bsi.

...making excellence a habit.™

bsi.

LIVE Free Webinar

PCI-DSS Compliance Technique

วันจันทร์ที่ 17 ตุลาคม 2565

เวลา 14.00-15.00 น.

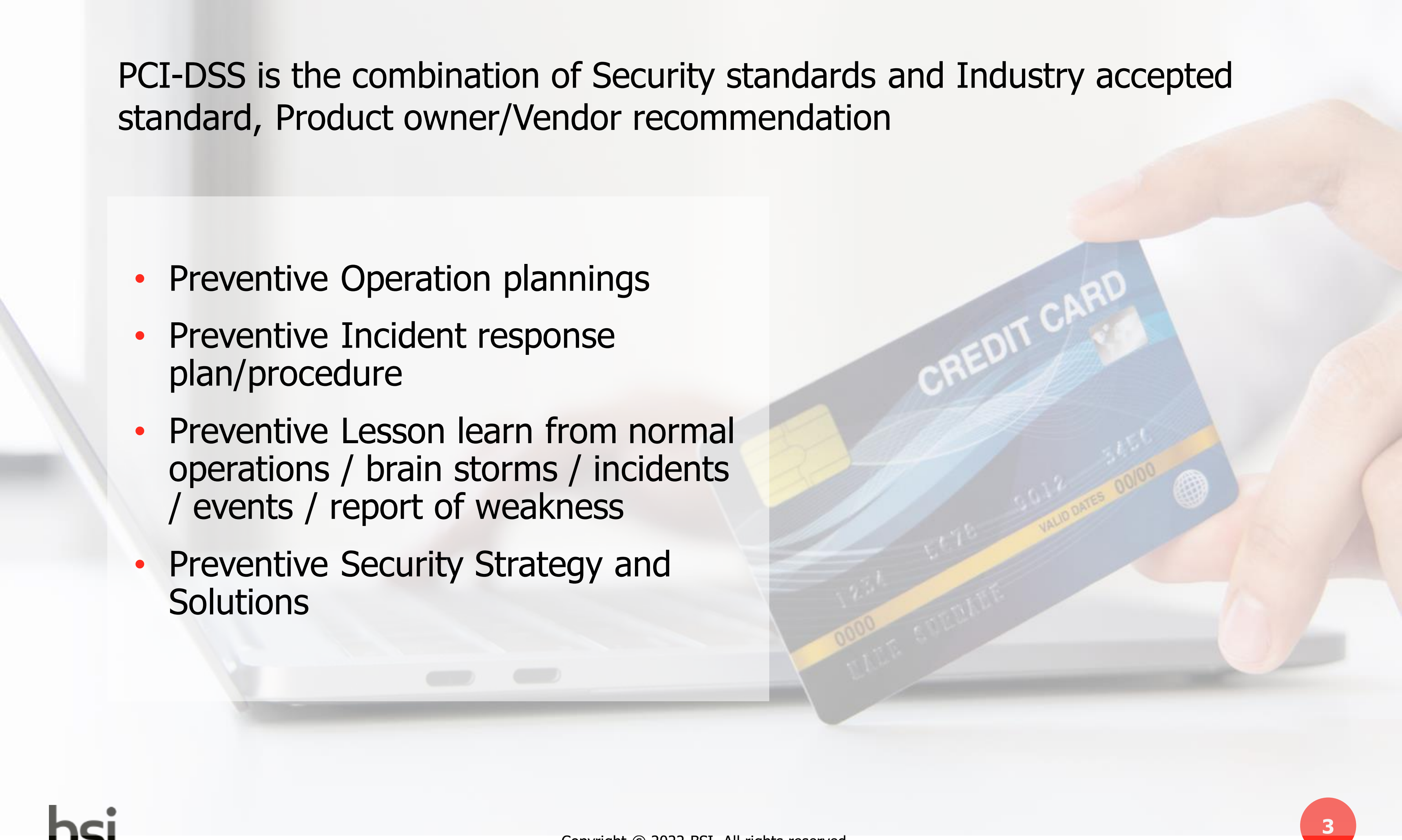
Presented by QSA Bancha Faungfu
Regional IS & IT Group Administrator
PCI-DSS QSA, Client Manager & Instructor
SMS, ISMS, PIMS, BCMS, CSA, PCI-DSS

By Royal Charter

Course aim and brief discussion

1. ใช้มาตรฐานอย่างไรให้ได้ประโยชน์
2. วิธีการรับการตรวจ PCI-DSS ให้ผ่านได้อย่างไม่ยาก
3. วิธีรักษามาตรฐานให้คงอยู่ แม้จะมีอุปสรรค

● ใช้มาตรฐานอย่างไรให้ได้ประโยชน์



PCI-DSS is the combination of Security standards and Industry accepted standard, Product owner/Vendor recommendation

- Preventive Operation plannings
- Preventive Incident response plan/procedure
- Preventive Lesson learn from normal operations / brain storms / incidents / events / report of weakness
- Preventive Security Strategy and Solutions

- วิธีการรับการตรวจ PCI-DSS ให้ผ่านได้อย่างไม่ยาก

สำหรับ Initial stage

สำหรับ Annually certification stage

สำหรับ Merchant and Service provider (Partial of 3, 9, 12)

สำหรับ Financial services (Full or Partial of 1-12)

สำหรับ Both and More (Full and/or Partial of 1-12)

bsi.

- วิธีการรับการตรวจ PCI-DSS ให้ผ่านได้อย่างไม่ยาก

2.1 Clear scope coverage & understanding

- Nature of organization: Merchant / Service provider (Datacenter, Payment gateway, etc) / Financial institution (Acquirer / Issuer) / Both and more
- Processes: Receives to Stores and Stores to Processes and Processes to Transmits
- Type of payment channels for Card present/not present: eCommerce Website / Portal / Interface / POS / Mobile Application / Applications and more

● วิธีการรับการตรวจ PCI-DSS ให้ผ่านได้อย่างไม่ยาก

2.2 Clear Diagrams

- Network diagram detail

- All connections > In & Out of scope,

- Wire, Wireless and others,

- All environments Public; Private; Extranet; Intranet; DMZ; Internal; Authorization; NTP; Antivirus; Logging, etc)

- Data flow diagram (Capture; Authorization; Settlement; Chargeback; etc)
- All active and to be inactive environment in all locations

bsi.

2.3 Clear Inventory

- Deeper detail of inventory:
  (Type; Vendor; Vendor URL; Latest Firmware/Software version with release date; Latest Update/Patch [Critical/Recommend with release date]; Latest action with change numbers
- Cover all environment
  (People, Processes, Technologies, Locations and others)
- Card holder storage
  (From input to databases; Active transaction files; Active process, History, Logs, Trace file, Temporary files; Others)
- Hardware, Software in Card holder data environment
- 3rd party applications/solutions with product version, PCI-DSS/PA/P2PE validated status; PCI SCC reference number; Expiry date of listing on PCI SSC

2.4 Clear Documentation and Usage of policies/procedure **(at least annually reviewed)**

Documentations

- Policies and Procedures
- High level network diagram
- Data flow diagram with steps from start to the end of all processes
- Data flow diagram with steps from start to the end of all processes
- Roles and Responsibilities assignment for all personnel [NOT POCITION BASED] (Management, Process owner and Operators)
- Logs
- Awareness Training records
- Roles and Responsibilities Acknowledgement in writings
- Scanning results (Segmentation; VA; ASV; etc)
- Quarterly Compliance testing/checking

