Information Security Standards Review

GDPR (General Data Protection Regulation

ISO27002

PCI DSS (Payment Card Industry Data Security Standard

Data Protection and Cyber Security Research and Development Center

25th of May
2018
THE GENERAL DATA PROTECTION REGULATION IS COMING FAST:
WILL YOU BE READY FOR 2018?

GDPR

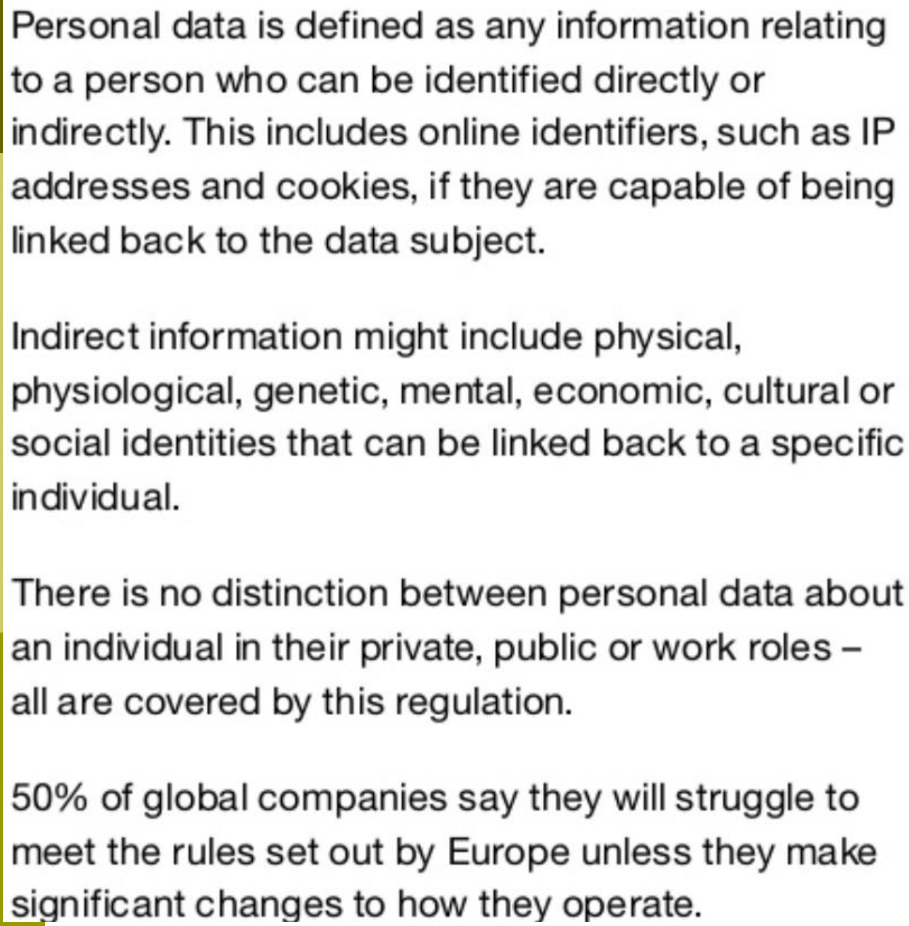
After four years of debate, the General Data Protection Regulation (GDPR) was ratified by the European Union during April 2016 and has now become law, although member states have a two-year period to implement it into national law.

This means that companies will be expected to be fully compliant from **25 May 2018**. The regulation is intended to establish one single set of data protection rules across Europe.

Organisations outside the EU are subject to this regulation when they collect data concerning any EU citizen.

GDPR is designed to give individuals better control over their personal data held by organisations, and may lead many to appoint a Data Protection Officer.

GDPR



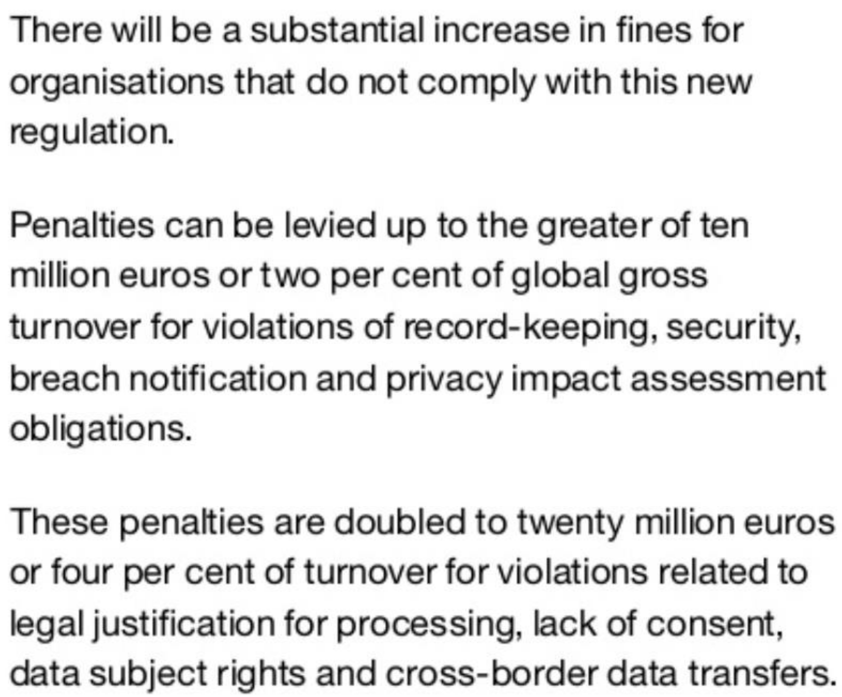
Personal data is defined as any information relating to a person who can be identified directly or indirectly. This includes online identifiers, such as IP addresses and cookies, if they are capable of being linked back to the data subject.

Indirect information might include physical, physiological, genetic, mental, economic, cultural or social identities that can be linked back to a specific individual.

There is no distinction between personal data about an individual in their private, public or work roles – all are covered by this regulation.

50% of global companies say they will struggle to meet the rules set out by Europe unless they make significant changes to how they operate.

GPDR



There will be a substantial increase in fines for organisations that do not comply with this new regulation.

Penalties can be levied up to the greater of ten million euros or two per cent of global gross turnover for violations of record-keeping, security, breach notification and privacy impact assessment obligations.

These penalties are doubled to twenty million euros or four per cent of turnover for violations related to legal justification for processing, lack of consent, data subject rights and cross-border data transfers.

GPDR

Companies will be required to "implement appropriate technical and organisational measures" in relation to the nature, scope, context and purposes of their handling and processing of personal data. Data protection safeguards must be designed into products and services from the earliest stages of development.

These safeguards must be appropriate to the degree of risk associated with the data held and might include:

- Pseudonymisation and/or encryption of personal data
- Ensuring the ongoing confidentiality, integrity, availability and resilience of systems
- Restoring the availability of, and access to, data in a timely manner following a physical or technical incident
- Introducing a process for regularly testing, assessing and evaluating the effectiveness of these systems.

