many factors which mean they must be assessed individually (the inspection environment, the system in general, its definition and configuration...)

AUDITING PROCESS

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
	to its contents			
9.10.2 Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed	**9.10.2** Verify that electronic media is destroyed beyond recovery by using a military wipe program to delete files, or via degaussing or otherwise physically destroying the media			

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	**10.1** Verify through observation and interviewing the system administrator, that audit trails are enabled and active, including for any connected wireless networks.			
10.2 Implement automated audit trails for all system components to reconstruct the following events:	**10.2** Verify though interviews, examination of audit logs, and examination of audit log settings, that the following events are logged into system activity logs:			
10.2.1 All individual accesses to cardholder data	**10.2.1** All individual access to cardholder data			
10.2.2 All actions taken by any individual with root or administrative privileges	**10.2.2** Actions taken by any individual with root or administrative privileges			
10.2.3 Access to all audit trails	**10.2.3** Access to all audit trails			

PCI DSS COMPLIANCE SERVICE

- **S21sec** is certified as:
  - Qualified Security Assessor Company (QSAC) to run on-site audits (with three certified professionals).
  - Approved Scanning Vendor (ASV) to run quarterly network scans.

- The services provided by **S21sec** to help organisations guarantee PCI DSS compliance are as follows:
  - Annual on-site audits.
  - Quarterly network scans.

- **S21sec** was the first Spanish company to be certified to provide PCI DSS compliance services in Europe and LATAM.

PCI DSS COMPLIANCE SERVICE

- **S21sec** can, additionally, help to implant other security measures which are required to guarantee PCI DSS compliance:
  - Expert assessment on the matter: Definition of the compliance strategy.
  - Permitting compliance with monitoring requirement 10.
  - Equipping a company with a vulnerabilities information system.
  - Running code reviews on the necessary applications.
  - Defining policies, standards and procedures in line with the standard (including secure configuration guides, managing key public infrastructures– PKI, or SDLC).
  - Providing equipment for secondary authentication factors.
  - Providing device management services securely (and remotely).

S21sec

La seguridad digital del futuro, hoy

CISCO

*[Thank you]

info@s21sec.com

Tel.+34 902 222 521