2.4 Clear Documentation and Usage of policies/procedure **(at least annually reviewed)**

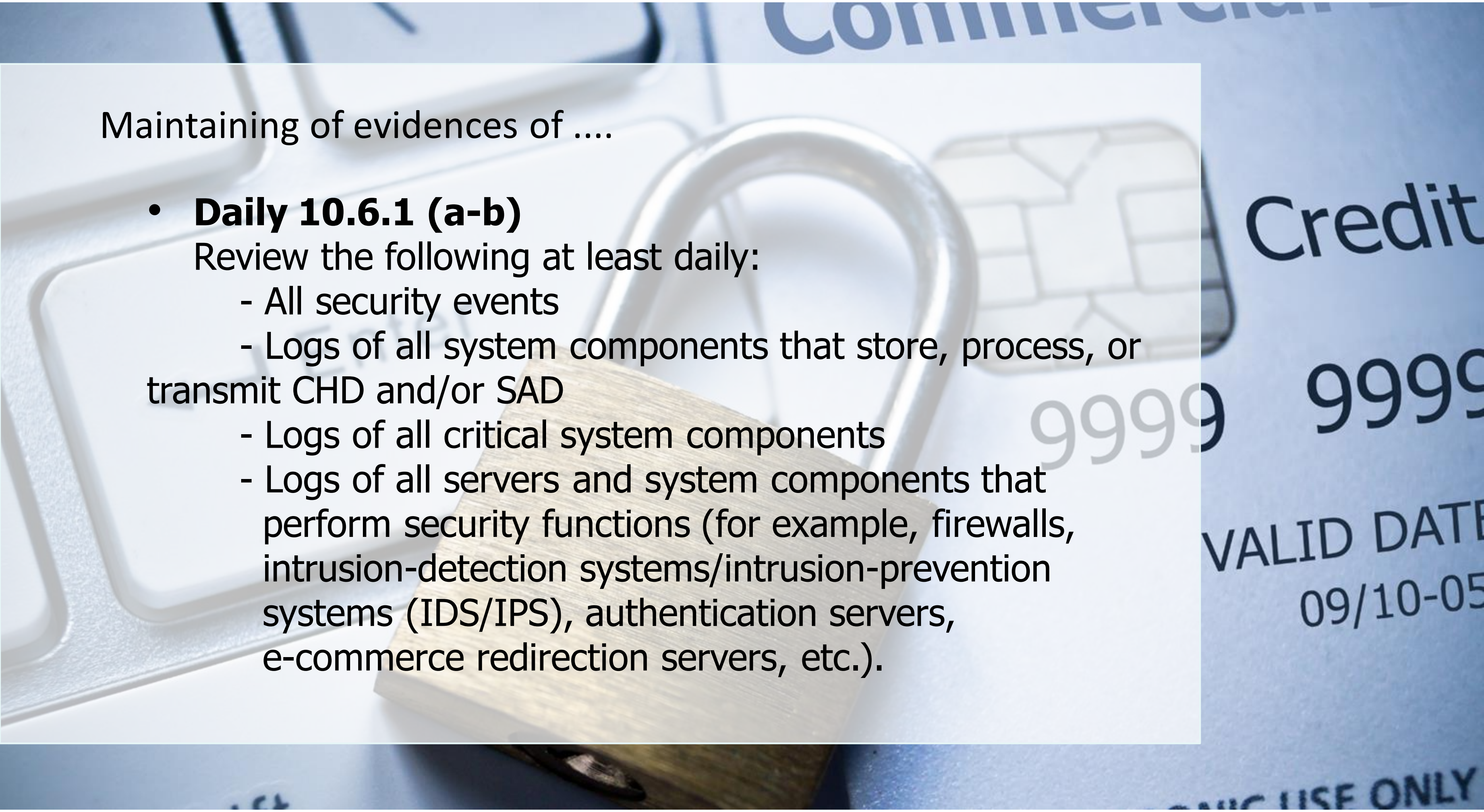
Standard - Policy - procedure

- Change management
- Asset inventory and Asset management
- Physical security
- Security / Network security / ISMS / PIMS
- Vulnerability and System Hardening
- User management
- Cryptography and Key management
- Vulnerability management
- Software development
- Disposal
- PCI DSS and Security Awareness programme
- PCI DSS and Security Awareness training
- Privilege management (MFA and etc)
- Security Incident Response more...

2.5 Clear understandings on Work to be verified by QSA

- Segmentation, Existence of Card holder data
- Security controls
- Access managements
- Card holder management process (Information displays; Database received; stored; transfer; display and accessibilities)
- est on How to access (Security control coverage and applied to)
- Test on credentials (Control of Accounts and passwords)
- Test on secure connections and functions (Secure and Insecure - Encryptions, Ports, services etc)
- Test on one primary functions with security controls
- Test on management of insecure(s)
- Test on all documentations and Support evidences
- Test on time and timing
- Test on availability and usable of information

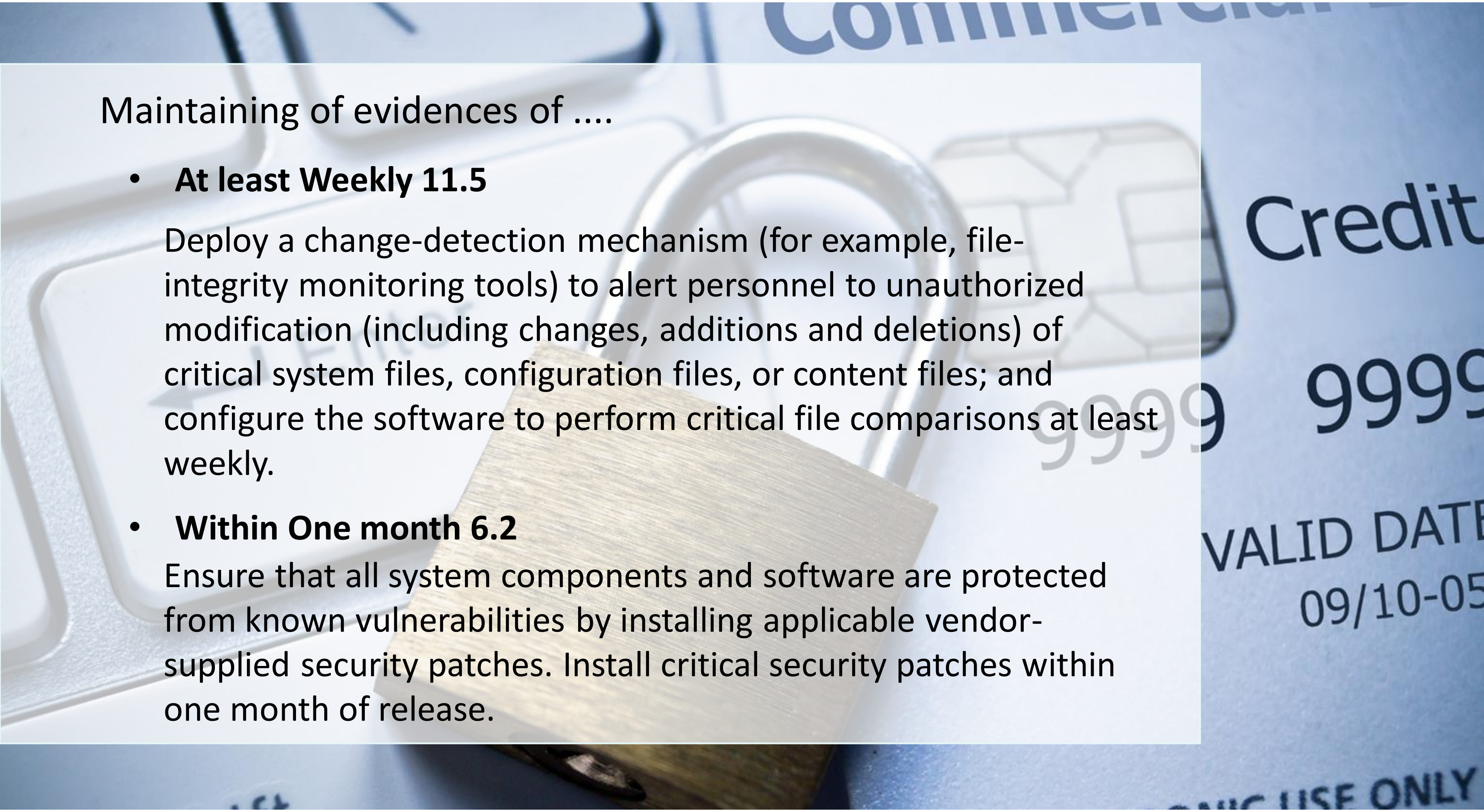
• วิธีรักษามาตรฐานให้คงอยู่ แม้จะมีอุปสรรค



Maintaining of evidences of ....