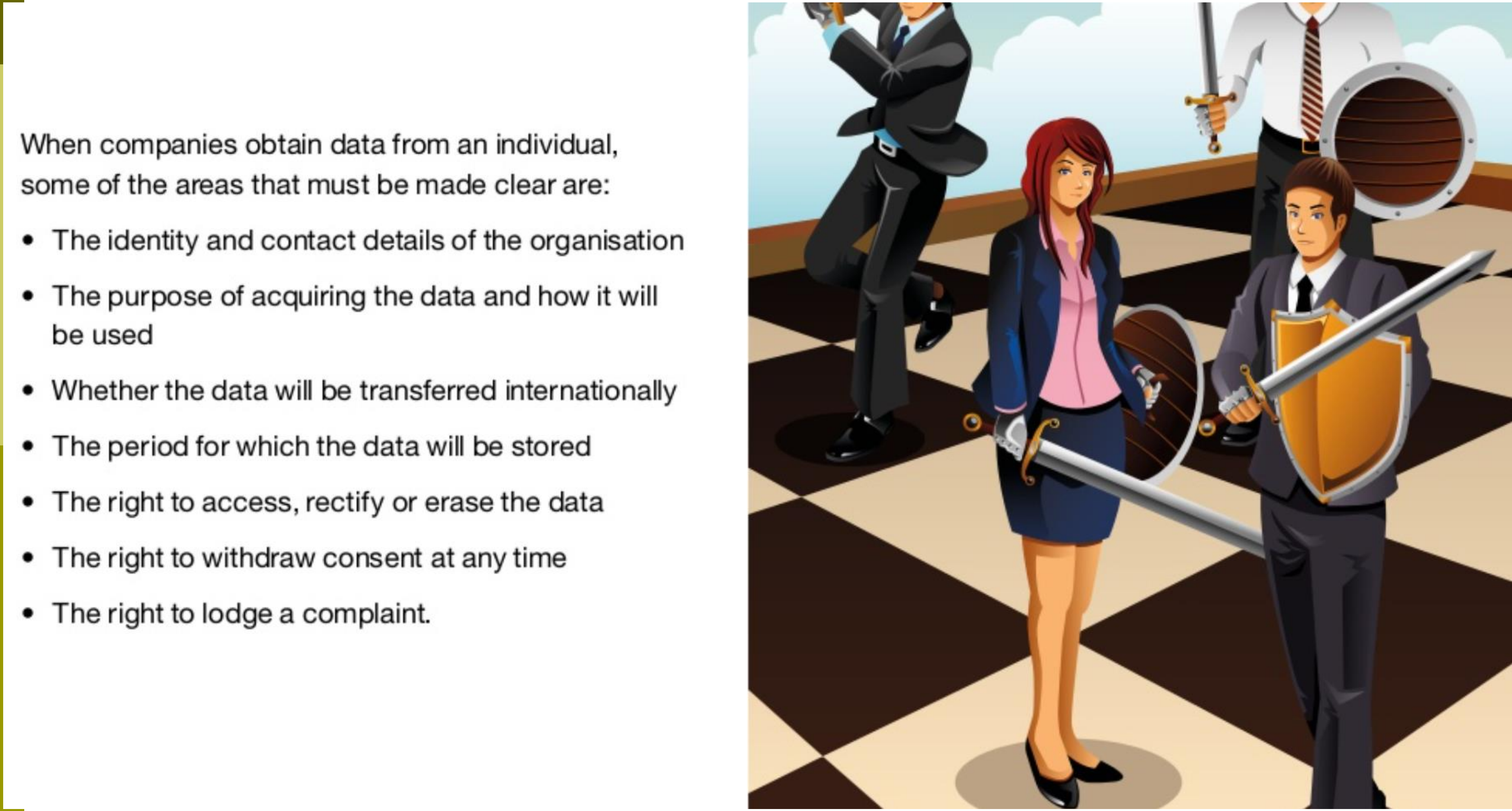
GPDR

A key part of the regulation requires consent to be given by the individual whose data is held. Consent means "any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed".

Organisations will need to be able to show how and when consent was obtained. This consent does not need to be explicitly given, it can be implied by the person's relationship with the company. However, the data obtained must be for specific, explicit and legitimate purposes.

Individuals must be able to withdraw consent at any time and have a right to be forgotten; if their data is no longer required for the reasons for which it was collected, it must be erased.

GPDR



When companies obtain data from an individual, some of the areas that must be made clear are:

- The identity and contact details of the organisation
- The purpose of acquiring the data and how it will be used
- Whether the data will be transferred internationally
- The period for which the data will be stored
- The right to access, rectify or erase the data
- The right to withdraw consent at any time
- The right to lodge a complaint.

