bsi.

...making excellence a habit.™

PCI-DSS Webinar

Introduction to PCI-DSS for Payment Card Business & Service Providers

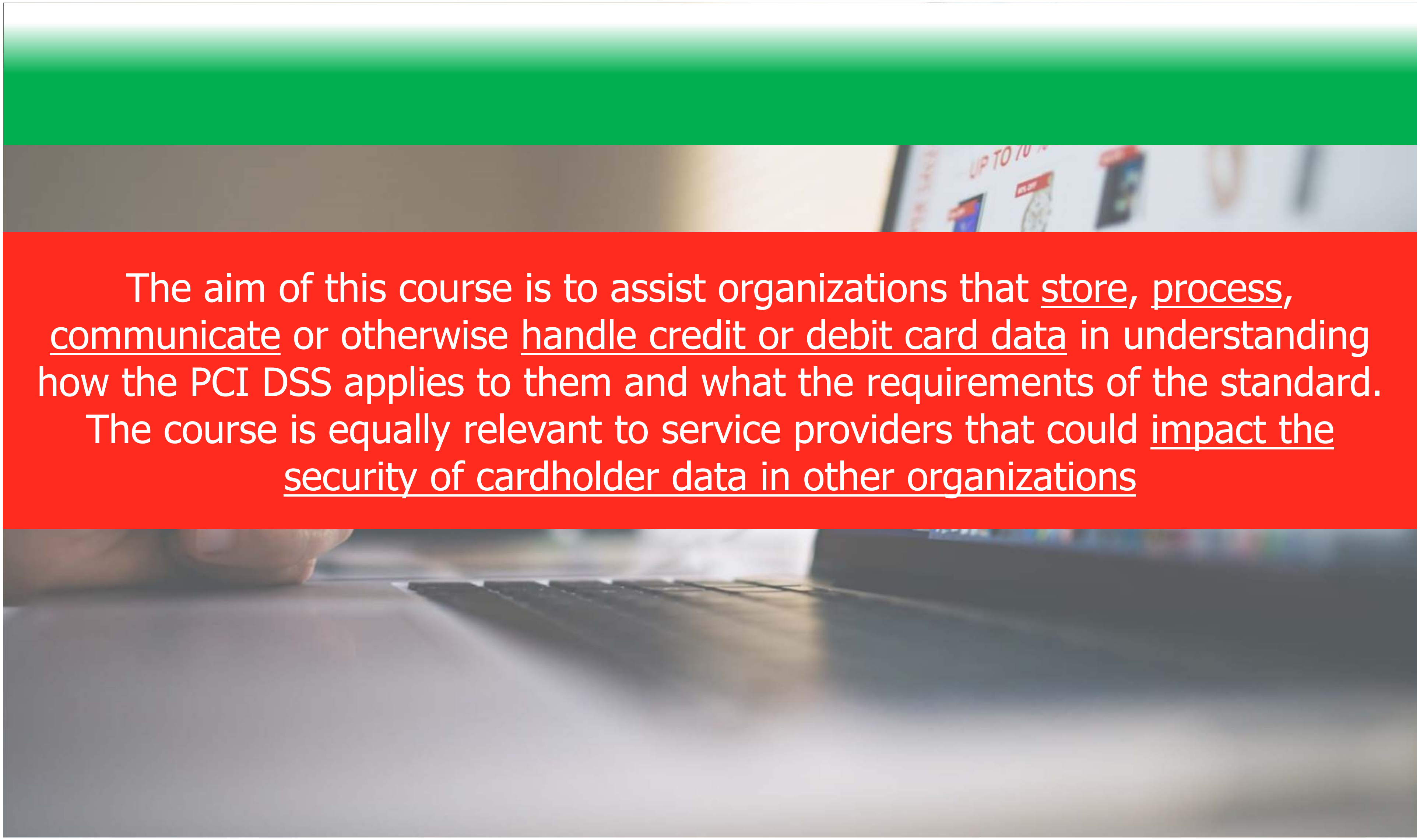
Presented by Instructor Bancha Faungfu

Regional IS & IT Group Administrator (ASIAPAC)
QSA, Client Manager, Lead Assessor and Instructor
Standard: SMS, ISMS, PIMS, BCMS, CSA, PCI-DSS

Copyright © 2017 BSI. All rights reserved.

By Royal Charter

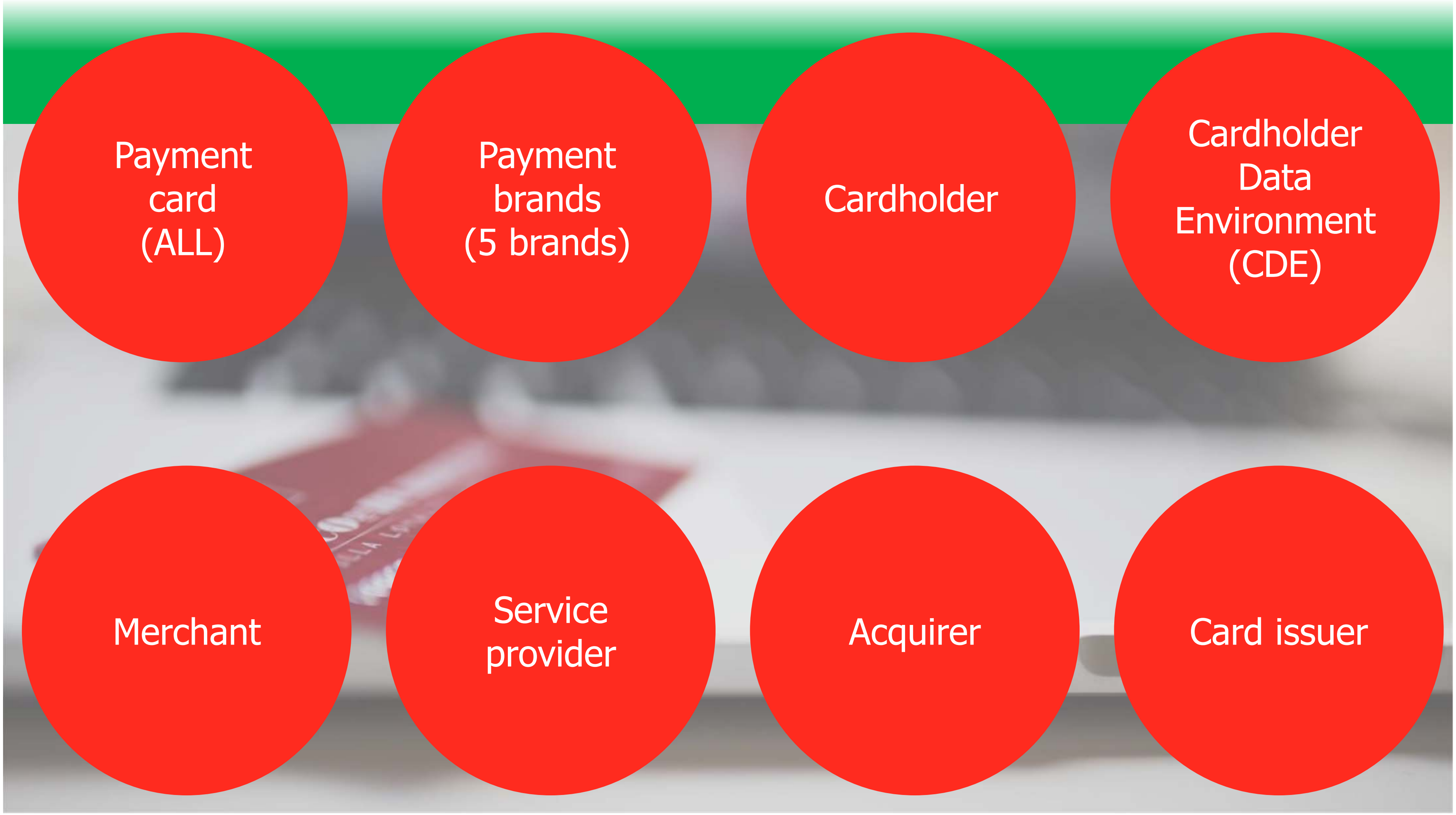
Course aim



The aim of this course is to assist organizations that store, process, communicate or otherwise handle credit or debit card data in understanding how the PCI DSS applies to them and what the requirements of the standard. The course is equally relevant to service providers that could impact the security of cardholder data in other organizations

Copyright © 2017 BSI. All rights reserved.

Useful definitions



Payment card (ALL)

Payment brands (5 brands)

Cardholder

Cardholder Data Environment (CDE)

Merchant

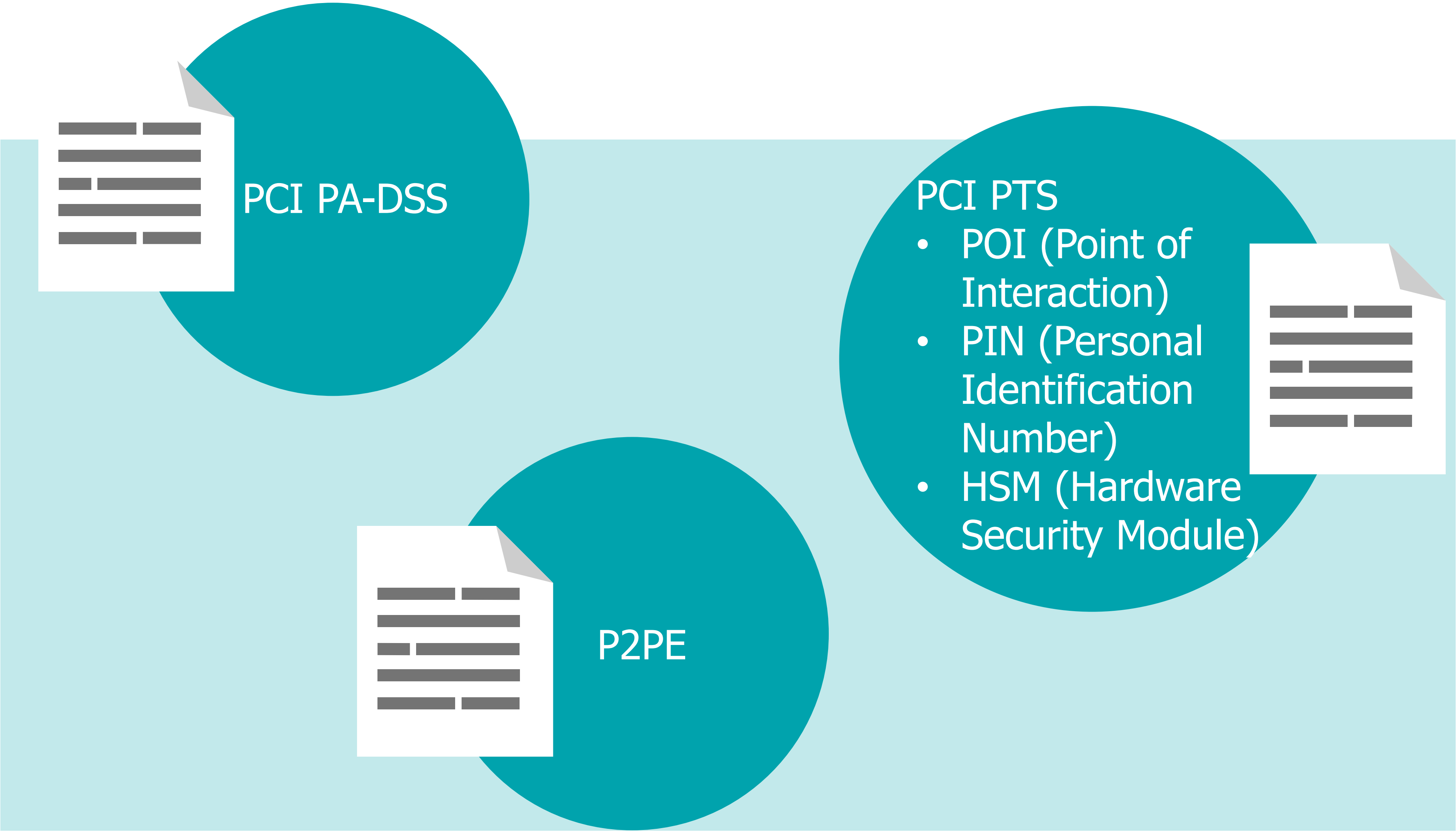
Service provider

Acquirer

Card issuer

Copyright © 2017 BSI. All rights reserved.