- **Daily 10.6.1 (a-b)**
  Review the following at least daily:
  - All security events
  - Logs of all system components that store, process, or transmit CHD and/or SAD
  - Logs of all critical system components
  - Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

● วิธีรักษามาตรฐานให้คงอยู่ แม้จะมีอุปสรรค



Maintaining of evidences of ....

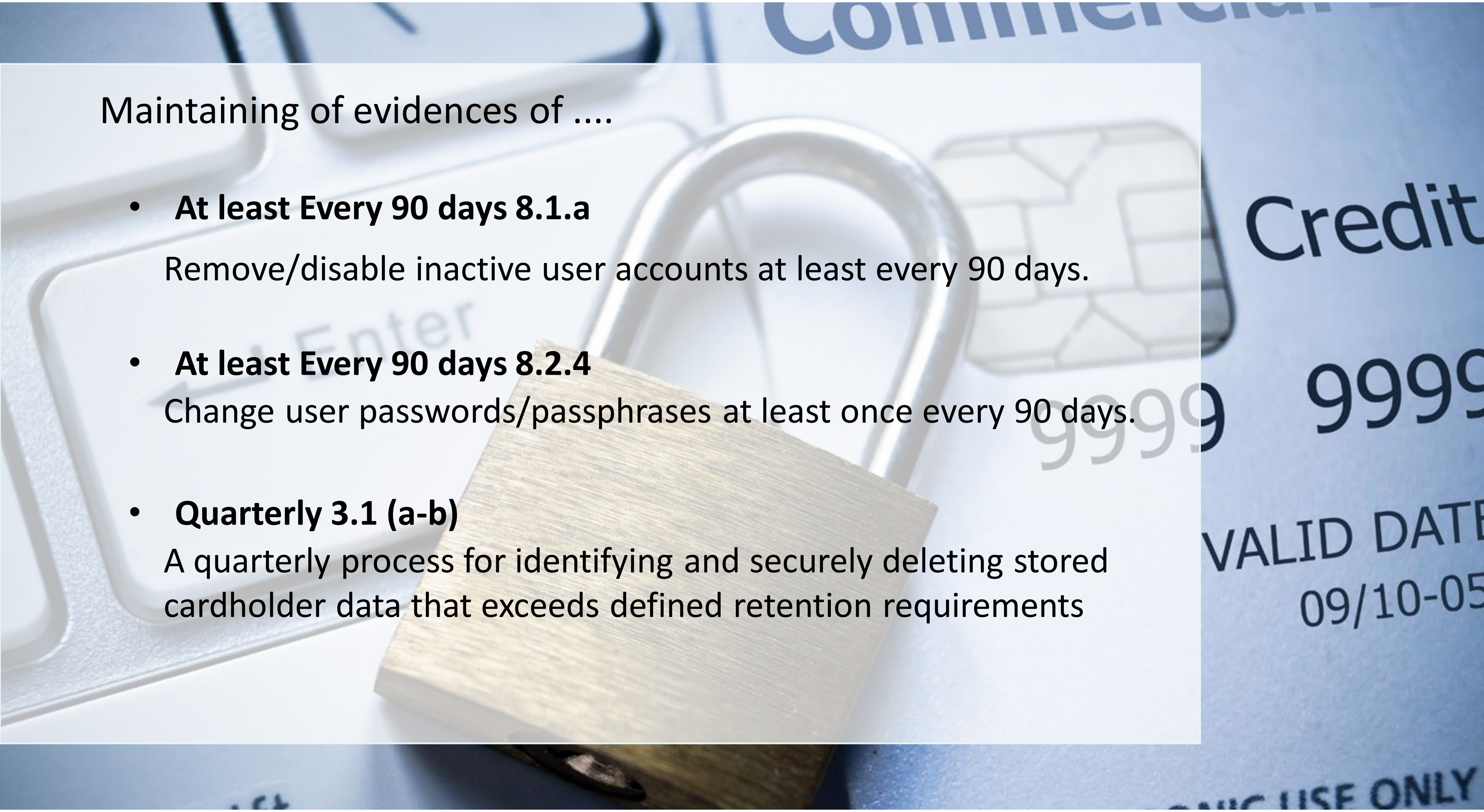
- **At least Weekly 11.5**

  Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

- **Within One month 6.2**

  Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

● วิธีรักษามาตรฐานให้คงอยู่ แม้จะมีอุปสรรค



Maintaining of evidences of ....

- **At least Every 90 days 8.1.a**

  Remove/disable inactive user accounts at least every 90 days.

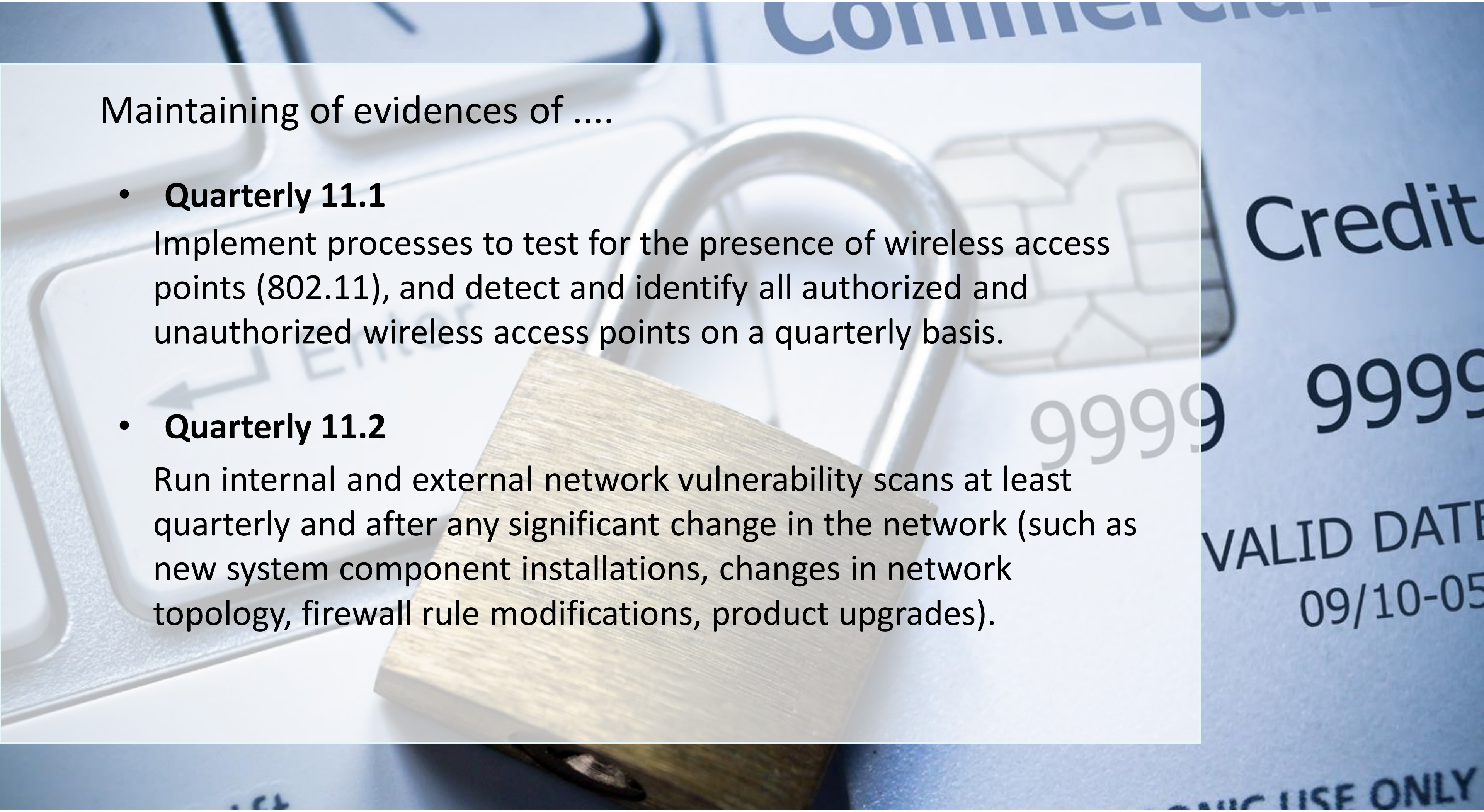
- **At least Every 90 days 8.2.4**

  Change user passwords/passphrases at least once every 90 days.