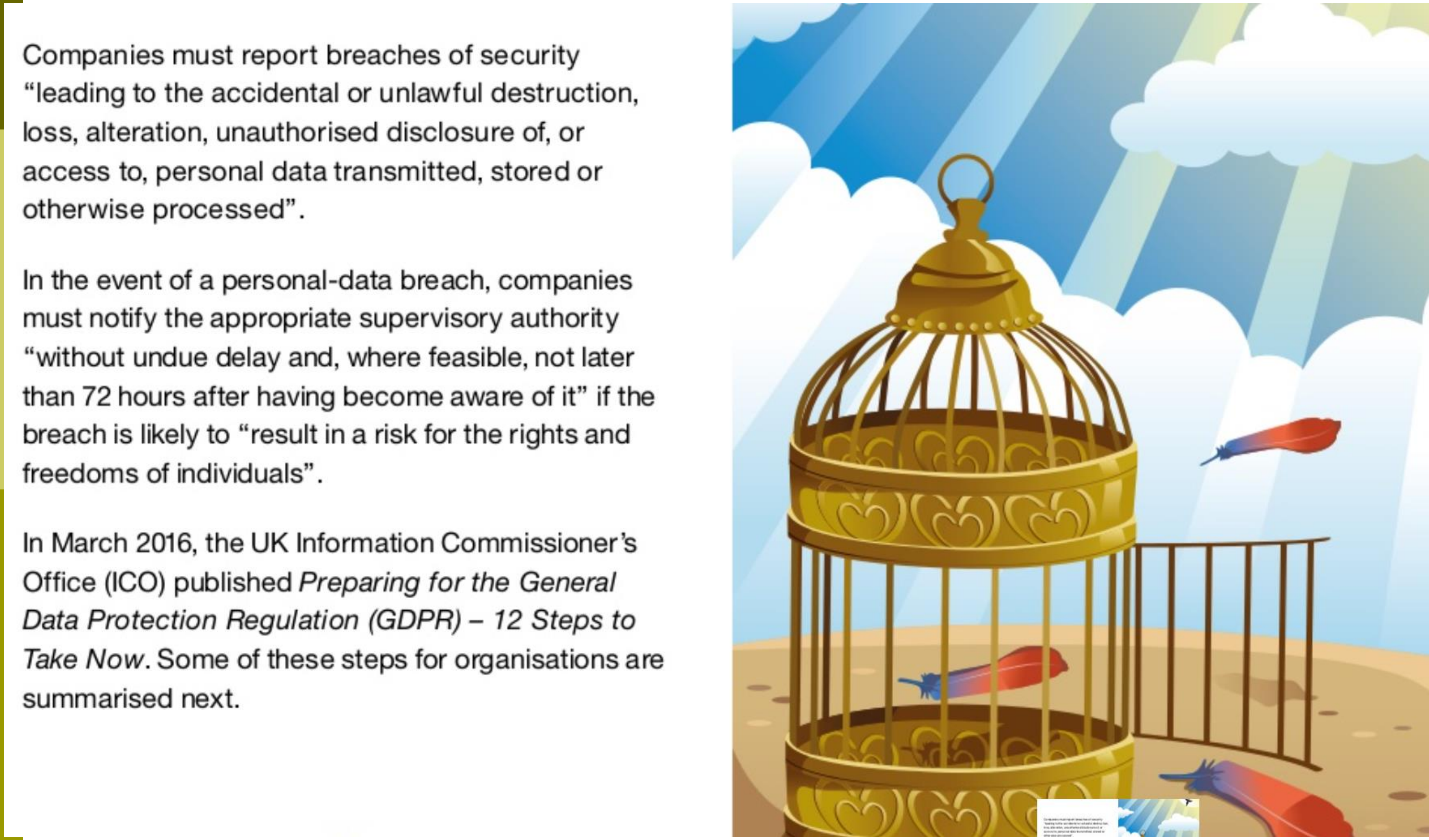
GPDR

The regulations demand that individuals must have full access to information on how their data is processed and this information should be available in a clear and understandable way.

Individuals can make requests, and these must be executed “without undue delay and at the latest within one month of receipt of the request”.

Where requests to access data are manifestly unfounded or excessive then small and medium-sized enterprises will be able to charge a fee for providing access.

GDPR



Companies must report breaches of security "leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

In the event of a personal-data breach, companies must notify the appropriate supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it" if the breach is likely to "result in a risk for the rights and freedoms of individuals".

In March 2016, the UK Information Commissioner's Office (ICO) published *Preparing for the General Data Protection Regulation (GDPR) – 12 Steps to Take Now*. Some of these steps for organisations are summarised next.

GDPR

1. Ensure key departments are aware that the law is changing, and anticipate the impact of GDPR.
2. Document what personal data is held, where it came from and with whom it is shared.
3. Review current privacy notices, and make any necessary changes.
4. Review procedures to address the new rights that individuals will have.
5. Plan how to handle requests within the new time frames, and provide the required information.
6. Identify and document the legal basis for each type of data processing activity.
7. Review how consent is sought, obtained and recorded.
8. Make sure procedures are in place to detect, report and investigate data breaches.
9. Designate a Data Protection Officer to take responsibility for data protection compliance.

Preparing for the General Data Protection Regulation (GDPR)

12 steps to take now

1 Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5 Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7 Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8 Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9 Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11 Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12 International

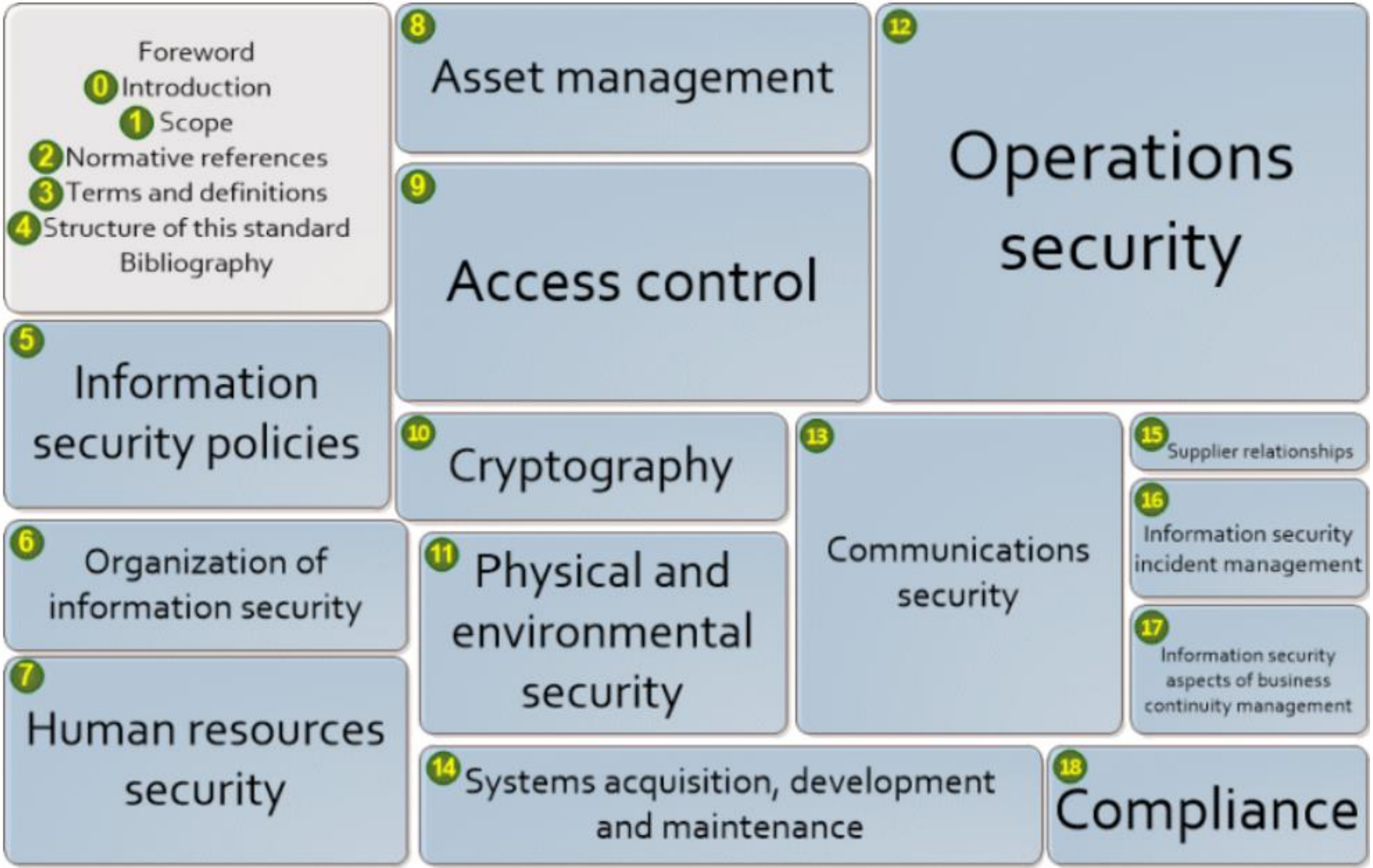
If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

ISO/IEC 27002:2013

Question: How to Ensure Secure Organisational Infrastructure and Manage Long Life Learning Staff?

