First Step To Web Application

(ISO 27001 vs PCIDSS vs 10 Ten OWASP)

faspay

Connecting Payment

LET'S BEGIN NOW!

HELLO! I AM...

Elias

System Development

2011 – Now - Faspay

SECTION 1

INTRODUCTION

REGULATION /GUIDANCE

WE MUST KNOW
WHAT THE
IMPORTANT THINGS.

- ISO 27001
- PCI DSS / PA DSS
- Peraturan Bank Indonesia Nomor 18/40/**PBI**/2016
- PP 11 Tahun 2008 (ITE) / PP 82 2012 Penyelengaraan Sistem dan Transaksi Elektronik / Permen No 4 TH 2016 Sistem ManajemenInformasi
- OWASP

Keamanan Informasi

Definisi :

Keamanan informasi merupakan perlindungan informasi dari berbagai ancaman agar menjamin kelanjutan proses bisnis, mengurangi risiko bisnis, dan meningkatkan *return of investment* (ROI) serta peluang bisnis (Chaeikar, etc., 2012). Meliputi aspek :

Confidentiality

Aspek yang menjamin kerahasiaan informasi atau data dan memastikan informasi hanya dapat diakses oleh pihak yang berwenang.

Integrity

Aspek yang menjamin data tidak dapat dirubah tanpa ada ijin pihak yang berwenang, menjaga kelengkapan informasi dan menjaga dari kerusakan atau ancaman lain yang bisa menyebabkan perubahan pada informasi atau data asli.

Availability

Aspek yang menjamin bahwa data akan tersedia pada saat dibutuhkan dan menjamin *user* dapat mengakses informasi tanpa adanya gangguan.

Similarities & Differences

Figure 2—High-level Mapping of PCI DSS Requirements to ISO/IEC 27001

PCI DSS Requirement	ISO/IEC 27001 Clause
1. Install and maintain a firewall configuration to protect cardholder data.	A.12 Operations security A.13 Communications security
2. Do not use vendor-supplied defaults for system passwords and other security parameters.	A.12 Operations security A.13 Communications security
3. Protect stored cardholder data.	A.12 Operations security A.13 Communications security
4. Encrypt transmission of cardholder data across open, public networks.	A.14 System acquisition, development and maintenance
5. Protect all systems against malware and regularly update antivirus software or programs.	A.14 System acquisition, development and maintenance
6. Develop and maintain secure systems and applications.	A.14 System acquisition, development and maintenance
7. Restrict access to cardholder data by business need to know.	A.12 Operations security A.13 Communications security
8. Identify and authenticate access to system components.	A.12 Operations security A.13 Communications security
9. Restrict physical access to cardholder data.	A.11 Physical and environmental security
10. Track and monitor all access to network resources and cardholder data.	A.12 Operations security A.13 Communications security
11. Regularly test security systems and processes.	A.14 System acquisition, development and maintenance A. 6 Organization of information security A.18 Compliance
12. Maintain a policy that addresses information security for all personnel.	A.5 Information security policies

Source: Tolga Mataracioglu. Reprinted with permission.

PCI DSS

Figure 7—The 14 Control Domains of ISO/IEC 27001

Control Domains	Number of Controls
A.5: Information security policies	2
A.6: Organization of information security	7
A.7: Human resources security	6
A.8: Asset management	10
A.9: Access control	14
A.10: Cryptography	2
A.11: Physical and environmental security	15
A.12: Operations security	14
A.13: Communications security	7
A.14: System acquisition, development and maintenance	13
A.15: Supplier relationships	5
A.16: Information security incident management	7
A.17: Information security aspects of business continuity management	4
A.18: Compliance	8
TOTAL:	114

Source: Tolga Mataracioglu. Reprinted with permission. Based on International Organization for Standardization, ISO/IEC 27002, Information technology—Security techniques—Code of practice for information security controls, *www.iso.org/iso/catalogue_detail?csnumber=54533*

ISO 27001

Similarities & Differences

A.5 Information Security **policies** (is related to requirement 12 of PCI-DSS)

A.6 Organization of information security (is related to requirement 12 of PCI-DSS)

A.7 Human resource security (is related to requirement 12 of PCI-DSS)

A.8 Asset management (is related to requirement 12 of PCI-DSS)

A.9 **Access control** (is related to requirement 7 of PCI-DSS)

A.10 **Cryptography** (is related to requirement 4 of PCI-DSS)