Useful standards



PCI PA-DSS

PCI PTS

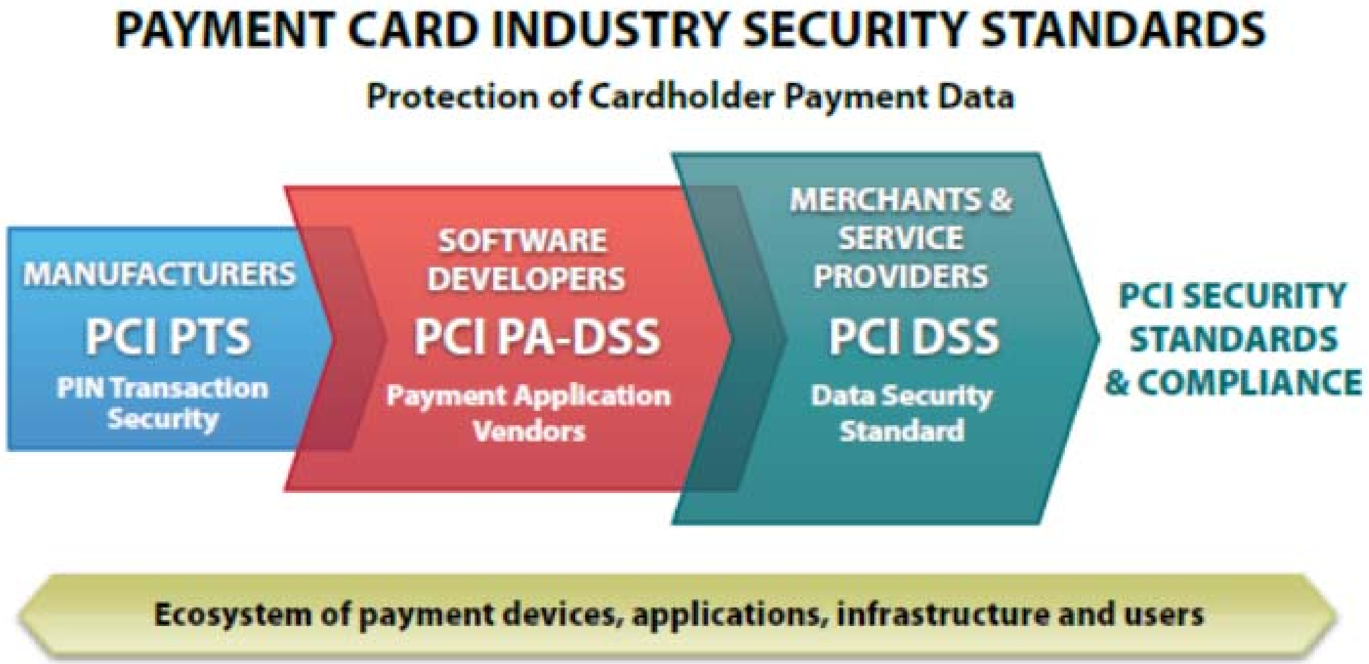
- POI (Point of Interaction)
- PIN (Personal Identification Number)
- HSM (Hardware Security Module)

P2PE

Copyright © 2017 BSI. All rights reserved.

Overview of PCI Requirements

PCI security standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The standards apply to all entities that store, process or transmit cardholder data – with guidance for software developers and manufacturers of applications and devices used in those transactions. The Council is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council, American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.


PAYMENT CARD INDUSTRY SECURITY STANDARDS
Protection of Cardholder Payment Data
MANUFACTURERS
PCI PTS
PIN Transaction Security
SOFTWARE DEVELOPERS
PCI PA-DSS
Payment Application Vendors
MERCHANTS & SERVICE PROVIDERS
PCI DSS
Data Security Standard
PCI SECURITY STANDARDS & COMPLIANCE
Ecosystem of payment devices, applications, infrastructure and users

Copyright © 2017 BSI. All rights reserved.

History of PCI DSS

Date	Version	Comments
Dec 15 2004	1.0	Card Brands
Sep 06 2006	1.1	PCI SSC Formed
Oct 01 2008	1.2	Addition of wireless networks
Oct 01 2010	2.0	Very few changes
Nov 06 2013	3.0	Integration into business as usual
Apr 15 2015	3.1	SSL removed
Apr 28 2016	3.2	Additional guidance and clarification on controls
May 2018	3.2.1	Current version
Q4, 2019	1st Draft 4.0	Reviewing draft version only
Q3-Q4, 2020	2st Draft 4.0	Reviewing draft version only
Q2, 2021	4.0	PCI DSS v4.0
Q4, 2021	4.0	Supporting documents, program, trainings

Copyright © 2017 BSI. All rights reserved.

What is the purpose of PCI DSS?

- Protect cardholder data
- Reduce risk of fraud through payment card system

Copyright © 2017 BSI. All rights reserved.

How are payment cards accepted?

Card present:

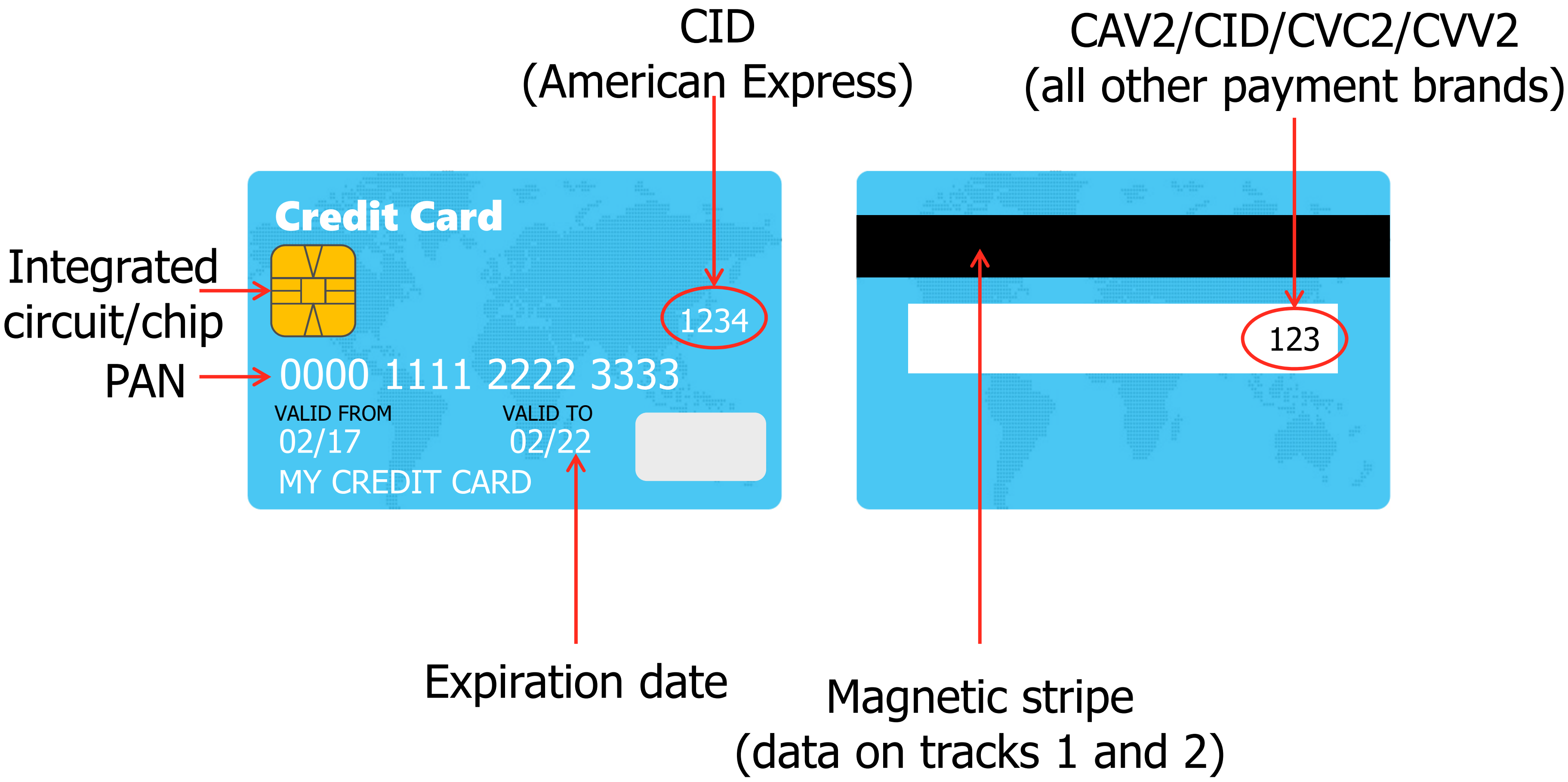
- Chip and Pin devices

Card not present:

- Forms submitted by post or fax
- Telephone, Websites
- Mobile, Apps, others

Copyright © 2017 BSI. All rights reserved.

What is cardholder data?



CID
(American Express)

CAV2/CID/CVC2/CVV2
(all other payment brands)

Integrated circuit/chip

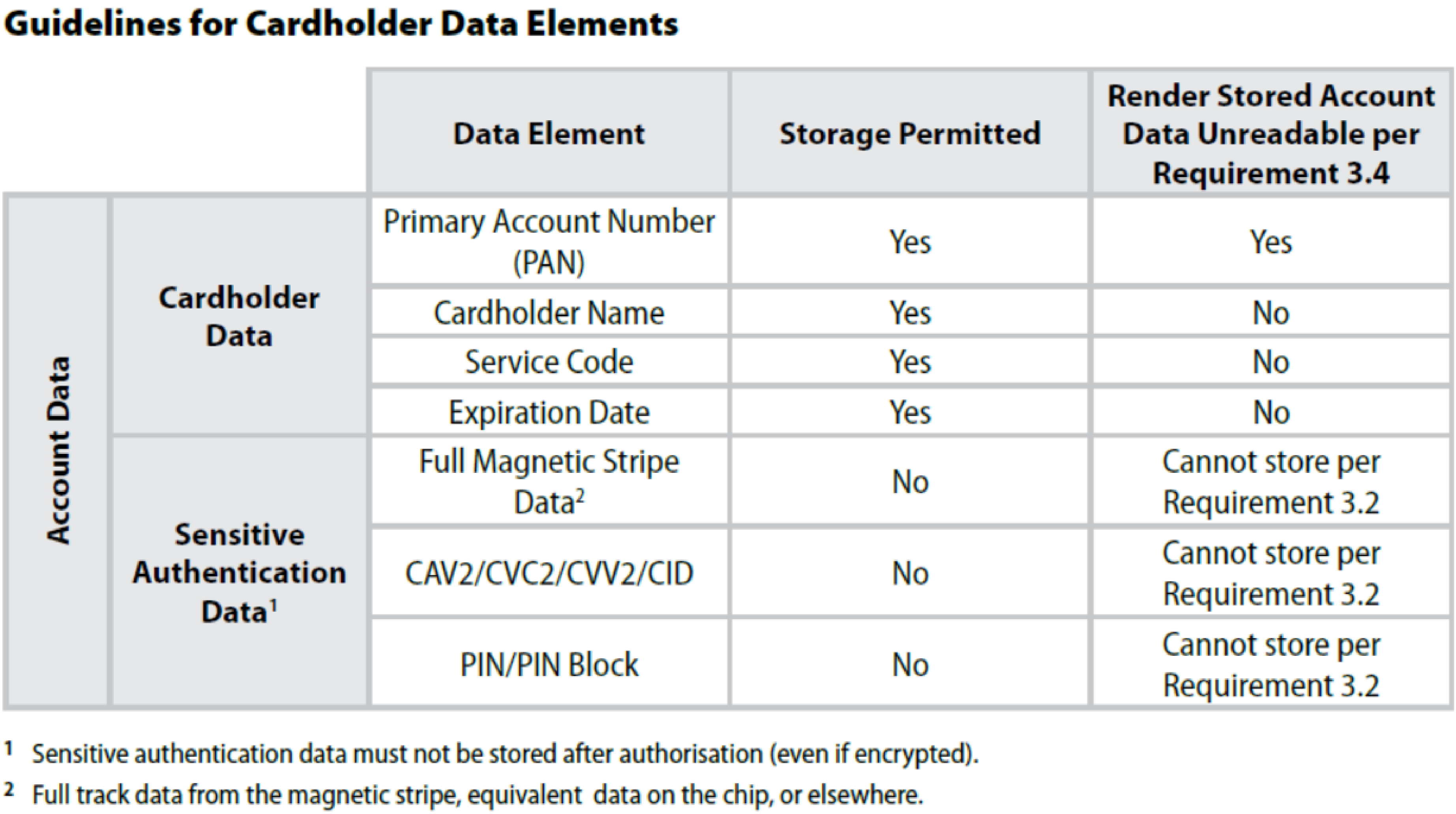
PAN

Expiration date

Magnetic stripe
(data on tracks 1 and 2)

Copyright © 2017 BSI. All rights reserved.