Answer: Implement ISO/IEC 27002:2013 Standard Complient Informational Security Management System (ISMS)!

ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls



Foreword

0 Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Structure of this standard

Bibliography

5 Information security policies

6 Organization of information security

7 Human resources security

8 Asset management

9 Access control

10 Cryptography

11 Physical and environmental security

12 Operations security

13 Communications security

14 Systems acquisition, development and maintenance

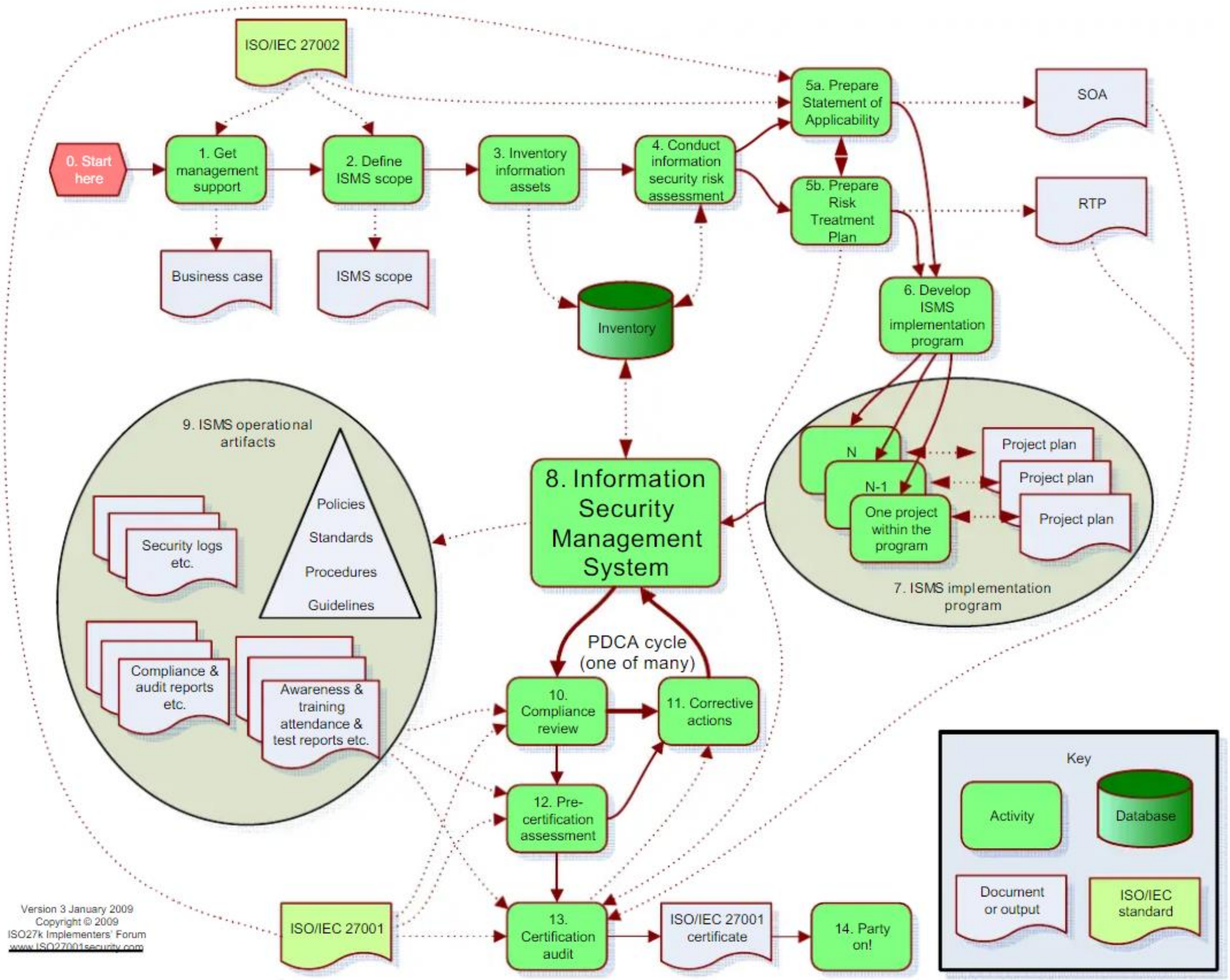
15 Supplier relationships

16 Information security incident management

17 Information security aspects of business continuity management

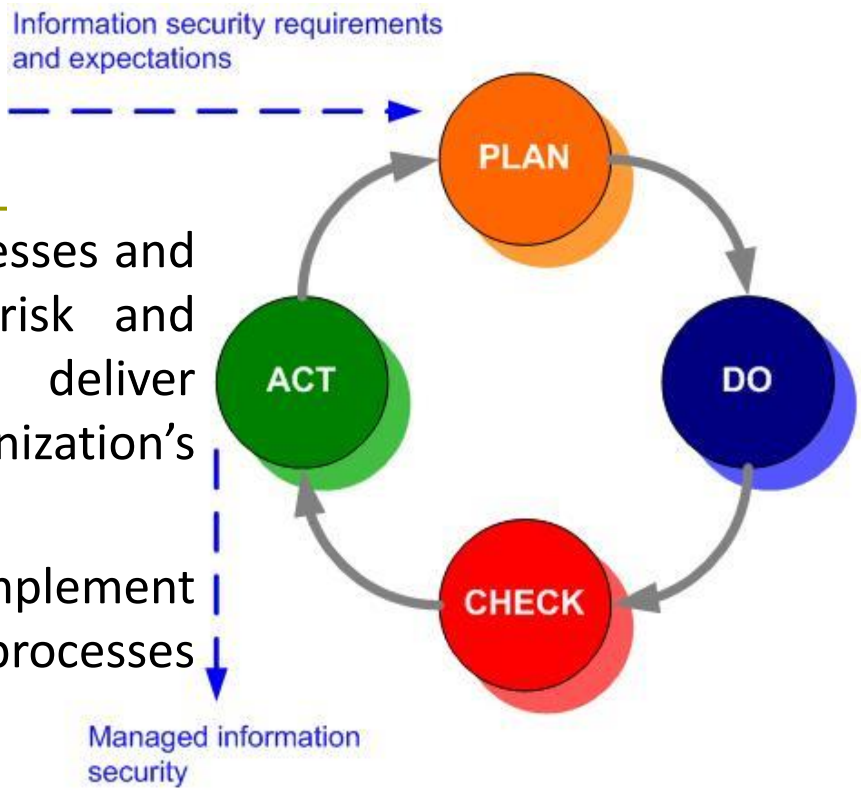
18 Compliance

ISMS Implementation and Certification Process


ISO/IEC 27002
0. Start here
1. Get management support
2. Define ISMS scope
3. Inventory information assets
4. Conduct information security risk assessment
5a. Prepare Statement of Applicability
5b. Prepare Risk Treatment Plan
SOA
RTP
Business case
ISMS scope
Inventory
6. Develop ISMS implementation program
9. ISMS operational artifacts
Policies
Standards
Procedures
Guidelines
Security logs etc.
Compliance & audit reports etc.
Awareness & training attendance & test reports etc.
8. Information Security Management System
N
N-1
One project within the program
Project plan
Project plan
Project plan
7. ISMS implementation program
PDCA cycle (one of many)
10. Compliance review
11. Corrective actions
12. Pre-certification assessment
13. Certification audit
ISO/IEC 27001
ISO/IEC 27001 certificate
14. Party on!
Key
Activity
Database
Document or output
ISO/IEC standard