- **Quarterly 3.1 (a-b)**

  A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements

● วิธีรักษามาตรฐานให้คงอยู่ แม้จะมีอุปสรรค



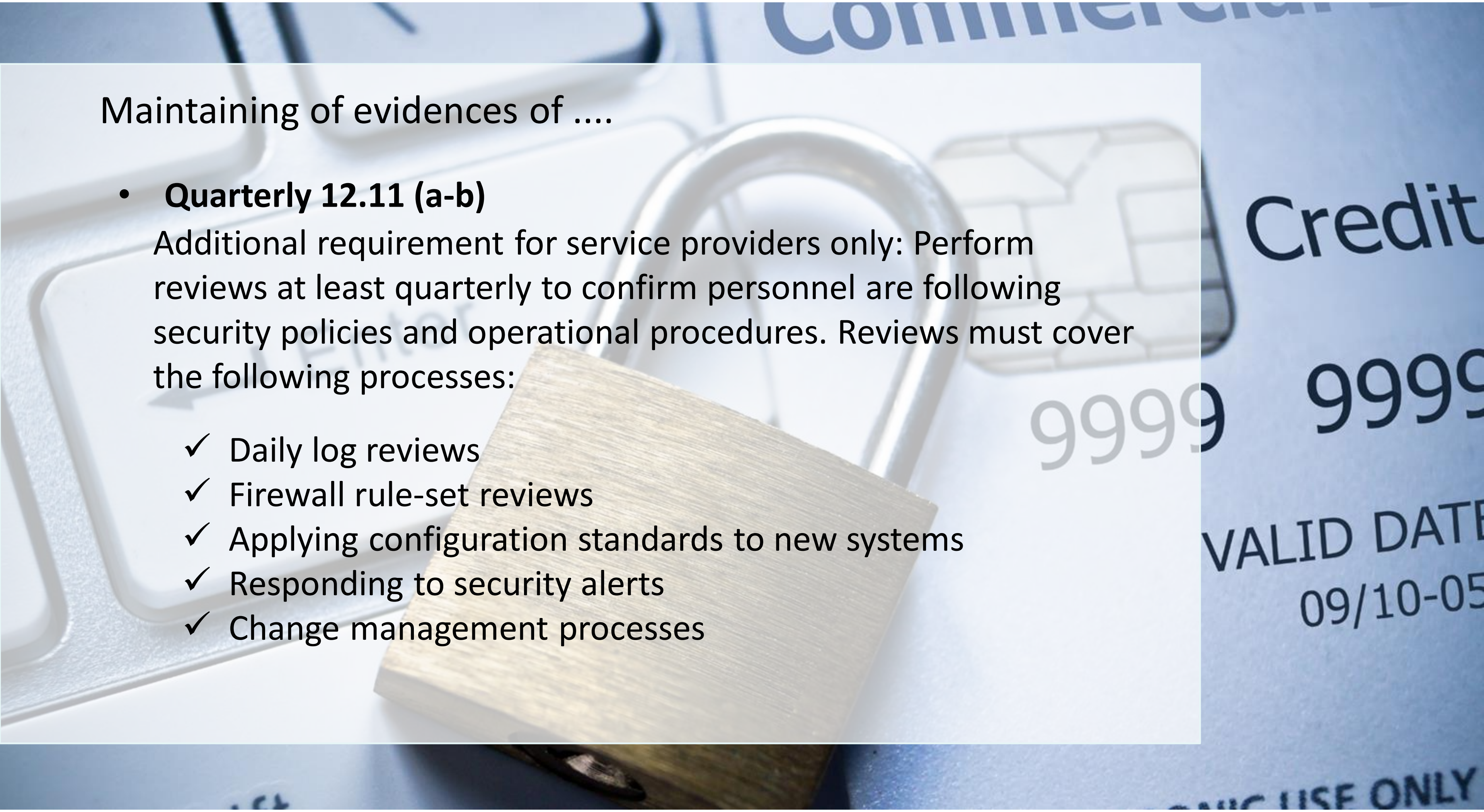
Maintaining of evidences of ....

- **Quarterly 11.1**
  Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.

- **Quarterly 11.2**

  Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

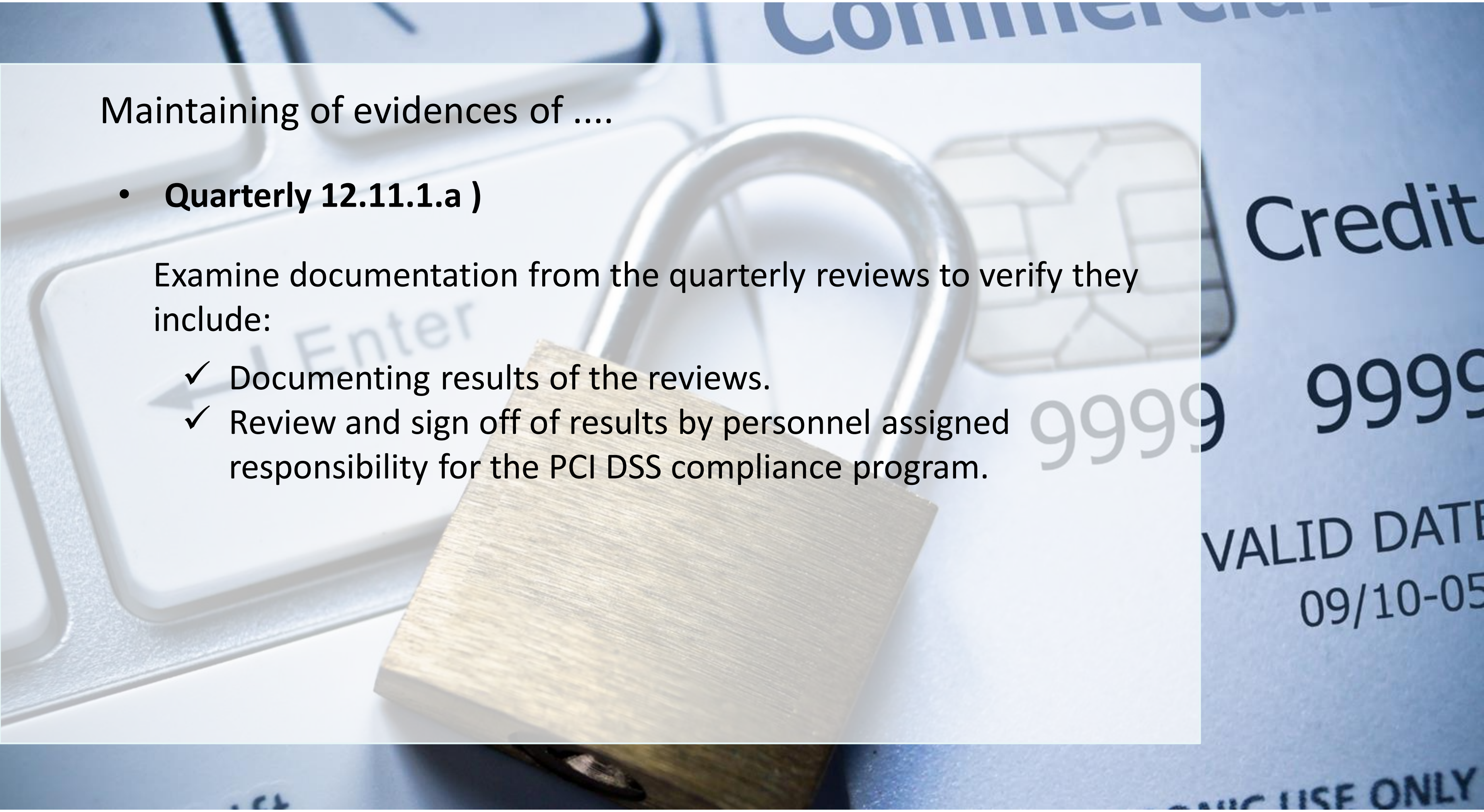
วิธีรักษามาตรฐานให้คงอยู่ แม้จะมีอุปสรรค



Maintaining of evidences of ....

