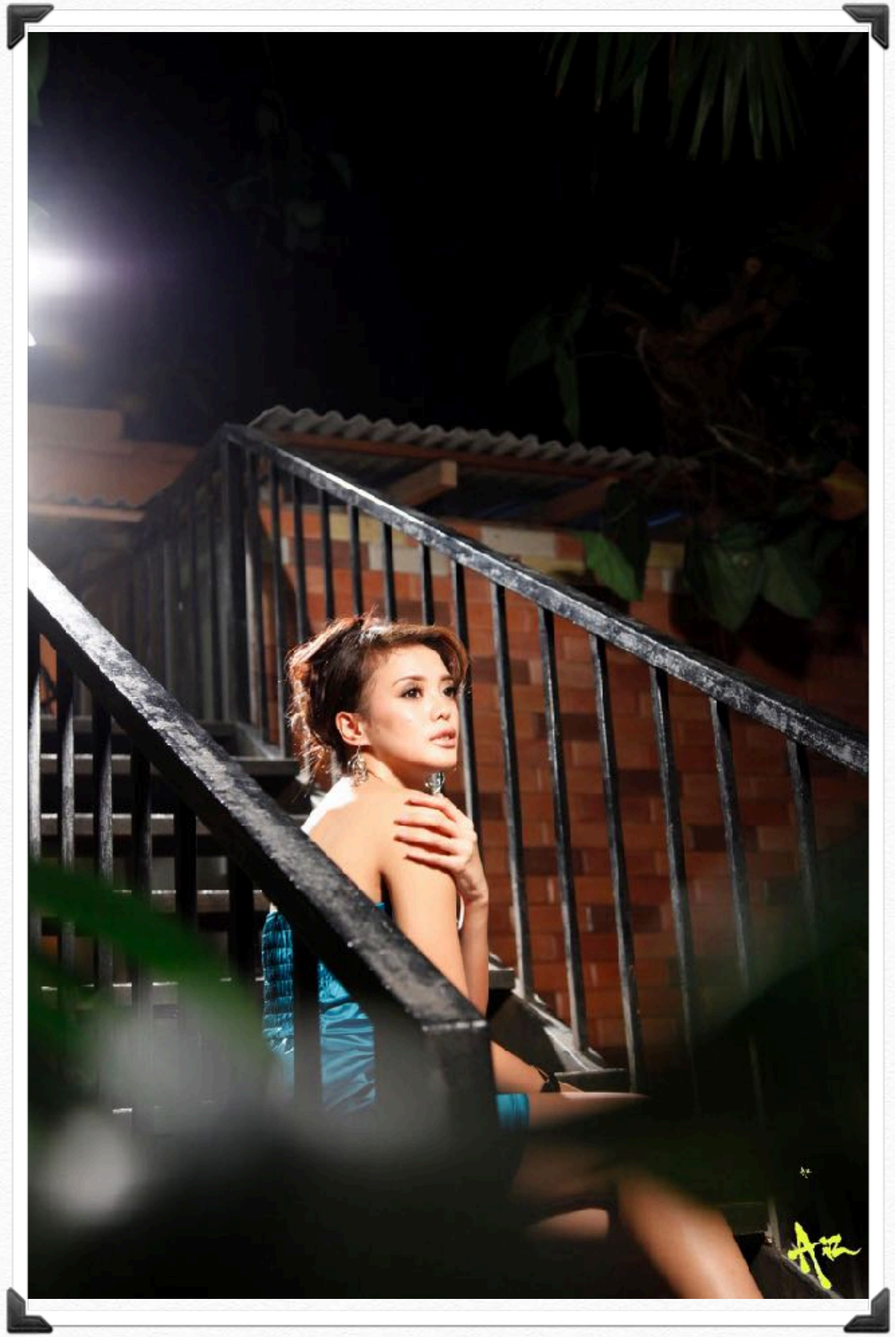
Server Hardening

Azis Kurniawan

Lembaga Sandi Negara
CISTECH.ID 2017



"Tidak ada yang aman di internet, tapi setidaknya usahakanlah yang terbaik untuk Anda"

About me

Azis Kurniawan

Pekerjaan:

Pengelola datacenter Communication and Command Center Lembaga Sandi Negara

Pendidikan: Sekolah Tinggi Sandi Negara (STSN), Teknik Kripto

Hobi: Fotografi

Pengalaman:

Programmer (JAVA, PHP, JavaScript, HTML5, Angular, C++, Mobile)