Version 3 January 2009
Copyright © 2009
ISO27k Implementers' Forum
www.ISO27001security.com

PDCA Model


Information security requirements and expectations
PLAN
DO
CHECK
ACT
Managed information security

- Plan (establish the ISMS)
  - Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
- Do (implement and operate the ISMS) Implement and operate the ISMS policy, controls, processes and procedures.
- Check (monitor and review the ISMS)
  - Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
- Act (maintain and improve the ISMS)
  - Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS Introduction

- + Started in 2001 as separate programs
  - ▪ Cardholder Information Security Program (Visa USA)
    ▪ Account Information Security (Visa INTL)
    ▪ Site Data Protection (SDP) Program (MasterCard)

- Standards consolidated December 15, 2004 under the naming of the **Payment Card Industry (PCI) Data Security Standard(DSS)**

- The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

PCI DSS Main Requirements Groups

Build and Maintain a Secure Network
Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data
Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt transmission of cardholder data across open, public networks

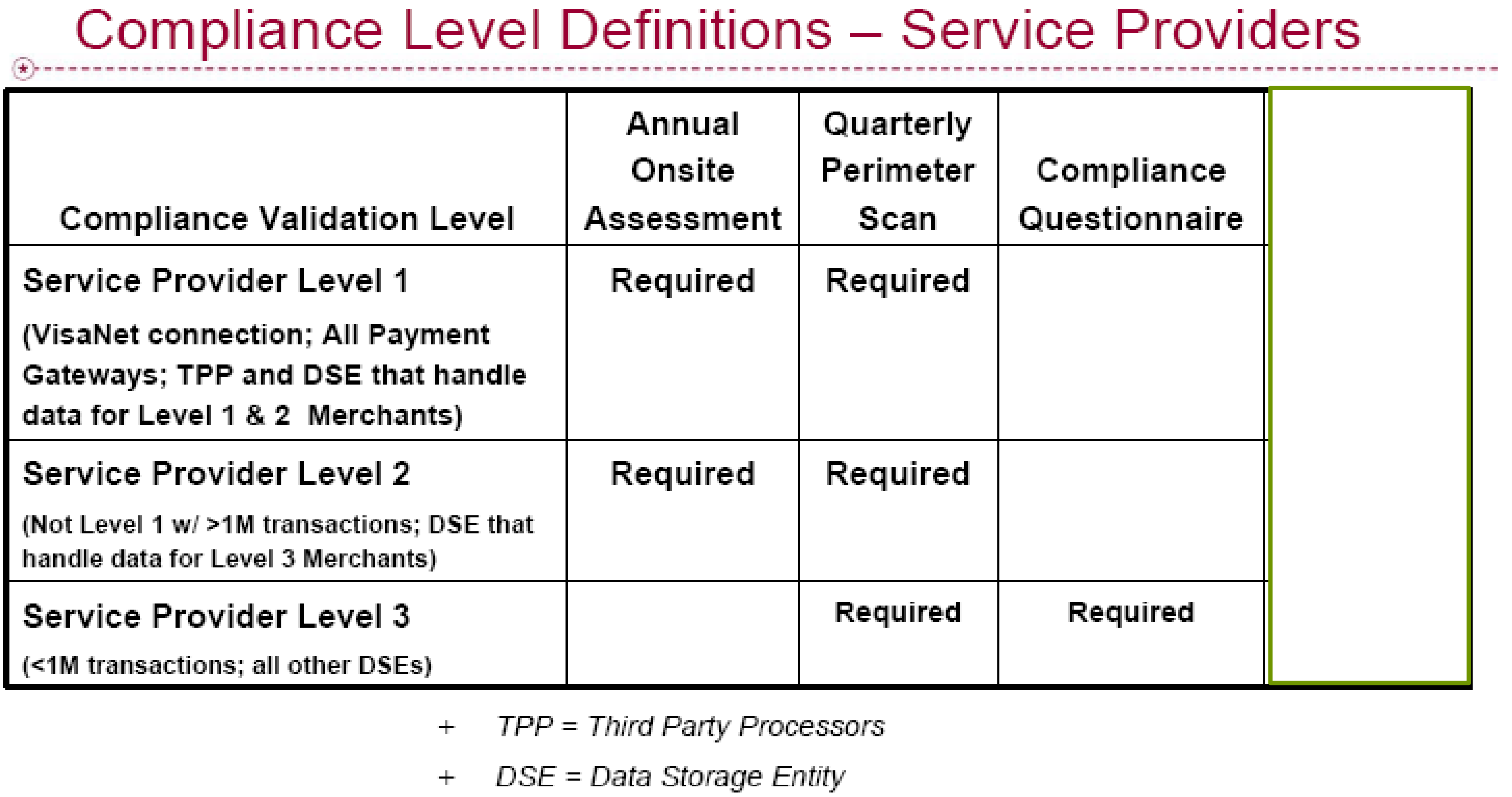
Maintain a Vulnerability Management Program
Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures
Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks
Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy
Requirement 12: Maintain a policy that addresses information security