- **Quarterly 12.11 (a-b)**
  Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes:
  - ✓ Daily log reviews
  - ✓ Firewall rule-set reviews
  - ✓ Applying configuration standards to new systems
  - ✓ Responding to security alerts
  - ✓ Change management processes

วิธีรักษามาตรฐานให้คงอยู่ แม้จะมีอุปสรรค



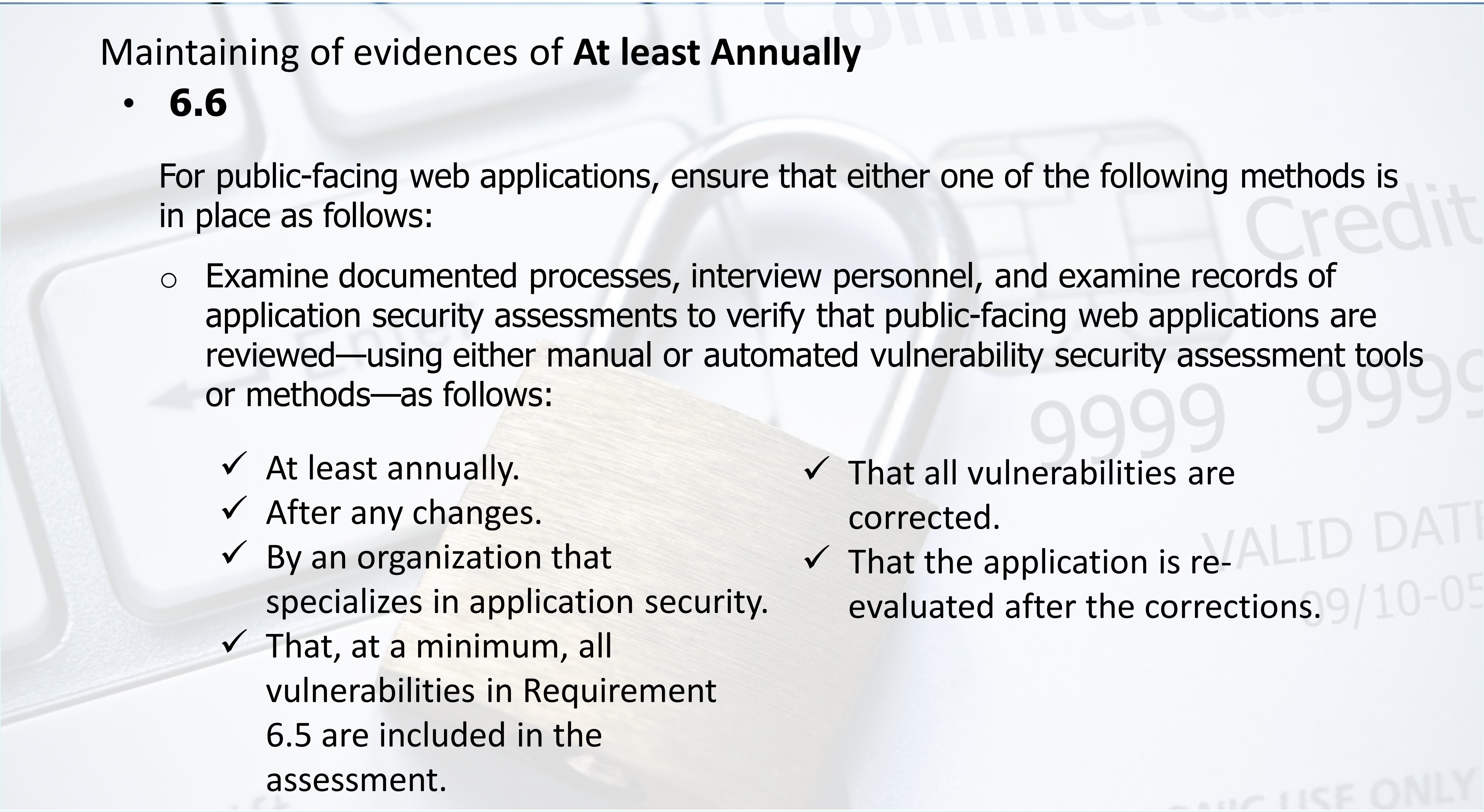
Maintaining of evidences of ....

- **Quarterly 12.11.1.a)**

  Examine documentation from the quarterly reviews to verify they include:

  ✓ Documenting results of the reviews.
  ✓ Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program.

● วิธีรักษามาตรฐานให้คงอยู่ แม้จะมีอุปสรรค



Maintaining of evidences of **At least Annually**

- **6.6**

For public-facing web applications, ensure that either one of the following methods is in place as follows:

○ Examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed—using either manual or automated vulnerability security assessment tools or methods—as follows:

✓ At least annually.

✓ After any changes.

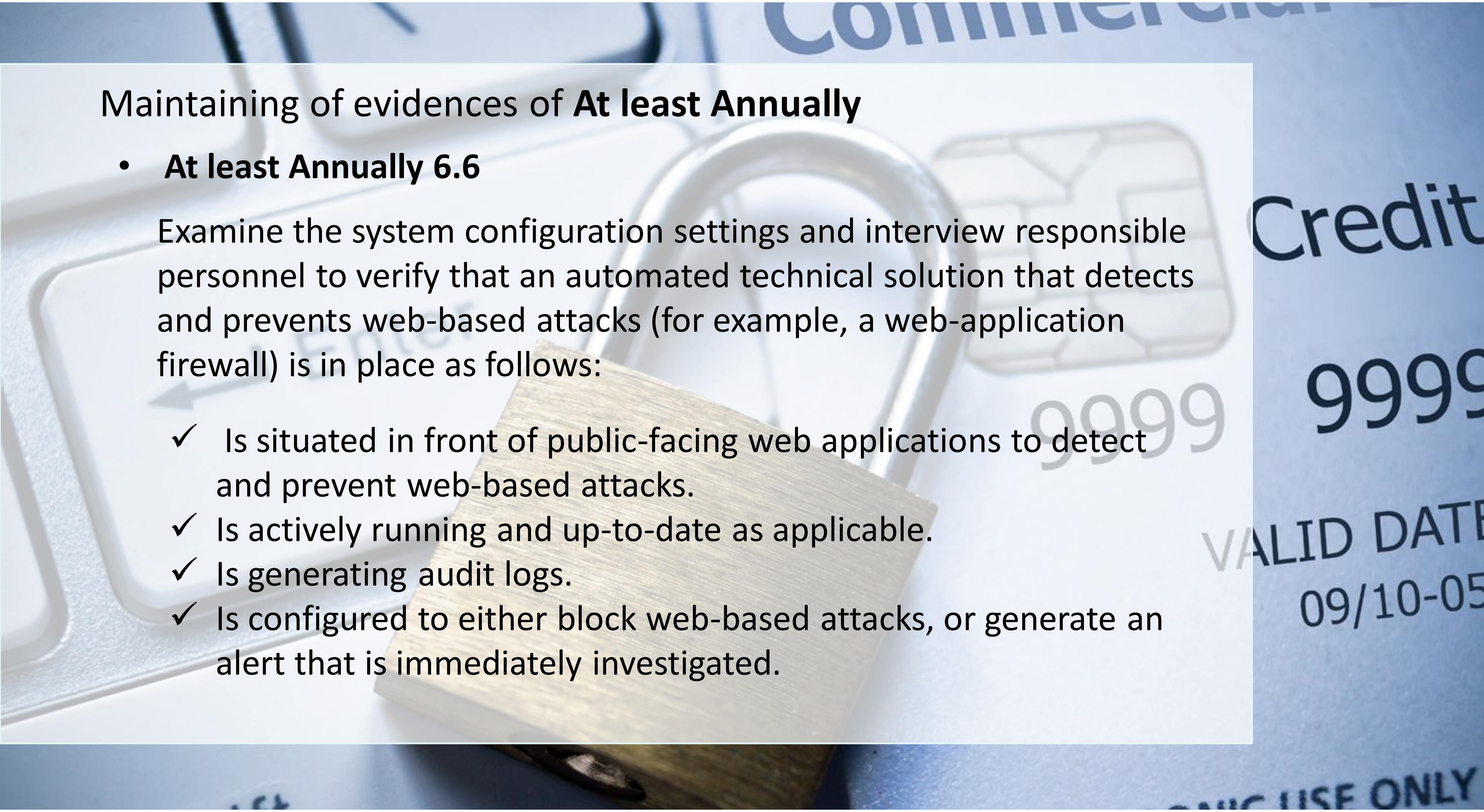
✓ By an organization that specializes in application security.