Storing cardholder data



Guidelines for Cardholder Data Elements

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data[1]	Full Magnetic Stripe Data[2]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

[1] Sensitive authentication data must not be stored after authorisation (even if encrypted).

[2] Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.

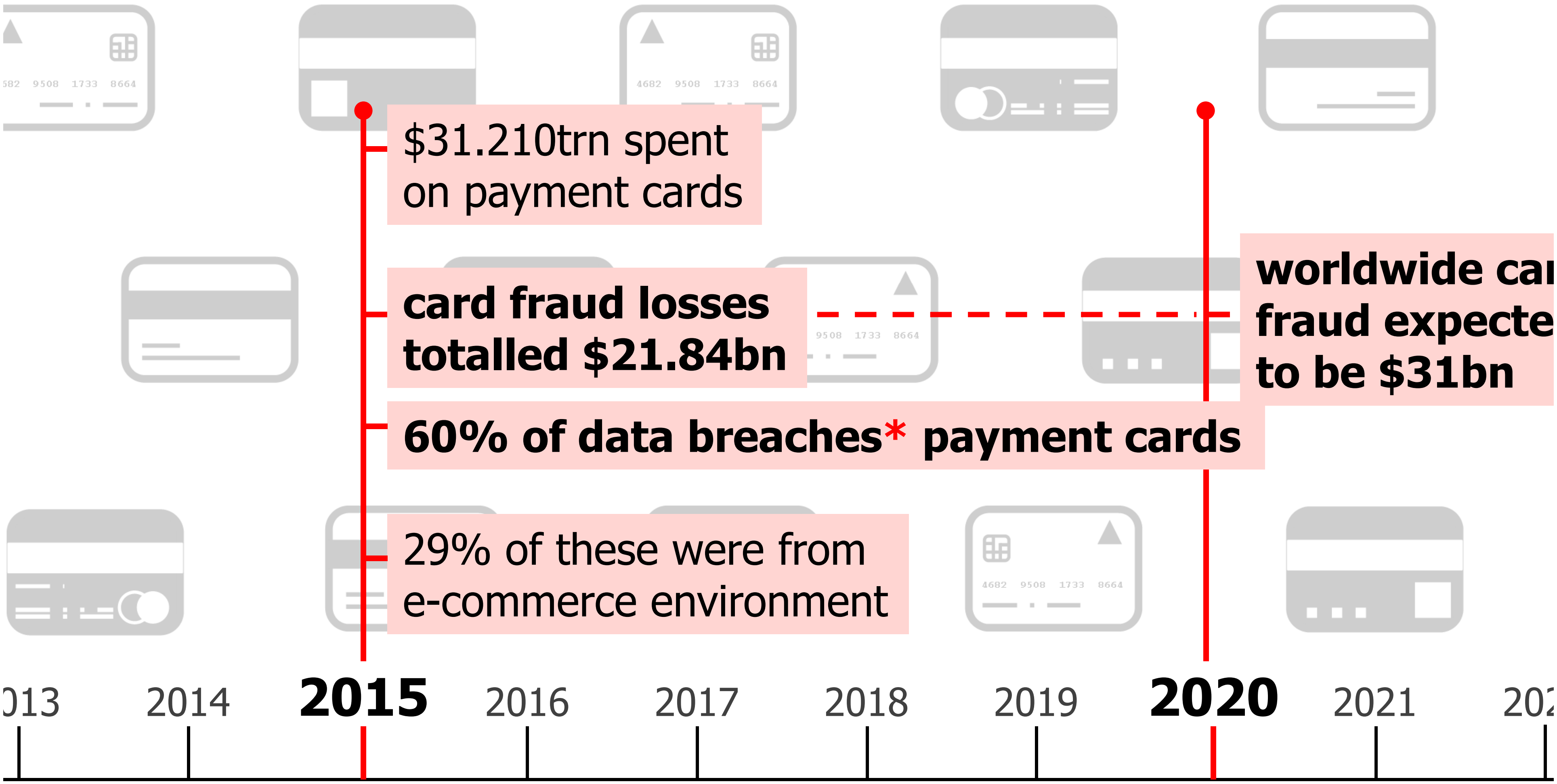
Copyright © 2017 BSI. All rights reserved.

Cardholder data do’s and don’ts

Do’s	**Don’ts**
Understand where cardholder data flows for the entire transaction process	Do not store cardholder data **unless it’s absolutely necessary**
Only use payment applications that comply with the Payment Application Data Security Standard (**PA-DSS**)	Do not store sensitive authentication data **after authorization**
Only retain cardholder data where there is an **authorized business need** and **ensure it is protected**	Do not store any payment card data in **payment card terminals or other unprotected endpoint devices, such as PCs, laptops or smart phones**

Copyright © 2017 BSI. All rights reserved.

Why is PCI DSS important?



$31.210trn spent on payment cards

card fraud losses totalled $21.84bn

worldwide ca fraud expecte to be $31bn

60% of data breaches* payment cards

29% of these were from e-commerce environment

* Data breaches investigated by Trustwave, as reported in the 2016 Trustwave Global Security Report.

Copyright © 2017 BSI. All rights reserved.

Useful definitions

Qualified Security Assessor (QSA)

Approved Scanning Vendor (ASV)

Report on Compliance (ROC)

Self Assessment Questionnaire (SAQ)

Attestation of Compliance (AOC)

Copyright © 2017 BSI. All rights reserved.

Level	Amex	Discover	JCB	MasterCard	Visa
1	Annual on-site assessment performed by a QSA **or** merchant if certified by the CEO, CFO, CISO **or** principle of the merchant	Annual on-site assessment performed by a QSA **or** merchant's internal auditor	Annual on-site assessment performed by a QSA	Annual on-site assessment performed by a QSA	Annual on-site assessment performed by a QSA
2	Annual self-assessment questionnaire performed by the merchant and certified by the CEO, CFO, CISO or principle of the merchant	Annual self-assessment questionnaire	Annual self-assessment questionnaire	Annual self-assessment questionnaire	Annual self-assessment questionnaire Attestation of Compliance
3	Annual self-assessment questionnaire	Annual self-assessment questionnaire	N/A	Annual self-assessment questionnaire	Annual self-assessment questionnaire
4	N/A	Compliance validation requirements determined by Acquirer	N/A	Compliance validation requirements determined by Acquirer	Annual self-assessment questionnaire recommended

Copyright © 2017 BSI. All rights reserved.

Level	Amex	Discover	JCB	MasterCard	Visa
1	Quarterly network scan by ASV	Quarterly network scan by ASV	Quarterly network scan by ASV	Quarterly network scan by ASV	Quarterly network scan by ASV
2	Quarterly network scan by ASV	Quarterly network scan by ASV	Quarterly network scan by ASV	Quarterly network scan by ASV	Quarterly network scan by ASV
3	Quarterly network scan by ASV	Quarterly network scan by ASV	N/A	Quarterly network scan by ASV	Quarterly network scan by ASV
4	N/A	Quarterly network scan by ASV	N/A	Quarterly network scan by ASV recommended	Quarterly network scan by ASV recommended

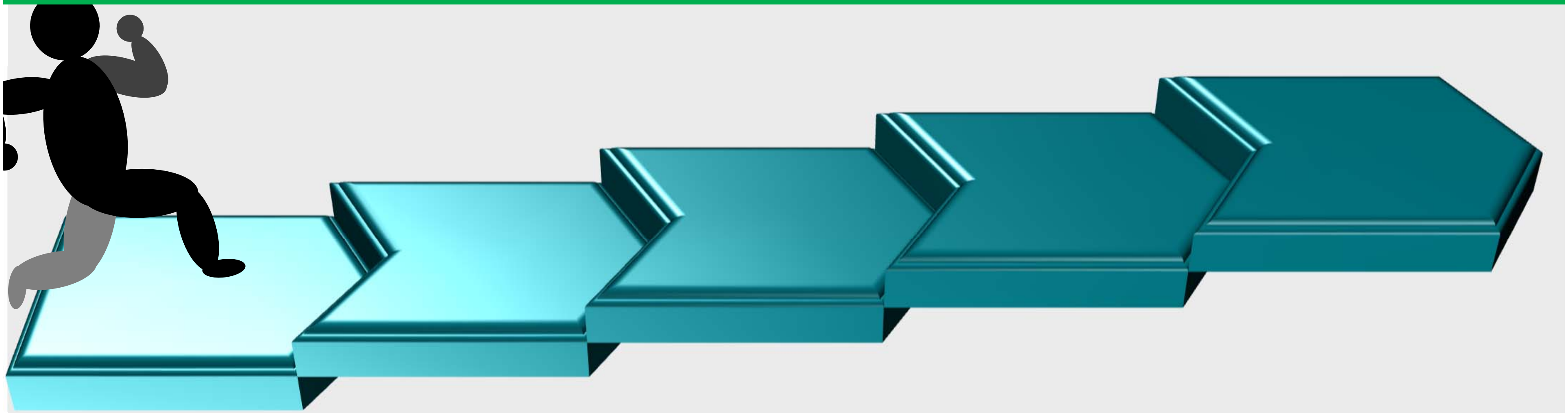
Copyright © 2017 BSI. All rights reserved.

Service provider reporting and validation requirements

Level	Amex	Discover	JCB	MasterCard	Visa
1	Annual on-site assessment performed by a QSA or service provider if certified by the CEO, CFO, CISO or principle of the merchant Quarterly network scan by ASV	Annual on-site assessment performed by a QSA or internal auditor (if signed by officer of service provider) or annual self-assessment Quarterly network scan by ASV	Annual on-site assessment performed by a QSA Quarterly network scan by ASV	Annual on-site assessment performed by a QSA Quarterly network scan by ASV	Annual on-site assessment performed by a QSA Quarterly network scan by ASV Attestation of Compliance
2	Annual on-site assessment performed by a QSA or service provider if certified by the CEO, CFO, CISO or principle of the merchant Quarterly network scan by ASV	N/A	N/A	Annual self-assessment questionnaire Quarterly network scan by ASV	Annual self-assessment questionnaire Quarterly network scan by ASV Attestation of Compliance
3	Annual self-assessment questionnaire Quarterly network scan by ASV	N/A	N/A	N/A	N/A

Copyright © 2017 BSI. All rights reserved.

Data flow analysis



Data flow analysis - scoping

Segmentation and consolidation

Access

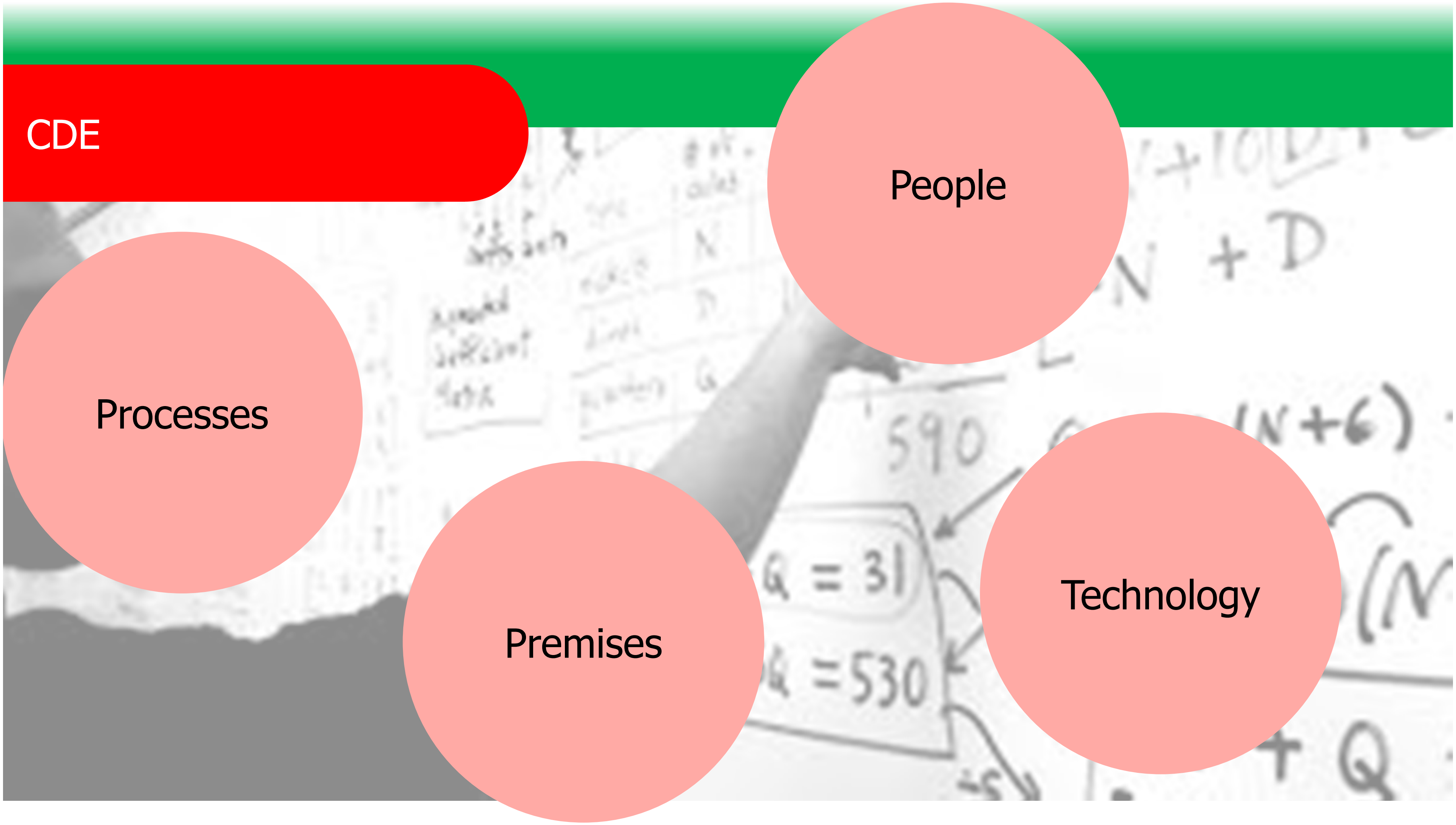
Remediation

Validation

bsi.