PCI DSS requirements for service providers

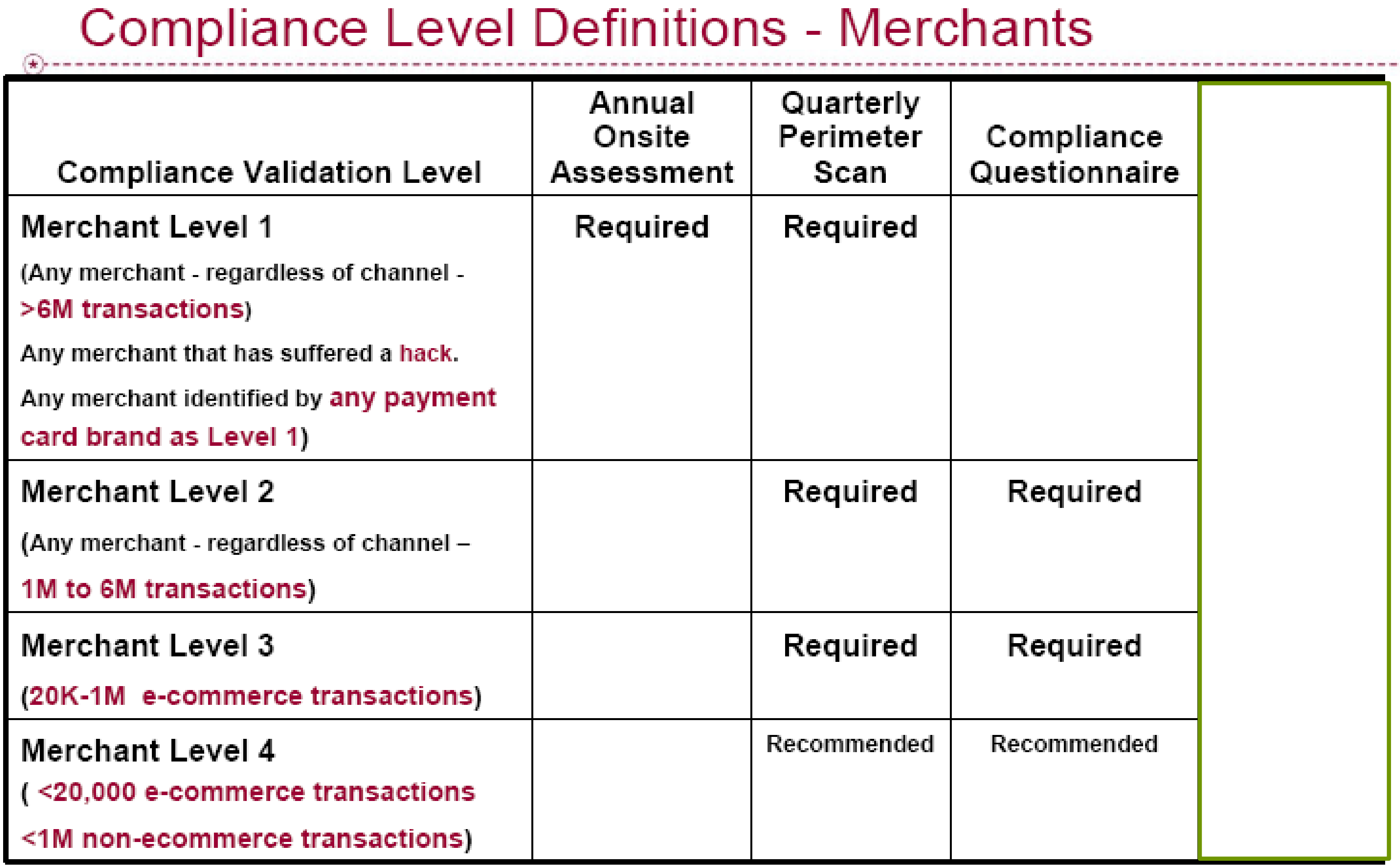


Compliance Level Definitions – Service Providers

Compliance Validation Level	Annual Onsite Assessment	Quarterly Perimeter Scan	Compliance Questionnaire
Service Provider Level 1 **(VisaNet connection; All Payment Gateways; TPP and DSE that handle data for Level 1 & 2 Merchants)**	**Required**	**Required**	
Service Provider Level 2 (Not Level 1 w/ >1M transactions; DSE that handle data for Level 3 Merchants)	**Required**	**Required**	
Service Provider Level 3 (<1M transactions; all other DSEs)		**Required**	**Required**