✓ That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment.

✓ That all vulnerabilities are corrected.

✓ That the application is re-evaluated after the corrections.

● วิธีรักษามาตรฐานให้คงอยู่ แม้จะมีอุปสรรค



Maintaining of evidences of **At least Annually**

- **At least Annually 6.6**

Examine the system configuration settings and interview responsible personnel to verify that an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is in place as follows:

✓ Is situated in front of public-facing web applications to detect and prevent web-based attacks.

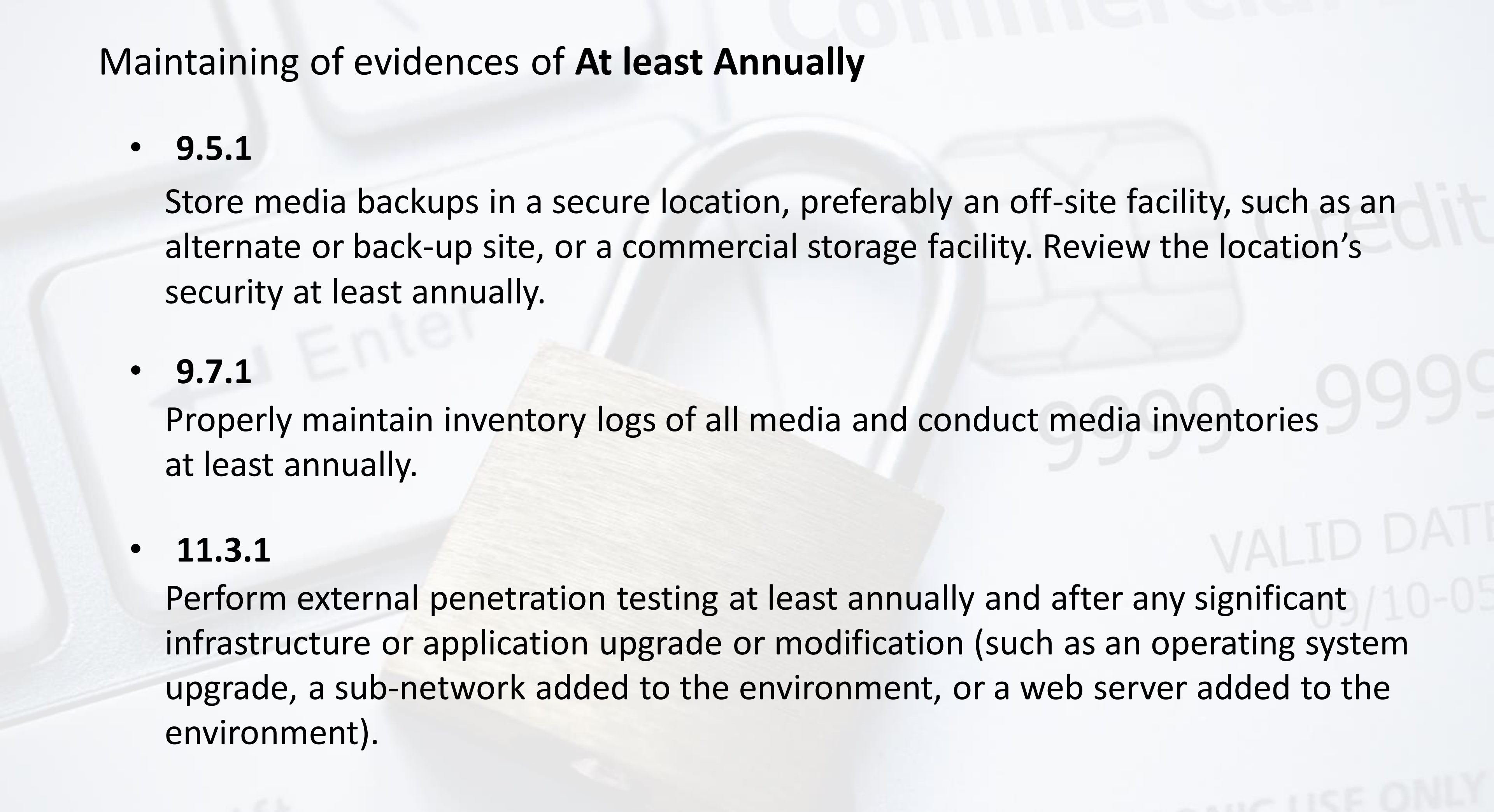
✓ Is actively running and up-to-date as applicable.

✓ Is generating audit logs.

✓ Is configured to either block web-based attacks, or generate an alert that is immediately investigated.

bsi.

● วิธีรักษามาตรฐานให้คงอยู่ แม้จะมีอุปสรรค



Maintaining of evidences of **At least Annually**

- **9.5.1**

  Store media backups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.