A.11 Physical and environmental security (is related to requirement 9 of PCI-DSS)

A.12 **Operations security** (is related to requirements 1, 5, 10, and 11 of PCI-DSS)

A.13 Communications security (is related to requirement 4 of PCI-DSS)

A.14 System acquisition, development and maintenance (is related to requirement 6 of PCI-DSS)

A.15 Supplier relationships

A.16 **Information security incident management**

A.17 Information security aspects of **business continuity** management

A.18 Compliance

SECTION 2

Synergy

Password Requirements

PCI DSS / PA DSS

PCI compliance password requirements as mandated by the Payment Card Industry Data Security Standards (PCI DSS) are clearly stated within Requirement 8

OWASP

A2:2017-Broken Authentication

Related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

ISO 27001

A.9 Access Control

Password management systems shall be interactive and shall ensure quality passwords.

PCI COMPLIANCE PASSWORD REQUIREMENTS

- Require a minimum length of at least seven characters.
- Contain both numeric and alphabetic characters.
- Users to change passwords at least every 90 day.
- Password parameters are set to require that new passwords cannot be the same as the four previously used passwords.
- First-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and changed after first use
- User accounts are temporarily locked-out after not more than six invalid access attempts.
- Once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.
- System/session idle time out features have been set to 15 minutes or less.
- Passwords are protected with strong cryptography during transmission and storage.

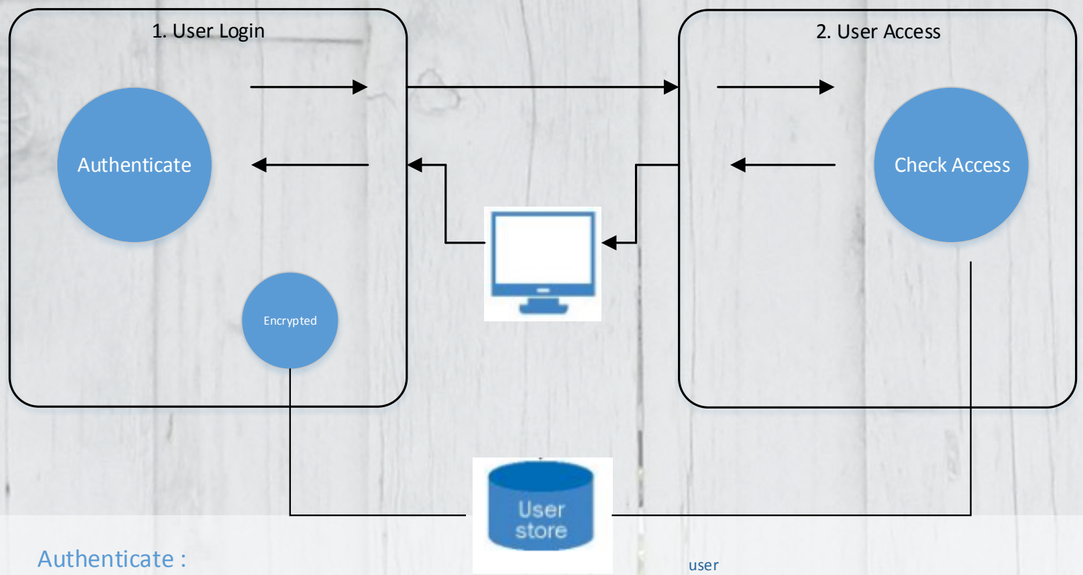
OWASP

- https://www.owasp.org/index.php/Authentication_Cheat_Sheet

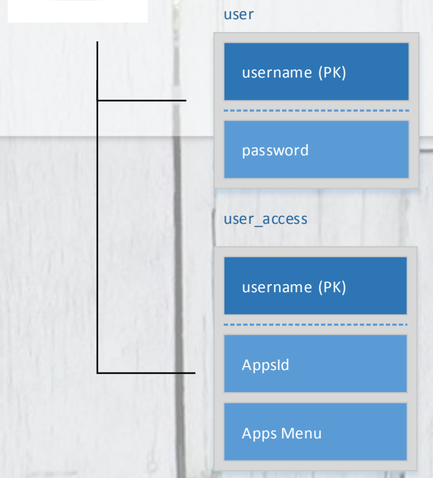
SECTION 3

DESIGN

DESIGN



Authenticate :
Function Length & Complexcity
Function ExpiryPassword
Function EncryptedPassword (Salt)



THANK YOU!

Do You Have Any Questions?