- *TPP = Third Party Processors*
- *DSE = Data Storage Entity*

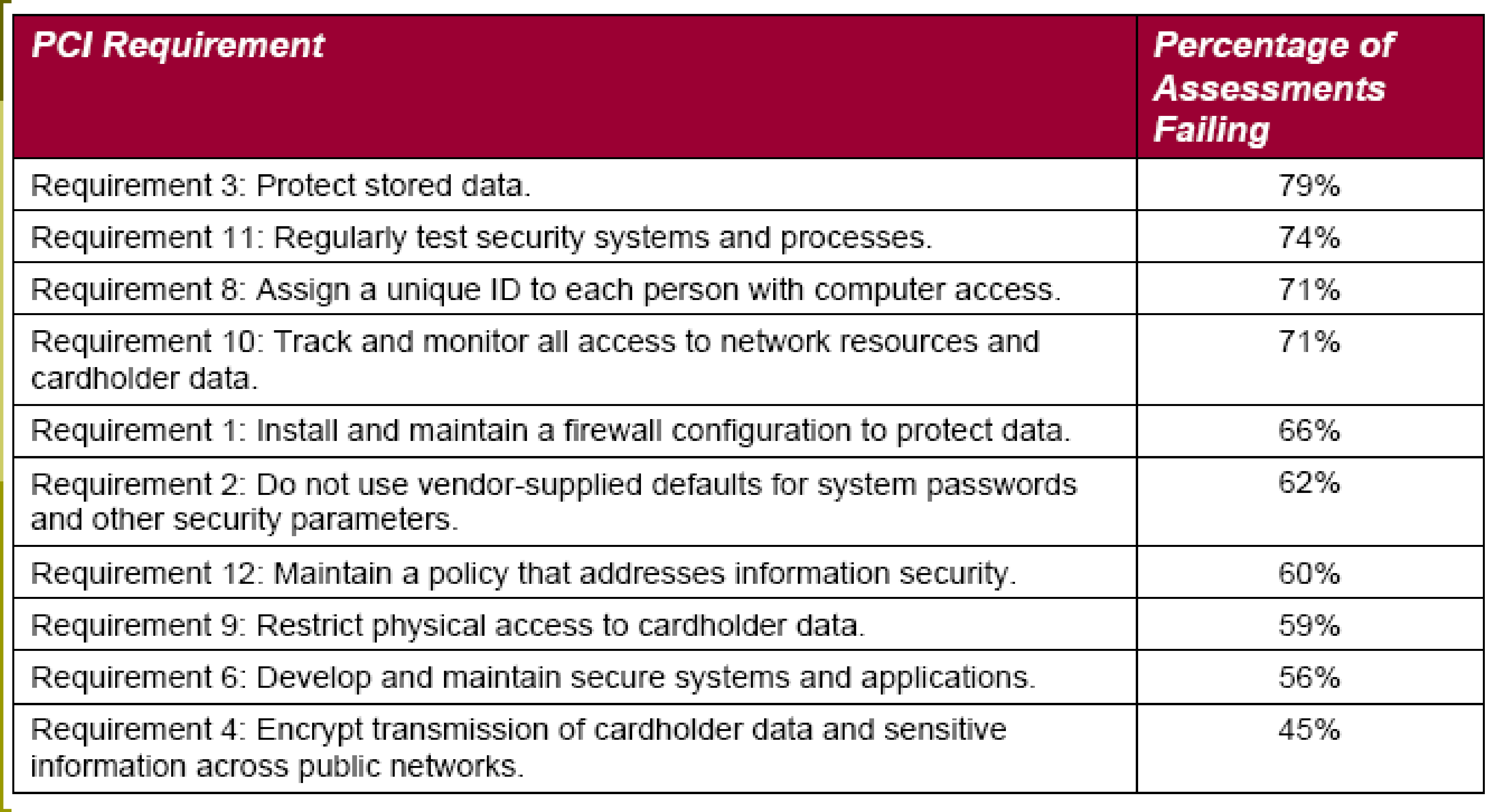
PCI DSS Requirements for Merchant’ams



Compliance Level Definitions - Merchants

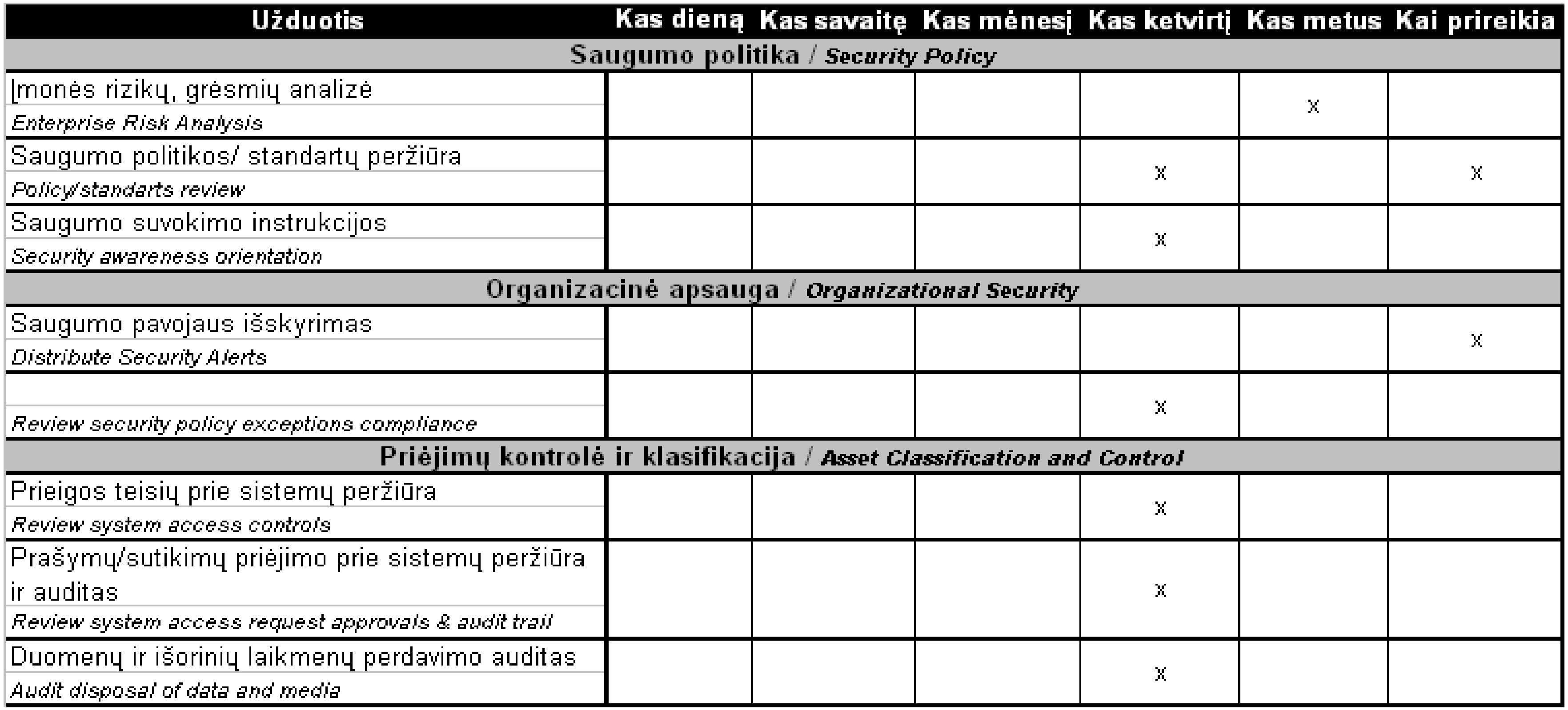
Compliance Validation Level	Annual Onsite Assessment	Quarterly Perimeter Scan	Compliance Questionnaire
Merchant Level 1 (Any merchant - regardless of channel - >6M transactions) Any merchant that has suffered a hack. Any merchant identified by any payment card brand as Level 1)	Required	Required	
Merchant Level 2 (Any merchant - regardless of channel – 1M to 6M transactions)		Required	Required
Merchant Level 3 (20K-1M e-commerce transactions)		Required	Required
Merchant Level 4 (<20,000 e-commerce transactions <1M non-ecommerce transactions)		Recommended	Recommended