Copyright © 2017 BSI. All rights reserved.

Scoping



CDE

People

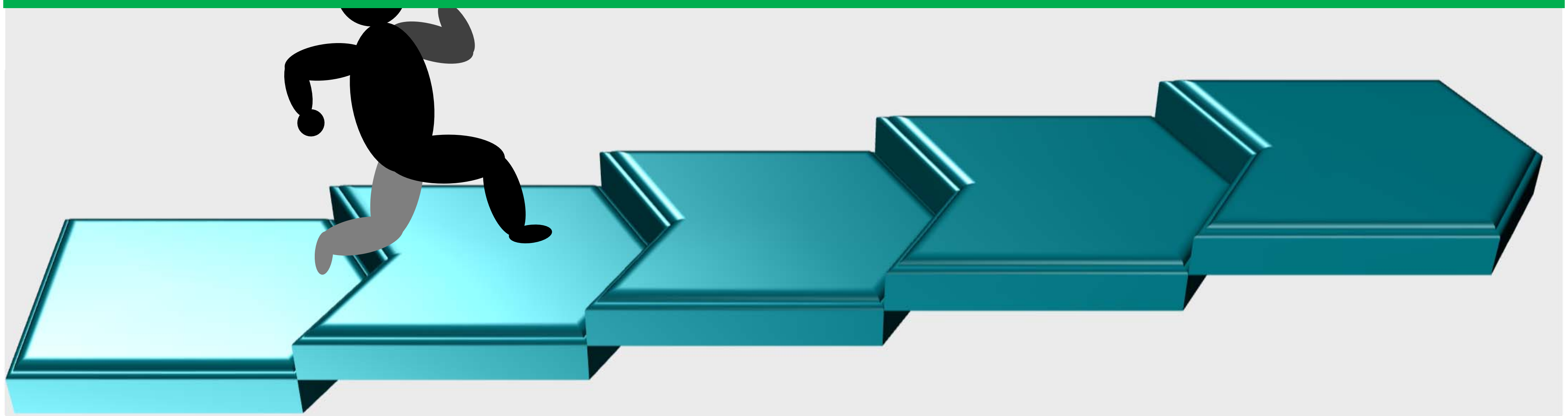
Processes

Premises

Technology

Copyright © 2017 BSI. All rights reserved.

Segmentation



Data flow analysis - scoping

Segmentation and consolidation

Access

Remediation

Validation

Copyright © 2017 BSI. All rights reserved.

PCI DSS requirements

Copyright © 2017 BSI. All rights reserved.

PCI DSS requirements

Goals	PCI DSS requirements
Build and maintain a secure network and systems	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Protect all systems against malware and regularly update antivirus software or programs
	6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need to know
	8. Identify and authenticate access to system components
	9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Information security policy	12. Maintain a policy that addresses information security for all personnel

Copyright © 2017 BSI. All rights reserved.

Example requirements and sub-requirements

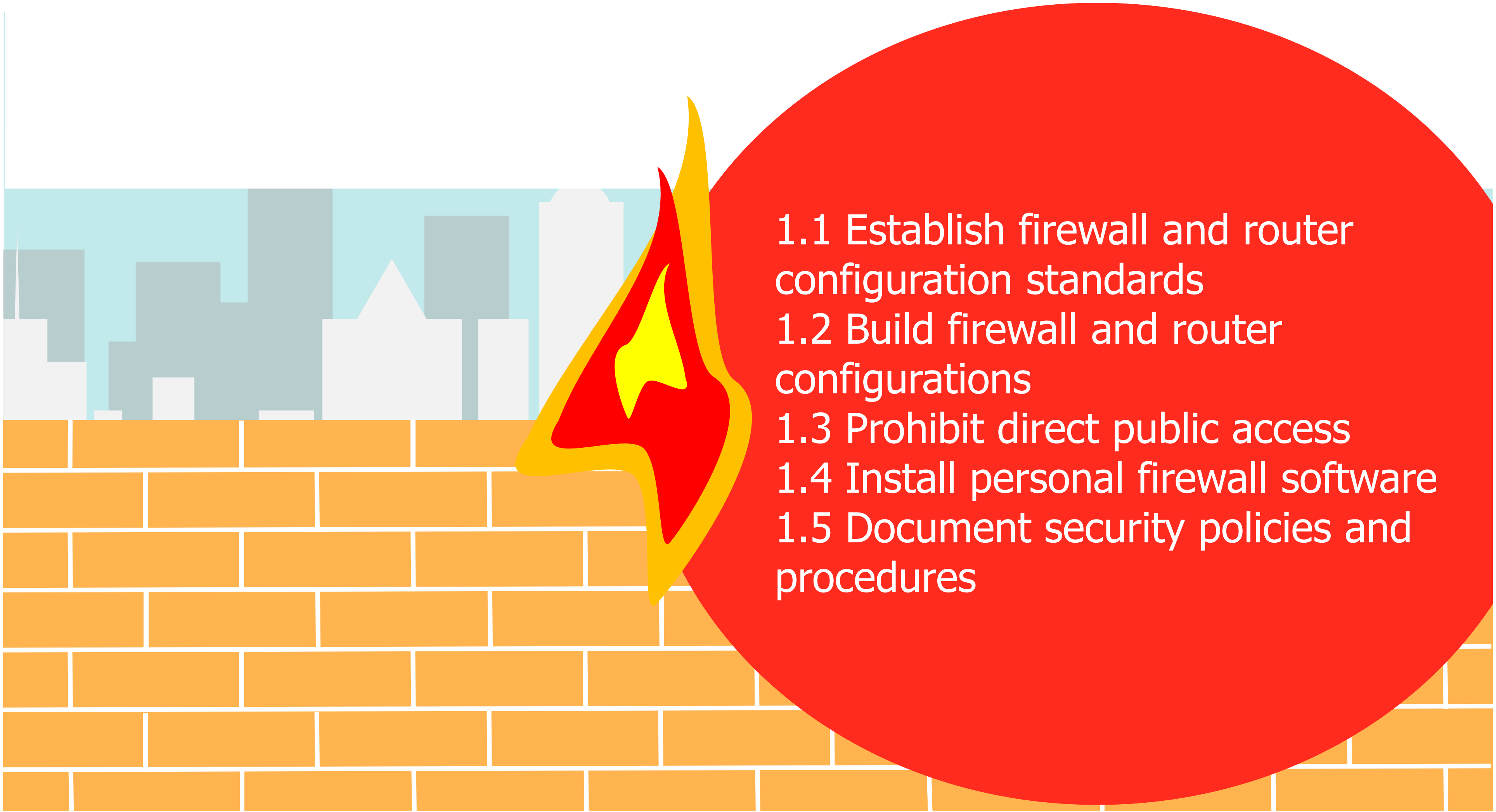
PCI DSS question		**Expected testing**	Response (mark 1 for each question)				
			Yes	Yes with CCW	No	N/A	Not tested
1.1	Are firewall and router configuration standards established and implemented to include the following:		□	□	□	□	□
1.1.1	Is there a formal process for approving and testing all network connections and changes to the firewall and router configurations?	• Review documented processes • Interview personnel • Examine network configurations	□	□	□	□	□
1.1.2	a) Is there a current network diagram that documents all connections between the CDE and other networks, including any wireless networks?	• Review current network diagram • Examine network configurations	□	□	□	□	□
	b) Is there a process to ensure the diagram is kept current?	• Interview responsible personnel	□	□	□	□	□
1.1.3	a) Is there a current diagram that shows all cardholder data flows across systems and networks?	• Review current dataflow diagram • Examine network configurations	□	□	□	□	□
	b) Is there a process to ensure the diagram is kept current?	• Interview personnel	□	□	□	□	□
1.1.4	a) Is a firewall required and implemented at each Internet connection and between any demilitarized zone and the internal network zone?	• Review firewall configuration standards • Observe network configurations to verify that a firewall(s) is in place	□	□	□	□	□

Build and maintain a secure network and systems

Requirement 1: Install and maintain a firewall configuration to protect data

Copyright © 2017 BSI. All rights reserved.

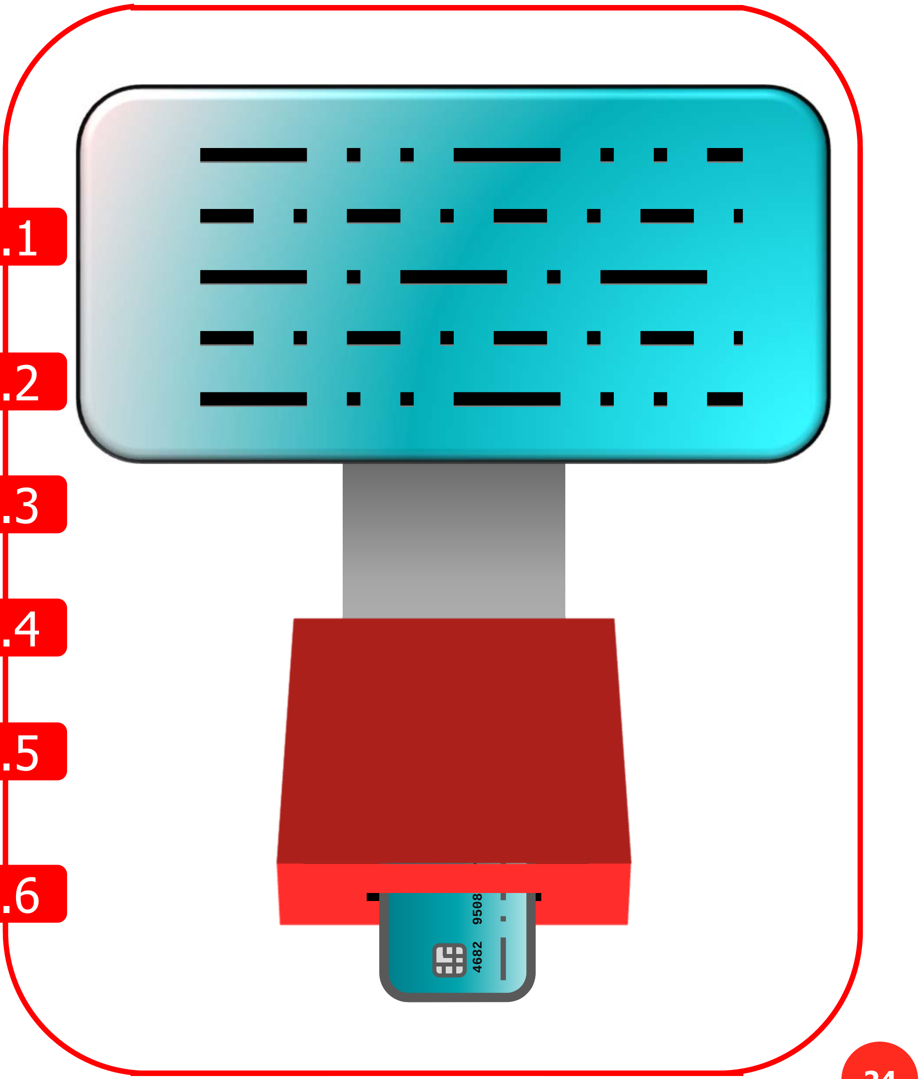
Req 1. Install and maintain a firewall configuration to protect cardholder data



1.1 Establish firewall and router configuration standards
1.2 Build firewall and router configurations
1.3 Prohibit direct public access
1.4 Install personal firewall software
1.5 Document security policies and procedures

Copyright © 2017 BSI. All rights reserved.