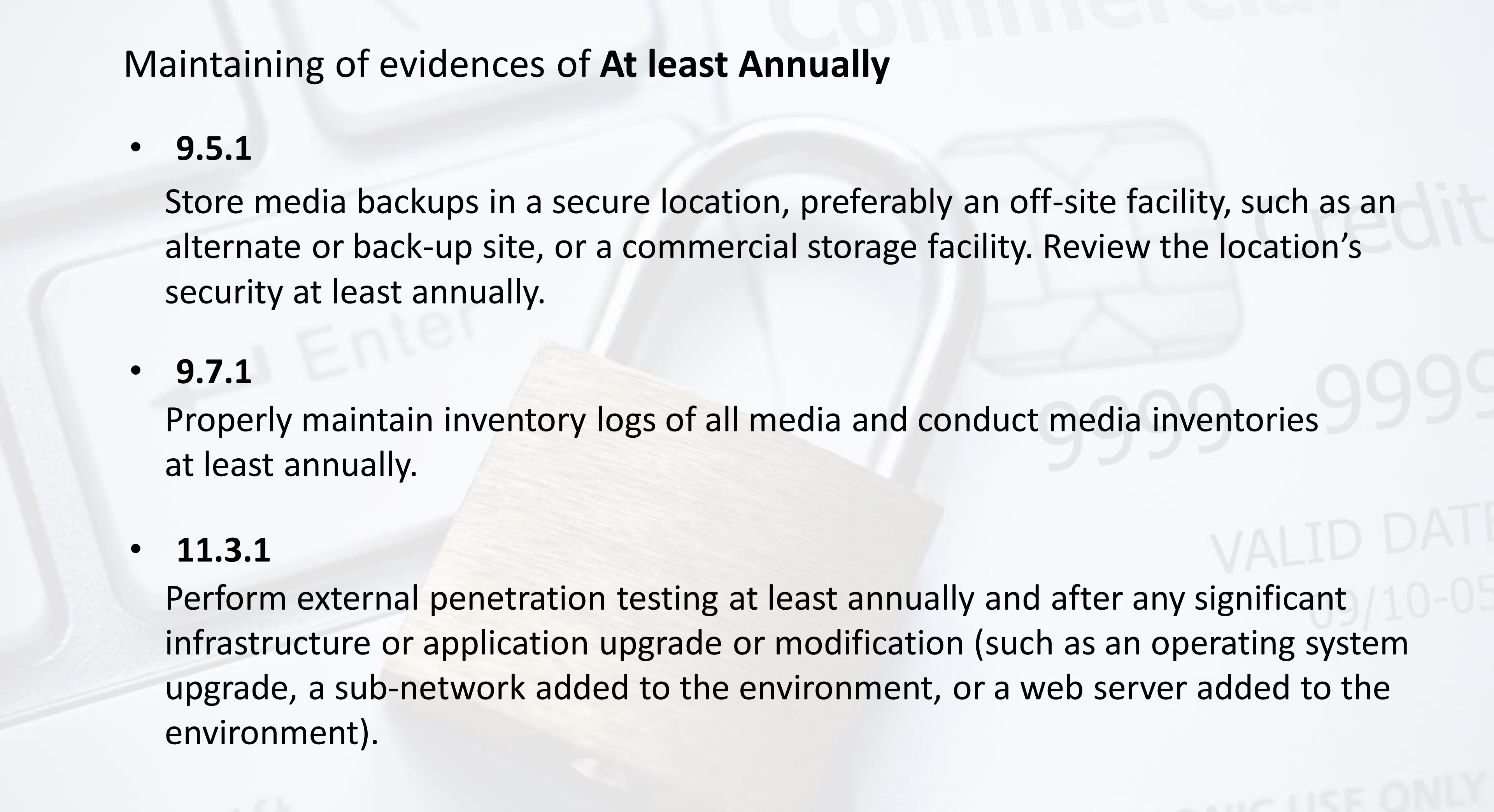
- **9.7.1**

  Properly maintain inventory logs of all media and conduct media inventories at least annually.

- **11.3.1**

  Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

วิธีรักษามาตรฐานให้คงอยู่ แม้จะมีอุปสรรค



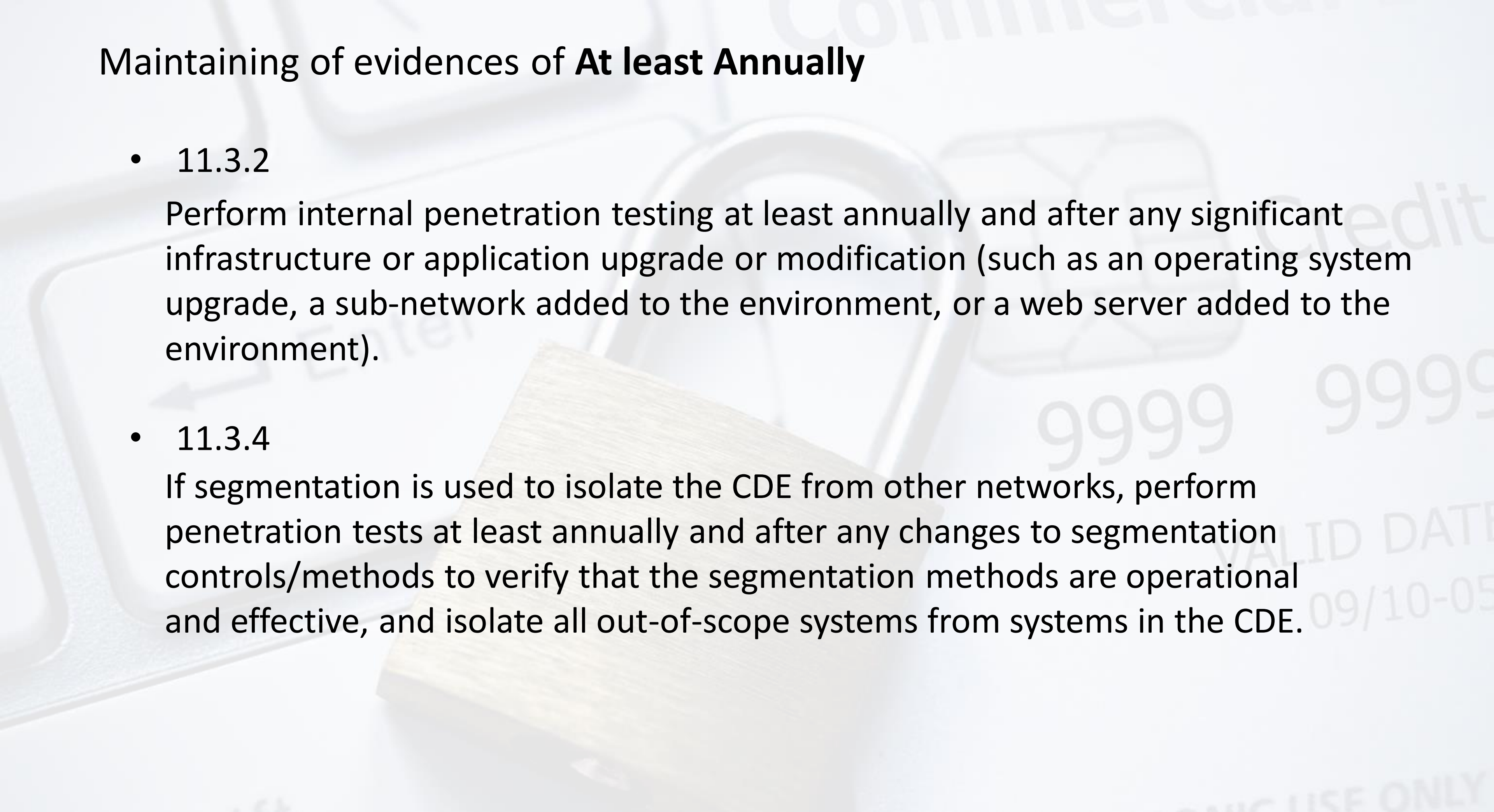
Maintaining of evidences of **At least Annually**

- **9.5.1**
  Store media backups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.

- **9.7.1**
  Properly maintain inventory logs of all media and conduct media inventories at least annually.

