**Information security audit plan for LDIL.DE**

**Auditing and Testing Technical Security**

Group A

Bachelor’s thesis or Master’s thesis

January 2018

Technology, communication and transport

Cyber Security

|  |  |  |
| --- | --- | --- |
| jamk_fi_tunnus_sininen | | **Description** |
| Author(s)  Last name, First name | Type of publication  Master’s thesis | Date Month Year |
| Language of publication: |
| Number of pages | Permission for web publication: x |
| Title of publication  **Title**  Possible subtitle | | |
| Degree programme | | |
| Supervisor(s)  Last name, First name | | |
| Assigned by | | |
| Abstract  When completing this form, start from this field, on the row under the instructions, so that the font size remains 11.  The basic structure of the abstract is as follows:   * background * task and objectives * implementation method * results * conclusions.   In other words, the abstract summarises the work that has been done – not the content of the report. If there is room, the content of the report may be briefly mentioned.  The entire space reserved for the abstract must be used.  The abstract should be written in the past tense and with a passive voice. The text must not refer to the thesis, i.e., the words ‘this thesis’ must not be used. | | |
| Keywords/tags ([subjects](https://janet.finna.fi/Search/Results?lookfor=asiasanastot&prefiltered=format_Database&SearchForm_submit=Find&retainFilters=0&filter%5b%5d=format%3A%220%2FDatabase%2F%22&lng=en-gb)) | | |
| Miscellaneous ([Confidential information](https://intra.jamk.fi/opiskelijat/student/thesis/Pages/publicity.aspx)) | | |

**Contents**

[1 Introduction 3](#_Toc502949428)

[2 Audit target 3](#_Toc502949429)

[3 Applicability 4](#_Toc502949430)

[3.1 Scoping 4](#_Toc502949431)

[4 Auditors 5](#_Toc502949432)

[5 Audit activities and schedule 5](#_Toc502949433)

[5.1 Schedule and premilinary work estimate 5](#_Toc502949434)

[5.2 Administrative and technical reviews of named technologies 5](#_Toc502949435)

[5.2.1 Network and systems security 5](#_Toc502949436)

[5.2.2 Configuration defaults 6](#_Toc502949437)

[5.2.3 Data protection 6](#_Toc502949438)

[5.2.4 Security of data transmissions 6](#_Toc502949439)

[5.2.5 Malware protection 6](#_Toc502949440)

[5.2.6 Secure systems and applications 7](#_Toc502949441)

[5.2.7 Access restrictions to data 7](#_Toc502949442)

[5.2.8 Access restrictions to systems 7](#_Toc502949443)

[5.2.9 Monitoring and testing 7](#_Toc502949444)

[5.2.10 Testing security systems and processes 8](#_Toc502949445)

[5.2.11 Information security policy 8](#_Toc502949446)

[6 Reporting 8](#_Toc502949447)

[References 9](#_Toc502949448)

**Figures**

No table of figures entries found.

**Tables**

**No table of figures entries found.**

# Introduction

Audit plan presented in this document is a group exercise related to Auditing and Testing Technical Security course. Main focus in this exercise is to assess functions of target organization and based on this to choose suitable audit criteria/framework. The end result includes full audit plan for fictional e-tailing company LDIL.

# Audit target

LDIL is a national e-tailing company that also has one physical retail store with a POS-system. LDIL business environment consists of information systems and different network domains. Target of this evaluation is LDIL's systems and networks related to customer and payment information.

PCI DSS constructs the audit framework for this security audit for reasons which will be presented more closely later in this document. LDIL operates in multiple categories of the PCI DSS context. Due to the basic retail shop business the role of the LDIL mostly falls in the category of merchant and it uses payment services provided by creditbanken.de. There are only small differences in these roles regarding the audit, but these two roles define different regional laws that should be noted:

* Payment Service Law (2010/290)
* Payment Institution Law (2010/297)

PCI DSS comprises a minimum set of requirements, which can be enhanced by regional laws and regulations. In this audit the criteria is defined only through the PCI Data Security Standard, while dependencies related to regional laws are left as a note.

This audit will be conducted before 7.1.2018.

# Applicability

PCI DSS requirements apply to organizations or entities that store, process or transmit cardholder data or sensitive authentication data. LDIL is an e-commerce company that administers their own e-commerce platform and a point of sale systems at their branch store, thus making LDIL's payment system applicable to PCI DSS requirements.

Storage of sensitive authentication data is forbidden by PCI DSS. On top of PCI DSS requirements, payment card brands can have their own instructions whether storage is permitted prior to authorization. Individual payment card brands requirements are left out the scope of this audit and focus is kept on PCI DSS requirements.

## Scoping

Purpose of scoping is to determine which components of LDIL's business environment are part of cardholder data environment. Cardholder data environment comprises of LDIL's payment system components and all other connected systems.

Determining the scale of cardholder data environment is done by reviewing LDIL's provided documentation of the current business environment and security measures. Once the cardholder data environment and cardholder data flow in the payment system is identified and documented, the determined PCI DSS scope is reviewed by the LDIL before beginning the assessment.