Req 2. Do not use vendor-supplied defaults for system passwords and other security parameters



2.1 Change defaults/remove unnecessary default accounts

2.2 Develop configuration standards for all components

2.3 Use strong cryptography

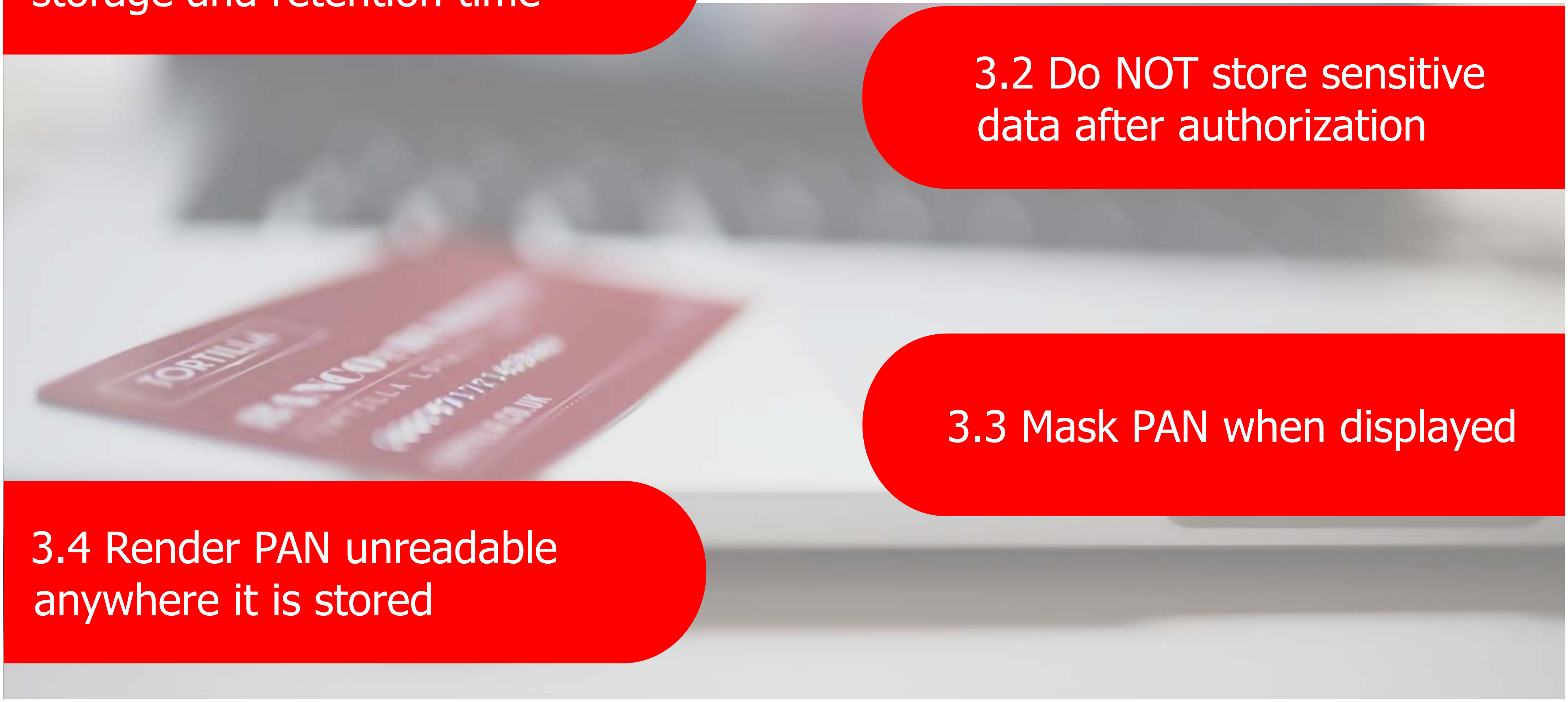
2.4 Maintain an inventory of system components

2.5 Document security policies and procedures

2.6 Shared hosting providers must protect each entity

Copyright © 2017 BSI. All rights reserved.

Req 3. Protect stored cardholder data



3.1 Limit cardholder data storage and retention time

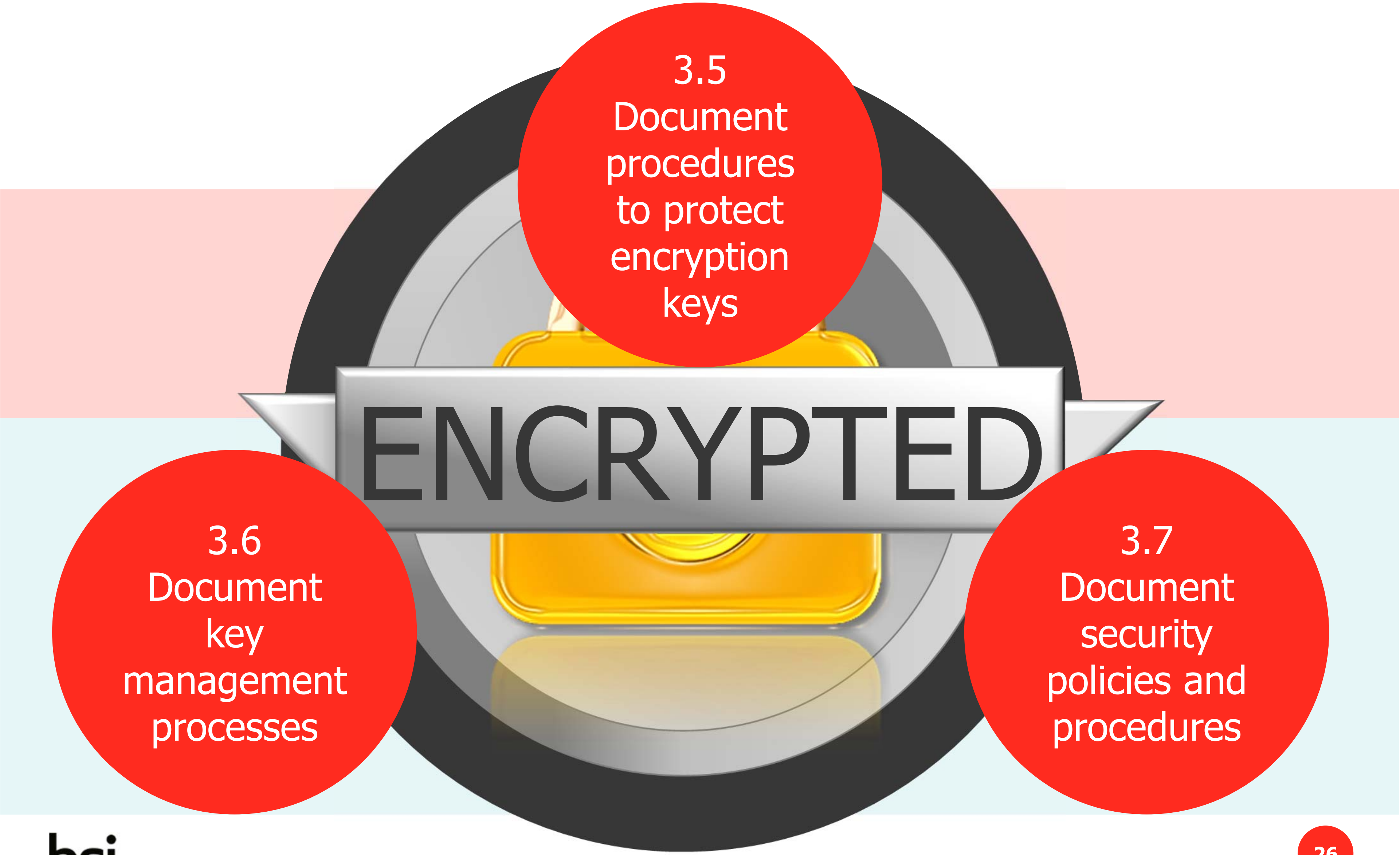
3.2 Do NOT store sensitive data after authorization

3.3 Mask PAN when displayed

3.4 Render PAN unreadable anywhere it is stored

Copyright © 2017 BSI. All rights reserved.

Protect stored cardholder data



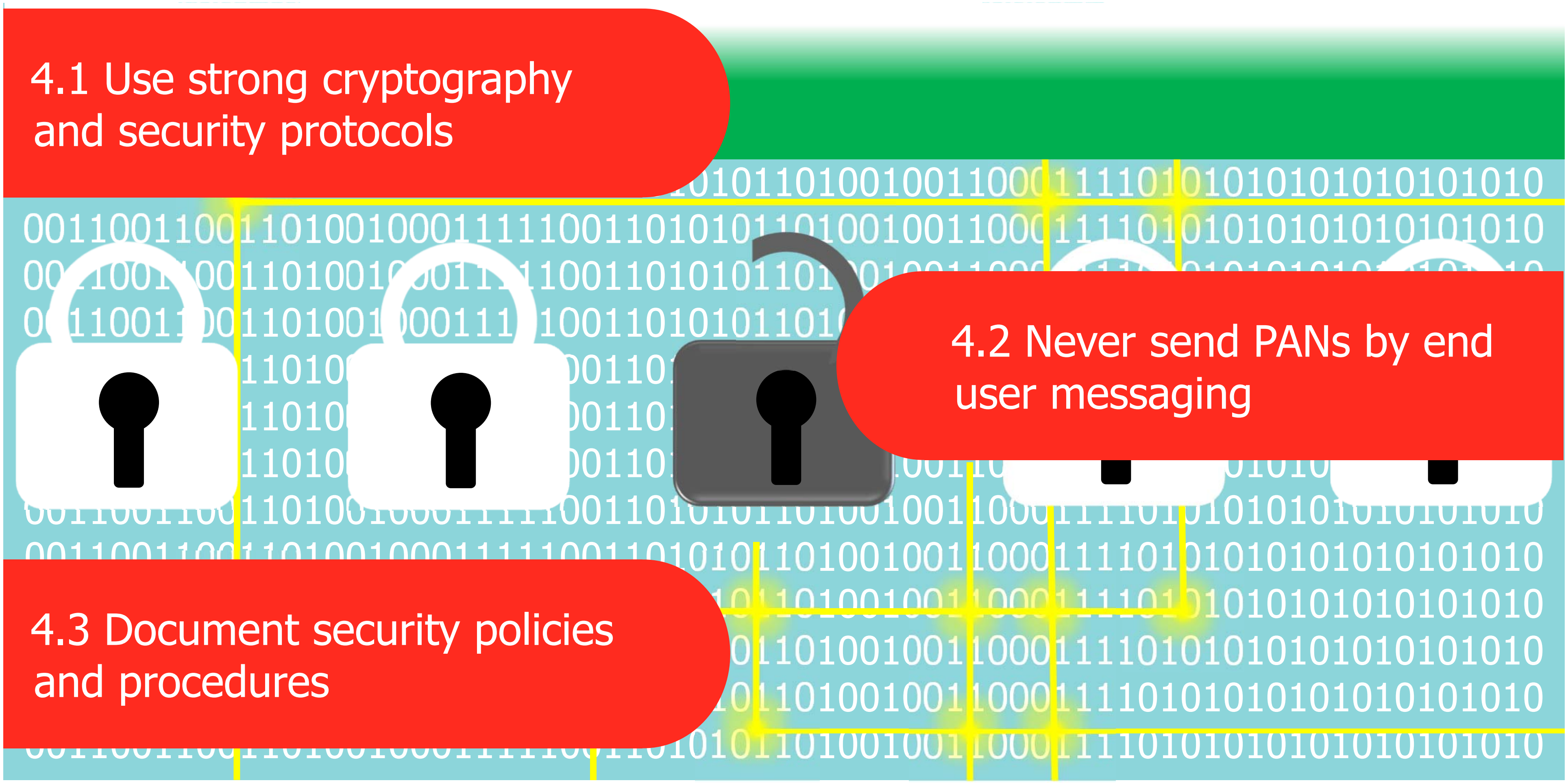
3.5
Document procedures to protect encryption keys

3.6
Document key management processes

3.7
Document security policies and procedures

Copyright © 2017 BSI. All rights reserved.