- **11.3.1**
  Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

● วิธีรักษามาตรฐานให้คงอยู่ แม้จะมีอุปสรรค



Maintaining of evidences of **At least Annually**

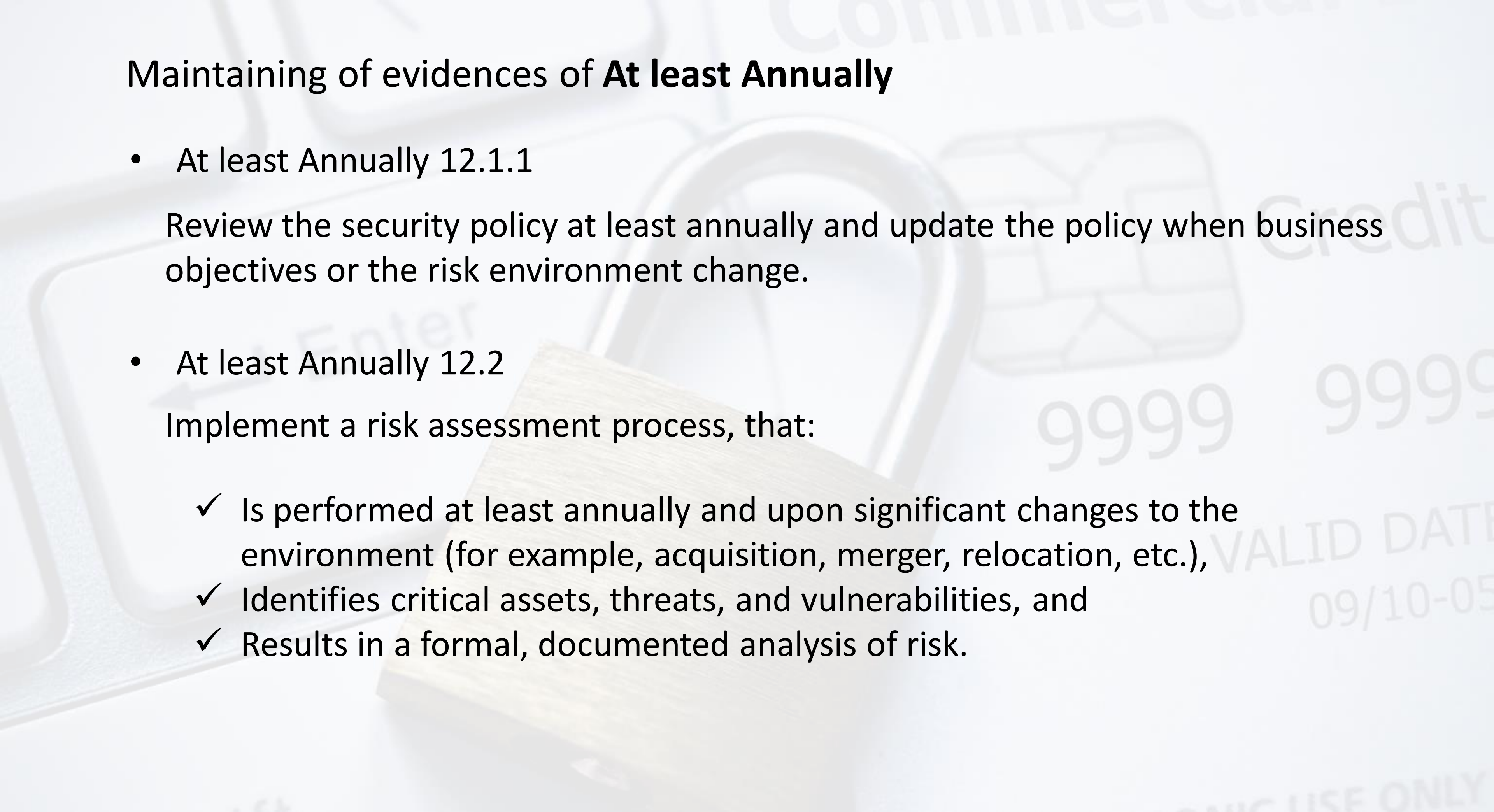
- 11.3.2

  Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

- 11.3.4

  If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.

● วิธีรักษามาตรฐานให้คงอยู่ แม้จะมีอุปสรรค



Maintaining of evidences of **At least Annually**

- At least Annually 12.1.1

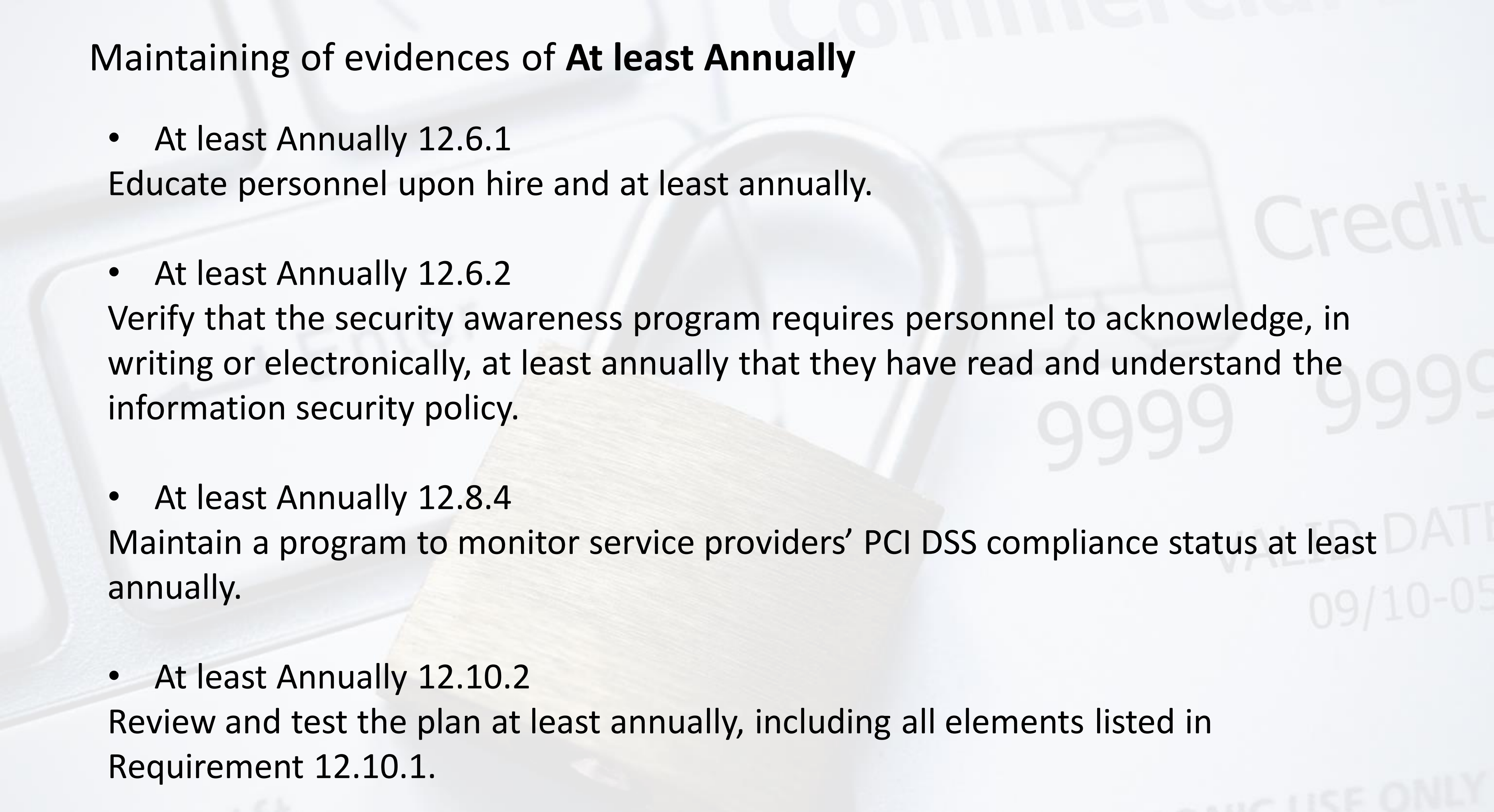
Review the security policy at least annually and update the policy when business objectives or the risk environment change.

- At least Annually 12.2

Implement a risk assessment process, that:

- ✓ Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.),
- ✓ Identifies critical assets, threats, and vulnerabilities, and
- ✓ Results in a formal, documented analysis of risk.

วิธีรักษามาตรฐานให้คงอยู่ แม้จะมีอุปสรรค



Maintaining of evidences of **At least Annually**

- At least Annually 12.6.1

Educate personnel upon hire and at least annually.

- At least Annually 12.6.2

Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy.

- At least Annually 12.8.4

Maintain a program to monitor service providers’ PCI DSS compliance status at least annually.

- At least Annually 12.10.2

Review and test the plan at least annually, including all elements listed in Requirement 12.10.1.

- **Thank you for participating**

Address:	BSI Group (Thailand) Co., Ltd. 127/29 Panjathani Tower, 24th Fl. Nonsee Road, Chongnonsee, Yannawa, Bangkok 10120
Tel:	02 294 4889-92
Fax:	02 294 4467
Email:	infothai@bsigroup.com
Web:	www.bsigroup.com/en-th