According to documentation LDIL cardholder data environment consists of the following systems (according to LDIL documentation fig. 1, page 8):

* Magento server (e-commerce platform, payment system component)
* All other hosts in DMZ network segment (located at the same segment as Magento)
* POS Cyclos (payment system component)
* All other hosts in Store branch network segment (located at the same segment as POS)
* Paloalto and PFSense firewalls (essential network infrastructure)

Magento and Cyclos should be studied at application level to have greater knowledge about their functionality. If applications use for example external database server it has impact on the scope of cardholder data environment.

# Auditors

Head auditors in this audit will be Jouni and Petri. Their responsibility will be the execution of the audit and possible focus changes during the evaluation. Supplementary auditors are Pauli, Jani, Otso, Vesa, Pinja, Teemu and Janne.

# Audit activities and schedule

## Schedule and premilinary work estimate

Audit is planned to be started during December 2017 and finalized in January 2018. Results of the audit will be presented during lectures in 12.1. – 13.1.2018.

Premilinary work estimate:

* Reviewing the material, planning and technical implementation: 32 h
* Review of administration and monitoring systems: 16 h
* Review of the ISMS including administration procedures and practices: 24 h
* Review of business continuity: 16 h
* Review of reporting procedures: 16 h
* Reporting: 16 h
* Total: 120

## Administrative and technical reviews of named technologies

### Network and systems security

Technical review

* Review of firewall rules and configurations against the documentation using manual portscanning utilizing nmap and manual review of firewall policy configuration
* Verification of documented zoning using scans and traffic capture collected with tcpdump

Administrative review

* Review of the change management process concerning router and firewall configuration changes
* Secure and documented settings, including e.g. ports and protocols
* Network diagrams
* Administrative roles
* Regular configuration review

### Configuration defaults

Technical review

* Manual verification from configuration files that default passwords and other configuration parameters have been changed
* Hardening of systems reviewed using Nessus agent and manual configuration checks
* Separation of server roles reviewed manually by checking sudo and rbac configuration
* Confirm that unnecessary protocols, services etc. have been disabled using manual checks, nmap and nessus
* Review that secure administration channels are being utilized using traffic capture by tcpdump

Administrative review

* Configuration management

### Data protection

Technical review

* Manual verification that no undocumented cardholder data persists in the systems
* Manual verification that sensitive data is masked as depicted in the requirements
* Manual verification that the security of encryption and encryption keys are sufficient

Administrative review

* Documentation of storing cardholder data

### Security of data transmissions

Technical review

* Manual review of the configuration and analyzation of traffic capture generated by tcpdump to verify that required data is transferred properly encrypted

Administrative review

* Encryption strength
* Encryption policies

### Malware protection

Technical review

* Confirm that antivirus programs are installed in the necessary systems
* Verify that antivirus programs are regularly updated
* Manual verification that antivirus software can detect test malware

Administrative review

* Awareness of current virus and malware threath

### Secure systems and applications

Technical review

* Confirm from logs that software updates are regularly applied
* Confirm from e.g. Nessus logs that software is scanned for vulnerabilities
* Confirm from e.g. Nessus logs that outer edge of network is scanned for vulnerabilities and undocumented services

Administrative review

* Update procedures for software
* Identification of required updates
* Regular software scans
* Change control

### Access restrictions to data

Technical review

* Manual review from system configuration that unnecessary access to cardholder data is prevented

Administrative review

* Documentation of access rights

### Access restrictions to systems

Technical review

* Verify user identification from configurations
* Verify limitations of user access from sudo or rbac configuration
* Verify documented logging, connection and password policies

Administrative review

* User ID policy
* Password policy
* Training of personnel for secure settings

### Monitoring and testing

Technical review

* Verification of generated audit logs
* Confirm that separation of duties is applied to log systems
* Verify log retention

Administrative review

* Audit log policy
* Documented separation of duties

### Testing security systems and processes

Technical review

* Manually confirm that IDS/IPS and HIDS exists and is correctly configured and the existing intrusion detection systems raise alarms during network testing

Administrative review

* Policy for regular testing, scanning and penetration testing
* Existing scan reports

### Information security policy

Technical review

* N/A

Administrative review

* Security policy
* Risk assessment policy
* Usage policies
* Inventories and ownerships
* Information security management
* Training of personnel
* Personnel screening
* Incident response plan

# Reporting

Following documents will be provided during the audit:

* Plan of the compliance audit (this document)
* Incident reporting during the audit concerning critical findings
* Final audit documentation

Reporting will be done by using the PCI DSS reporting on compliance template available at <https://www.pcisecuritystandards.org/documents/PCI DSS-v3_2-ROC-Reporting-Template.pdf>. Audit author produces incident report from the possible findings and reports critical findings immediately when noticed.

Report will be distributed to the audit target organization and regulatory/legislative authority when applicable.

Report is classified as company confidential.

References