Req 4. Encrypt transmission of cardholder data across open, public networks



4.1 Use strong cryptography and security protocols

4.2 Never send PANs by end user messaging

4.3 Document security policies and procedures

Copyright © 2017 BSI. All rights reserved.

Req 5. Protect all systems against malware and regularly update anti-virus software or programs

5.1 Deploy anti-virus software on all systems

5.2 Ensure anti-virus is current, running and generating audit logs

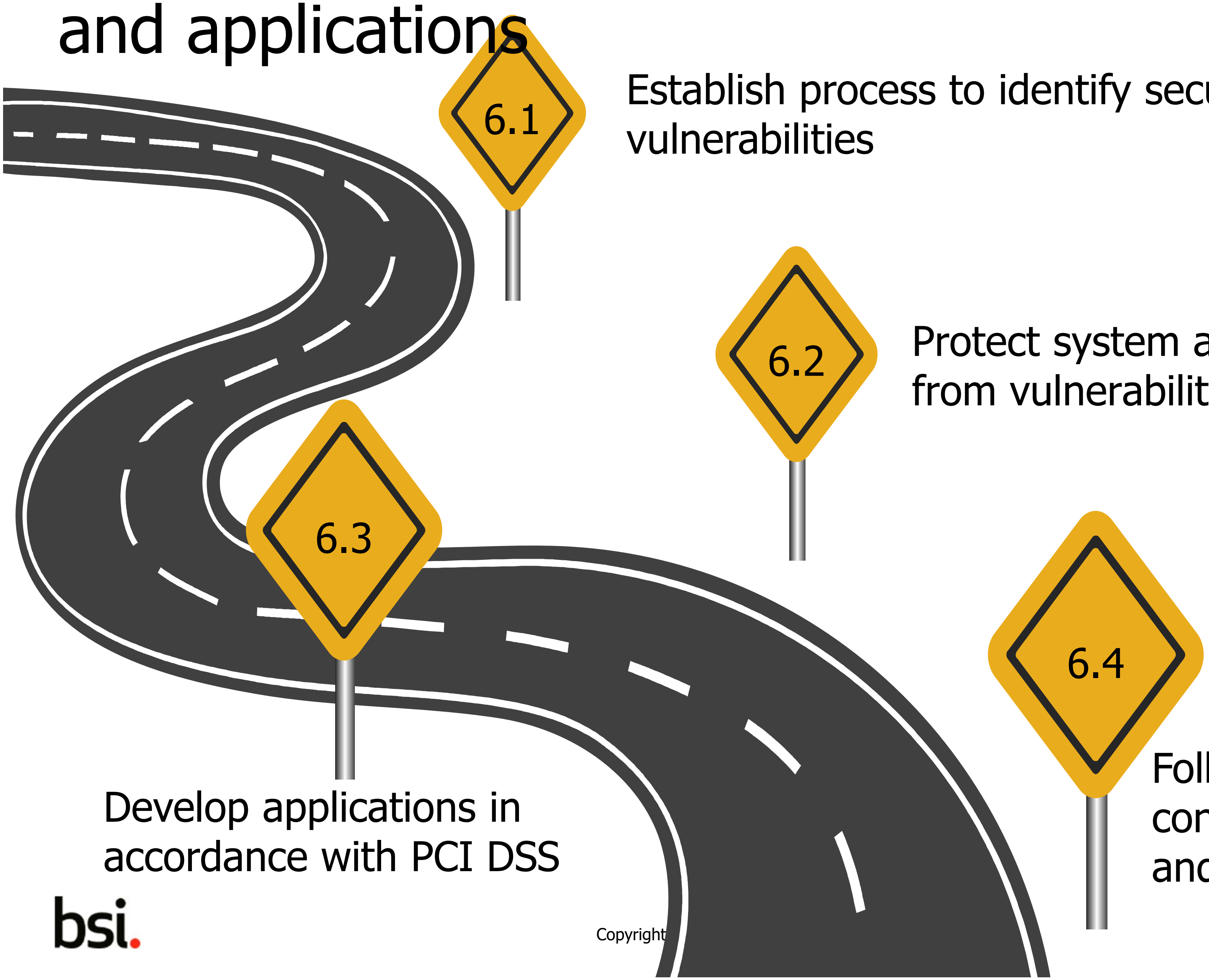
5.3 Ensure anti-virus cannot be disabled/altered

5.4 Document security policies and procedures

bsi.

Copyright © 2017 BSI. All rights reserved.

Req 6. Develop and maintain secure systems and applications



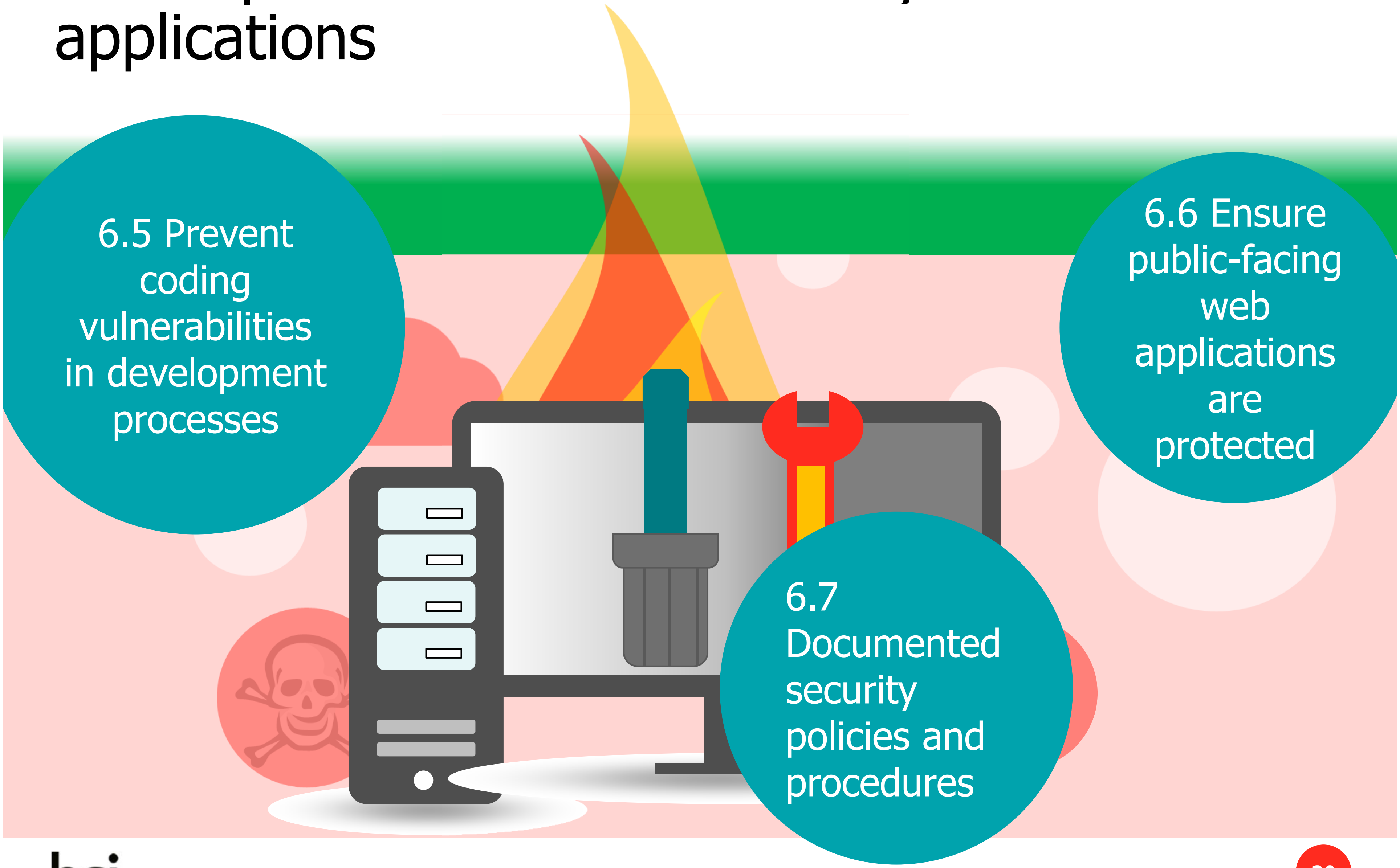
Establish process to identify security vulnerabilities

Protect system and software from vulnerabilities

Develop applications in accordance with PCI DSS

Follow change control processes and procedures

Develop and maintain secure systems and applications



6.5 Prevent coding vulnerabilities in development processes

6.6 Ensure public-facing web applications are protected

6.7 Documented security policies and procedures

Copyright © 2017 BSI. All rights reserved.

Req 7. Restrict access to cardholder data by business need to know

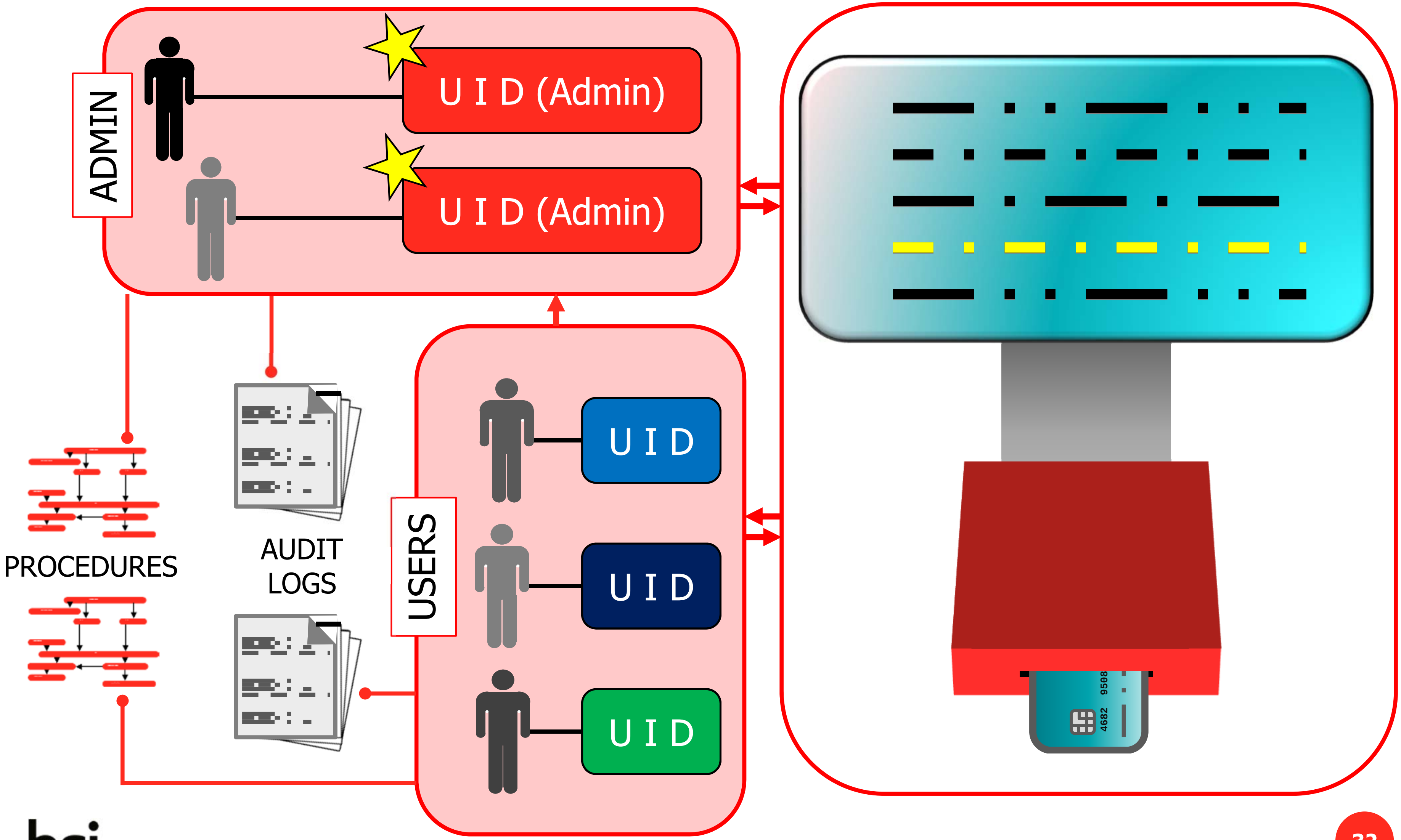
7.1 Limit access to system components and card data

7.2 Establish access control system(s) for components

7.3 Documented security policies and procedures

Copyright © 2017 BSI. All rights reserved.