The Most Common Non-Conformances During the PCI DSS audit



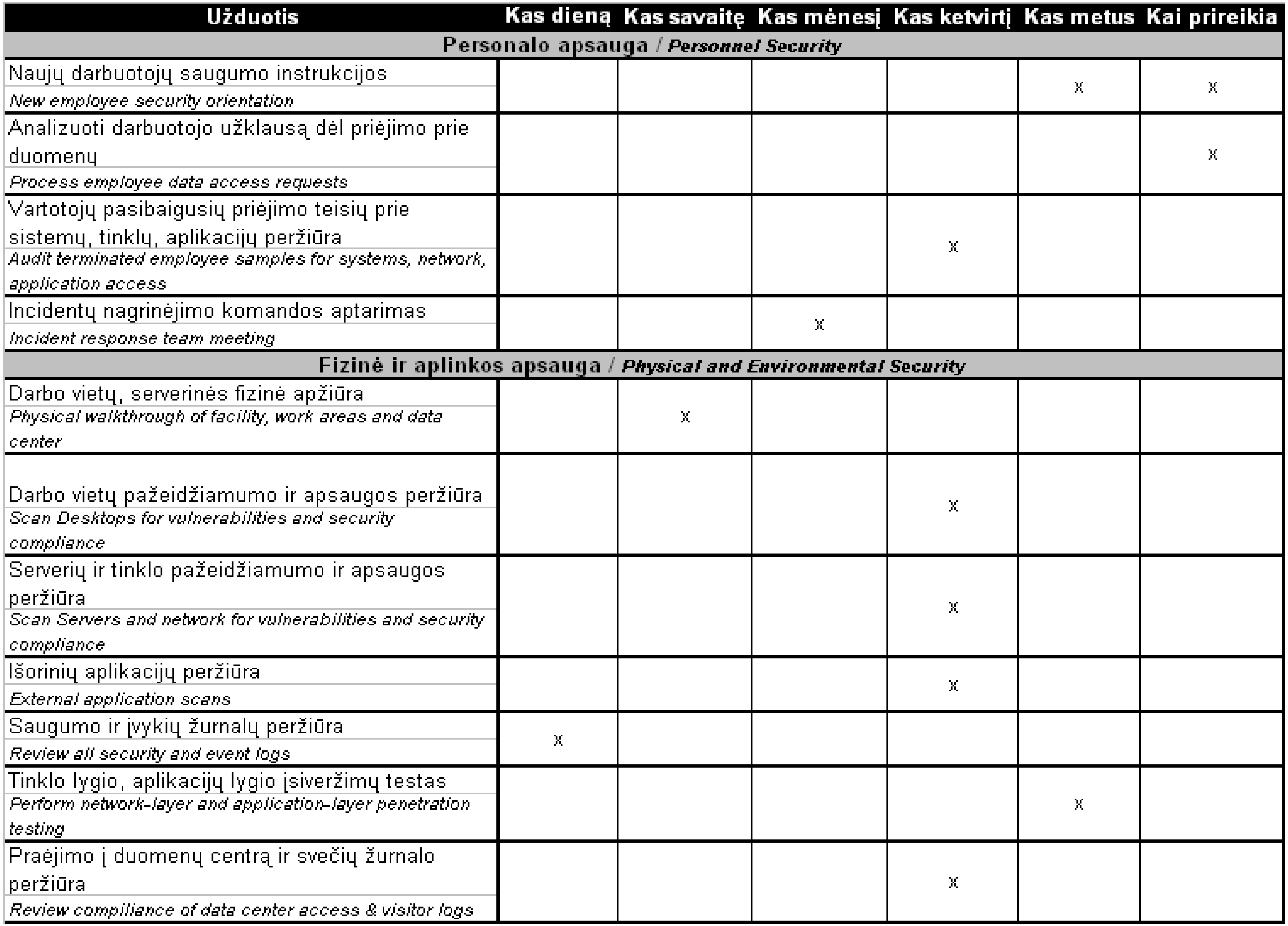
PCI Requirement	***Percentage of Assessments Failing***
Requirement 3: Protect stored data.	79%
Requirement 11: Regularly test security systems and processes.	74%
Requirement 8: Assign a unique ID to each person with computer access.	71%
Requirement 10: Track and monitor all access to network resources and cardholder data.	71%
Requirement 1: Install and maintain a firewall configuration to protect data.	66%
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.	62%
Requirement 12: Maintain a policy that addresses information security.	60%
Requirement 9: Restrict physical access to cardholder data.	59%
Requirement 6: Develop and maintain secure systems and applications.	56%
Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks.	45%

Periodical Procedures According PCI DSS (1)



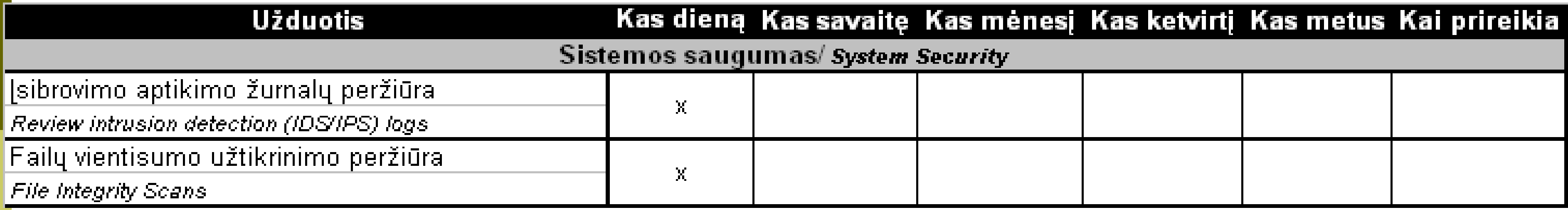
Užduotis	Kas dieną	Kas savaitę	Kas mėnesį	Kas ketvirtį	Kas metus	Kai prireikia
Saugumo politika / *Security Policy*						
Įmonės rizikų, grėsmių analizė *Enterprise Risk Analysis*					x	
Saugumo politikos/ standartų peržiūra *Policy/standarts review*				x		x
Saugumo suvokimo instrukcijos *Security awareness orientation*				x		
Organizacinė apsauga / *Organizational Security*						
Saugumo pavojaus išskyrimas *Distribute Security Alerts*						x
Review security policy exceptions compliance				x		
Priėjimų kontrolė ir klasifikacija / *Asset Classification and Control*						
Prieigos teisių prie sistemų peržiūra *Review system access controls*				x		
Prašymų/sutikimų priėjimo prie sistemų peržiūra ir auditas *Review system access request approvals & audit trail*				x		
Duomenų ir išorinių laikmenų perdavimo auditas *Audit disposal of data and media*				x		

Periodical Procedures According PCI DSS (2)



Užduotis	Kas dieną	Kas savaitę	Kas mėnesį	Kas ketvirtį	Kas metus	Kai prireikia
Personalo apsauga / *Personnel Security*						
Naujų darbuotojų saugumo instrukcijos *New employee security orientation*					x	x
Analizuoti darbuotojo užklausą dėl priėjimo prie duomenų *Process employee data access requests*						x
Vartotojų pasibaigusių priėjimo teisių prie sistemų, tinklų, aplikacijų peržiūra *Audit terminated employee samples for systems, network, application access*				x		
Incidentų nagrinėjimo komandos aptarimas *Incident response team meeting*			x			
Fizinė ir aplinkos apsauga / *Physical and Environmental Security*						
Darbo vietų, serverinės fizinė apžiūra *Physical walkthrough of facility, work areas and data center*		x				
Darbo vietų pažeidžiamumo ir apsaugos peržiūra *Scan Desktops for vulnerabilities and security compliance*				x		
Serverių ir tinklo pažeidžiamumo ir apsaugos peržiūra *Scan Servers and network for vulnerabilities and security compliance*				x		
Išorinių aplikacijų peržiūra *External application scans*				x		
Saugumo ir įvykių žurnalų peržiūra *Review all security and event logs*	x					
Tinklo lygio, aplikacijų lygio įsiveržimų testas *Perform network-layer and application-layer penetration testing*					x	
Praėjimo į duomenų centrą ir svečių žurnalo peržiūra *Review compiliance of data center access & visitor logs*				x		

Periodical Procedures According PCI DSS(3)



Užduotis	Kas dieną	Kas savaitę	Kas mėnesį	Kas ketvirtį	Kas metus	Kai prireikia
Sistemos saugumas/ ***System Security***						
Įsibrovimo aptikimo žurnalų peržiūra *Review intrusion detection (IDS/IPS) logs*	x					
Failų vientisumo užtikrinimo peržiūra *File Integrity Scans*	x					