Req 8. Identify and authenticate access to system components

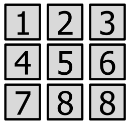


Copyright © 2017 BSI. All rights reserved.

Identify and authenticate access to system components

DO

8.6 Use other authentication mechanisms

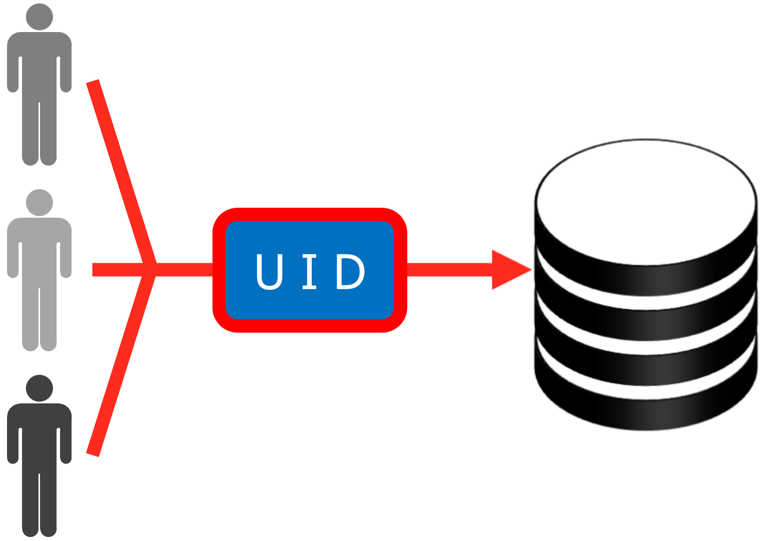


8.7 Restrict access to any cardholder database

8.8 Document security policies and procedures

DON'T

8.5 Do not use group, shared, or generic IDs



Copyright © 2017 BSI. All rights reserved.

Req 9. Restrict physical access to cardholder data

9.1
Use appropriate facility entry controls

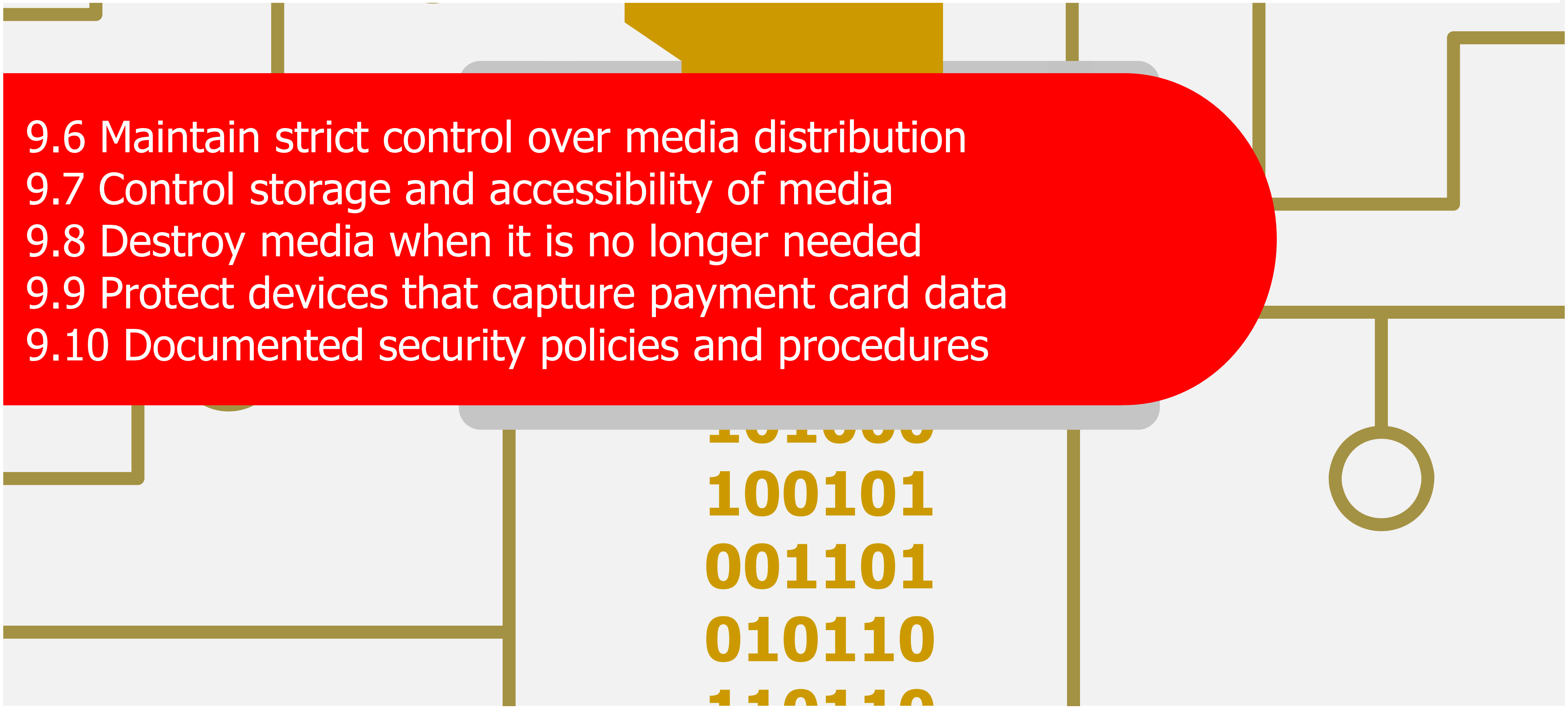
9.2
Distinguish between onsite personnel and visitors

9.3
Control physical access to sensitive areas

9.4
Ensure all visitors are authorized

9.5
Physically secure all media

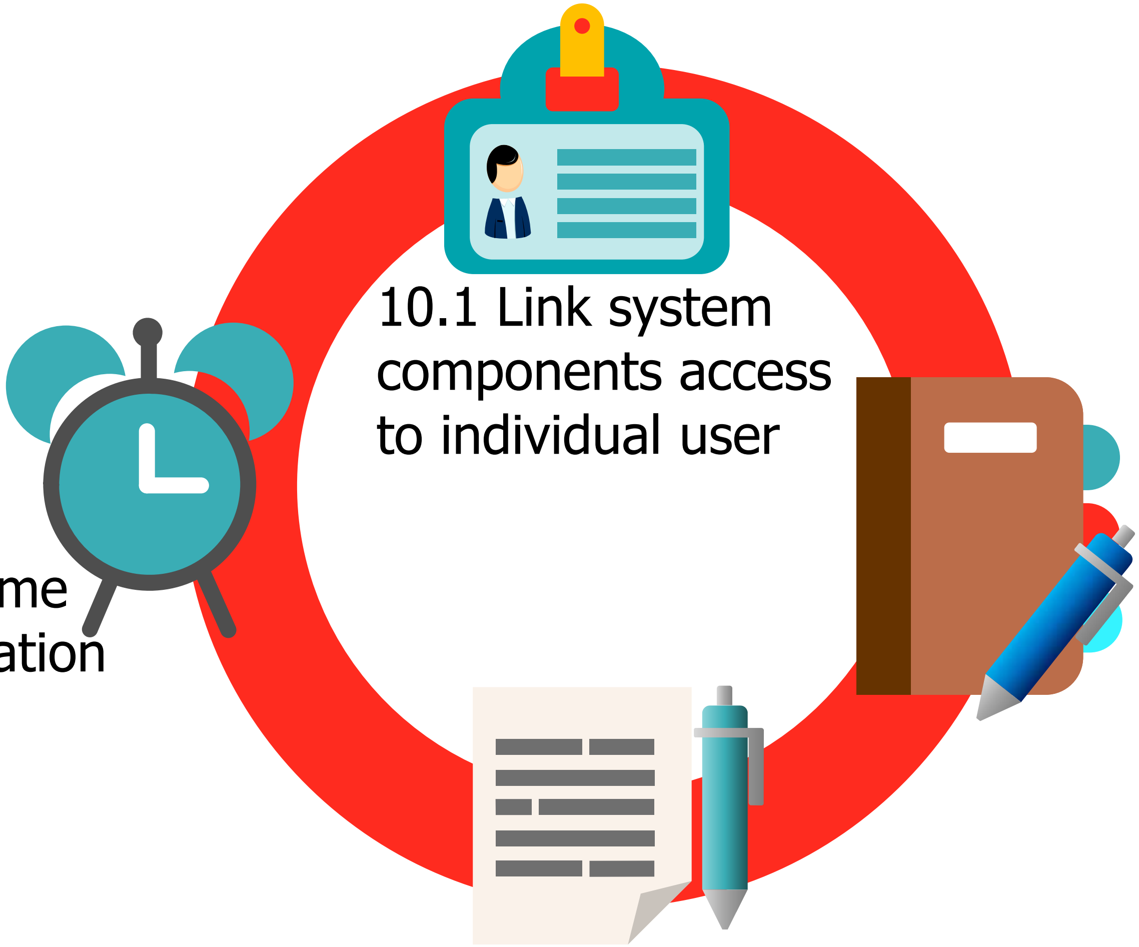
Restrict physical access to cardholder data



9.6 Maintain strict control over media distribution
9.7 Control storage and accessibility of media
9.8 Destroy media when it is no longer needed
9.9 Protect devices that capture payment card data
9.10 Documented security policies and procedures

Copyright © 2017 BSI. All rights reserved.

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



10.1 Link system components access to individual user

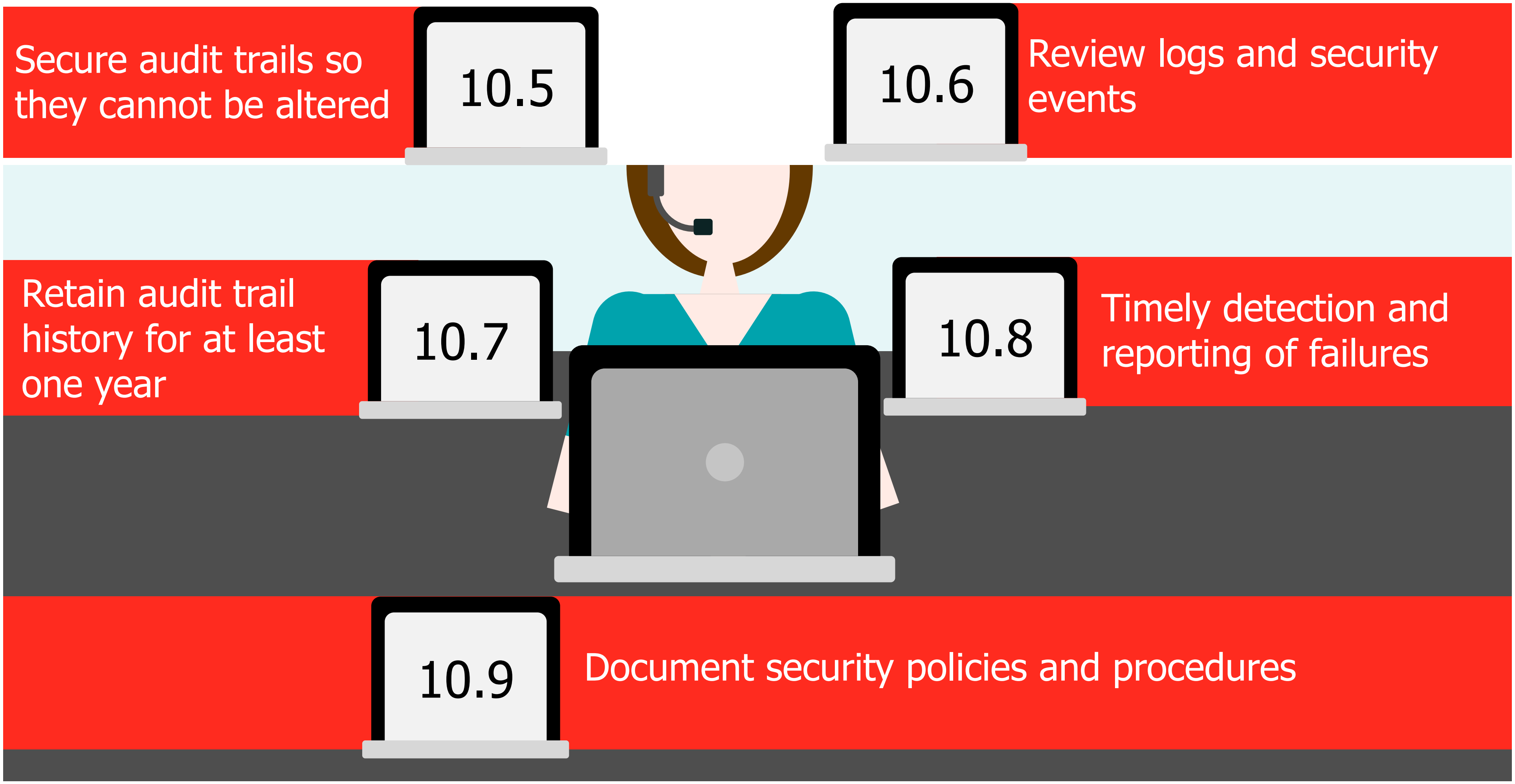
10.2 Implement audit trails for all system components

10.3 Record audit trail entries for system components

10.4 Use time synchronization technology

Copyright © 2017 BSI. All rights reserved.

Track and monitor all access to network resources and cardholder data



10.5 Secure audit trails so they cannot be altered

10.6 Review logs and security events

10.7 Retain audit trail history for at least one year

10.8 Timely detection and reporting of failures

10.9 Document security policies and procedures

Copyright © 2017 BSI. All rights reserved.

Req 11. Regularly test security systems and processes

- 11.1 Test for the presence of wireless access points
- 11.2 Run network vulnerability scans
- 11.3 Develop methodology for penetration testing

bsi.

Copyright © 2017 BSI. All rights reserved.

Regularly test security systems and processes

- 11.4 Use network intrusion detection/prevention
- 11.5 Deploy a change detection mechanism
- 11.6 Documented security policies and procedures

Copyright © 2017 BSI. All rights reserved.

Req 12. Maintain a policy that addresses information security for all personnel

12.1 Establish a security policy
12.2 Implement annual risk assessment process
12.3 Develop usage policies for critical technologies
12.4 Define information security responsibilities

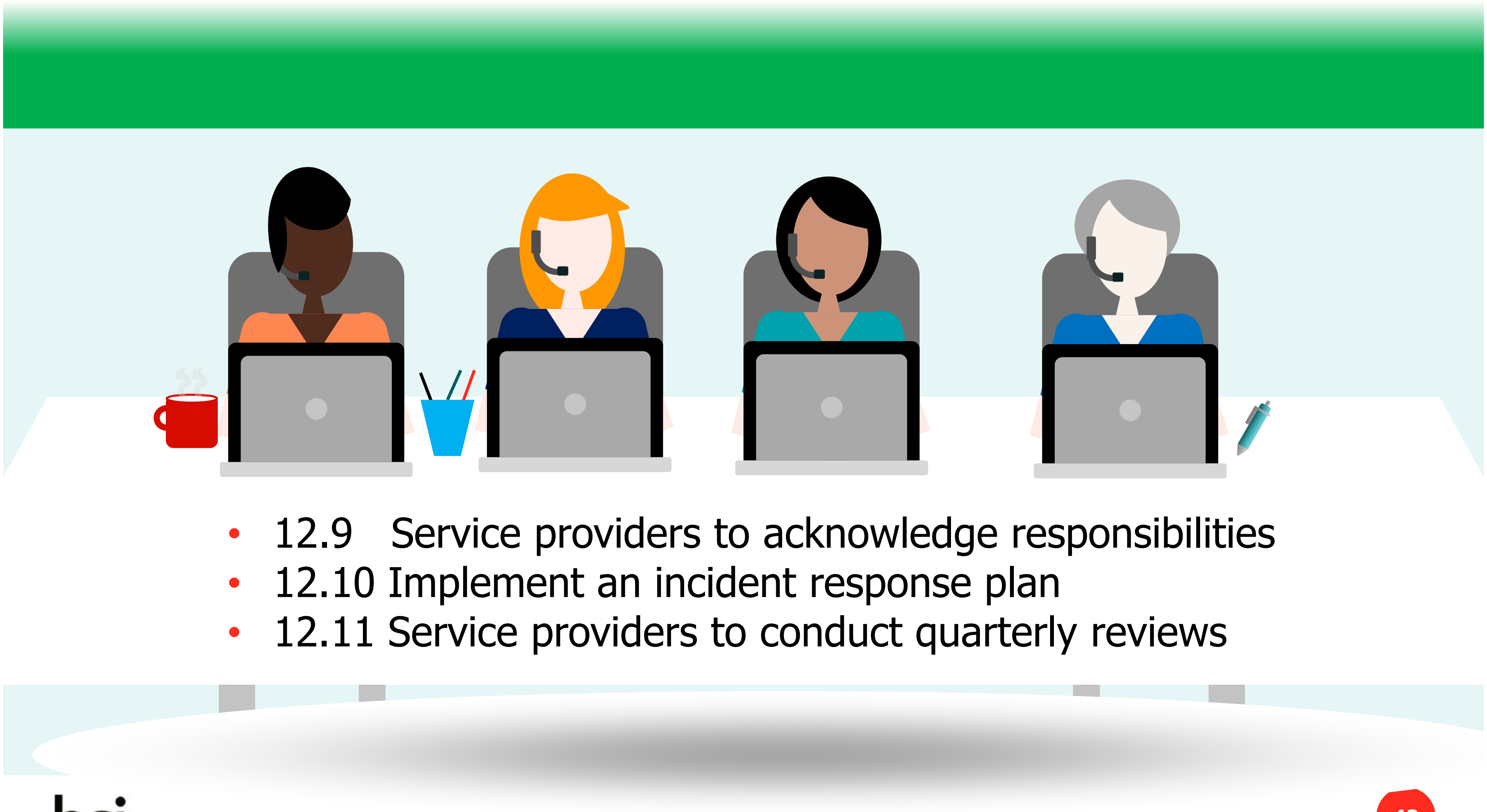
Copyright © 2017 BSI. All rights reserved.

Maintain a policy that addresses information security for all personnel

12.5 Assign information security responsibilities
12.6 Implement a formal security awareness program
12.7 Screen potential personnel prior to hire
12.8 Manage service providers

Copyright © 2017 BSI. All rights reserved.

Maintain a policy that addresses information security for all personnel



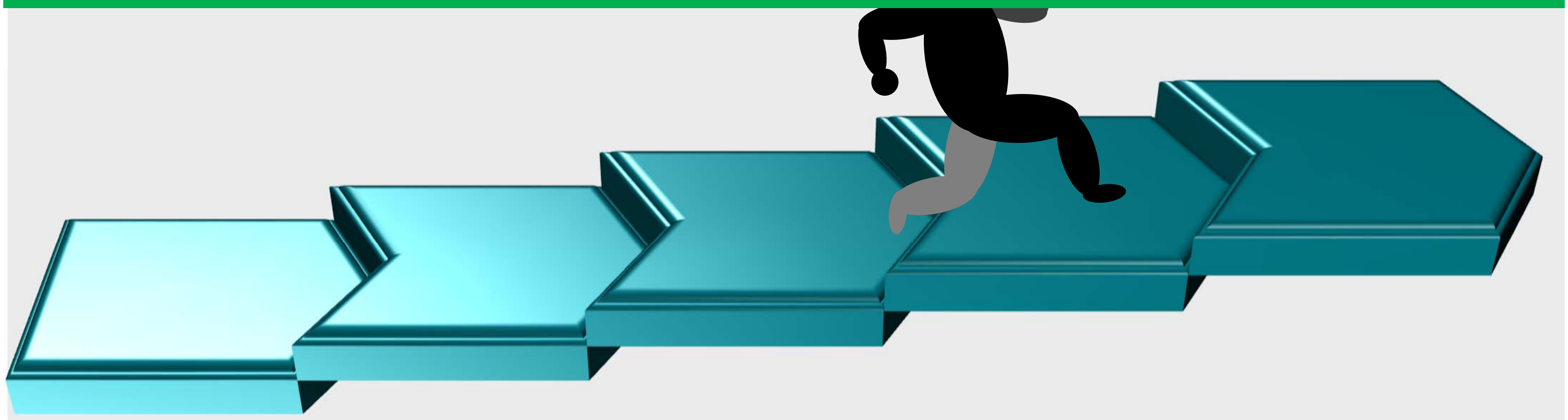
- 12.9 Service providers to acknowledge responsibilities
- 12.10 Implement an incident response plan
- 12.11 Service providers to conduct quarterly reviews

Copyright © 2017 BSI. All rights reserved.

Remediation and validation

Copyright © 2017 BSI. All rights reserved.

Remediation



Data flow analysis - scoping | Segmentation and consolidation | Access | **Remediation** | Validation

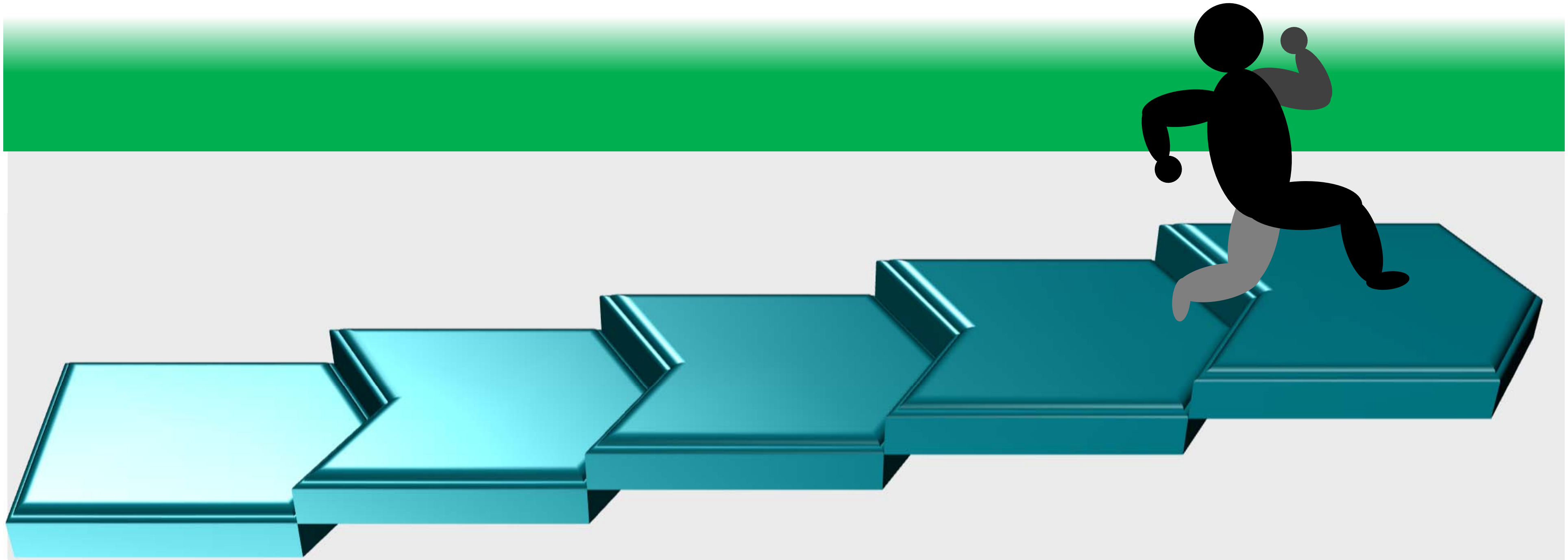
Copyright © 2017 BSI. All rights reserved.

Prioritized approach

Milestone	Goals
1	**Remove sensitive authentication data and limit data retention.** This milestone targets a key area of risk for entities that have been compromised. Remember, if sensitive authentication data and other cardholder data are not stored, the effects of a compromise will be greatly reduced. If you don't need it, don't store it.
2	**Protect systems and networks, and be prepared to respond to a system breach.** This milestone targets controls for points of access to most compromises, and the process for responding.
3	**Secure payment card applications.** This milestone targets controls for applications, application processes, and application servers. Weaknesses in these areas offer easy prey for compromising systems and obtaining access to cardholder data.
4	**Monitor and control access to your system.** Controls for this milestone allows you to detect the who, what, when, and how concerning who is accessing your network and CDE.
5	**Protect stored cardholder data.** For those organizations that have analysed their business processes and determined that they must store PANs. Milestone five targets key protection mechanisms for that stored data.
6	**Finalize remaining compliance efforts, and ensure all controls are in place.** The intent of Milestone six is to complete PCI DSS requirements, and to finalize all remaining related policies, procedures, and processes needed to protect the CDE.

Copyright © 2017 BSI. All rights reserved.

Validation



Data flow analysis - scoping

Segmentation and consolidation

Access

Remediation

Validation

Copyright © 2017 BSI. All rights reserved.

Ongoing management

Management system framework

- Assign accountability for maintaining PCI DSS compliance
- Define charter for PCI DSS compliance
- Perform reviews at least quarterly

Copyright © 2017 BSI. All rights reserved.