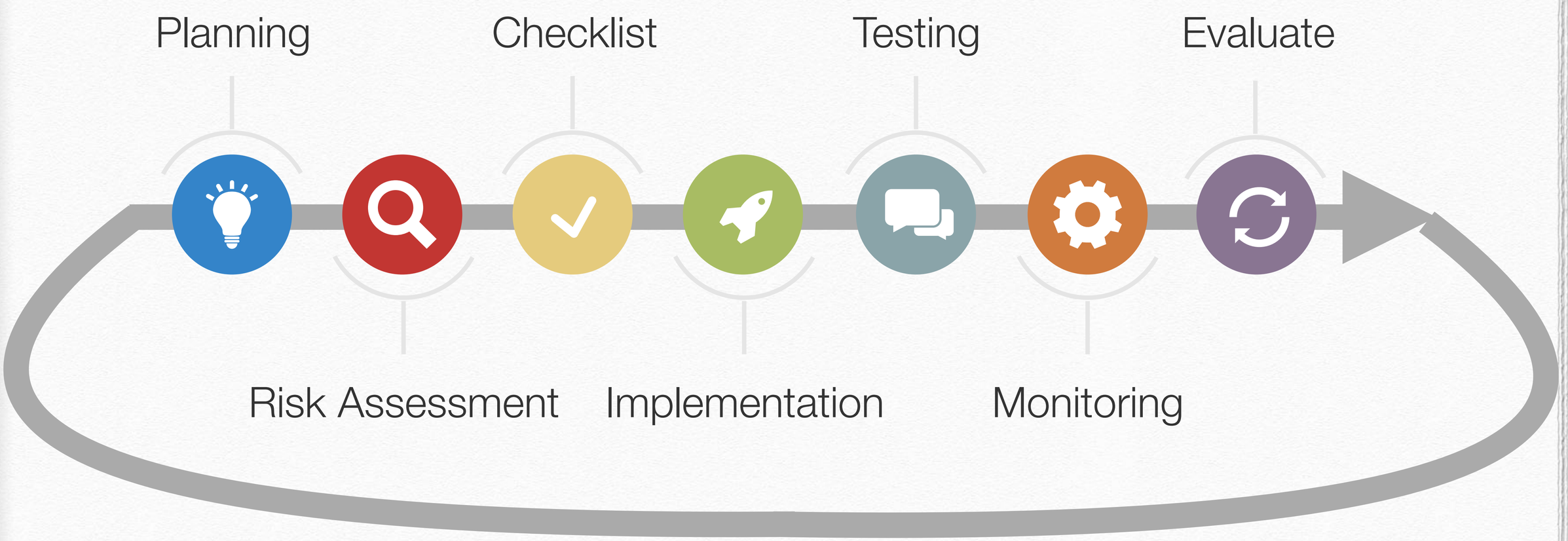
System administator (Windows Server, Linux, spesialisasi: FreeBSD)

Network engineer (CCNA)

Top 10 OWASP 2017 RC

OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

Server Hardening



Planning

Definisikan
service catalog

Instalasi server

Perkuat askes

Firewall rules

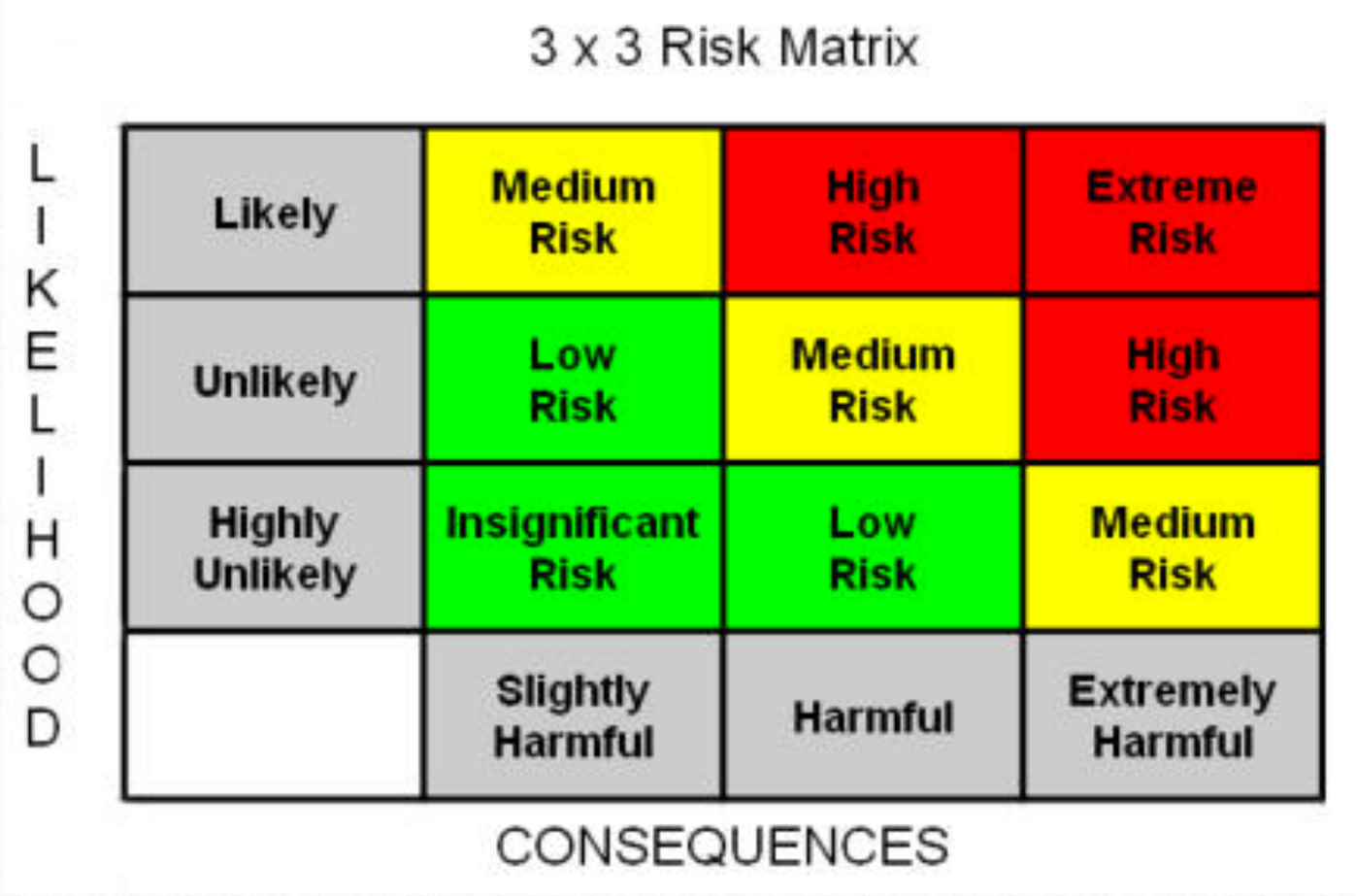
Akses
pengguna

Enkripsi

Keamanan
tambahan

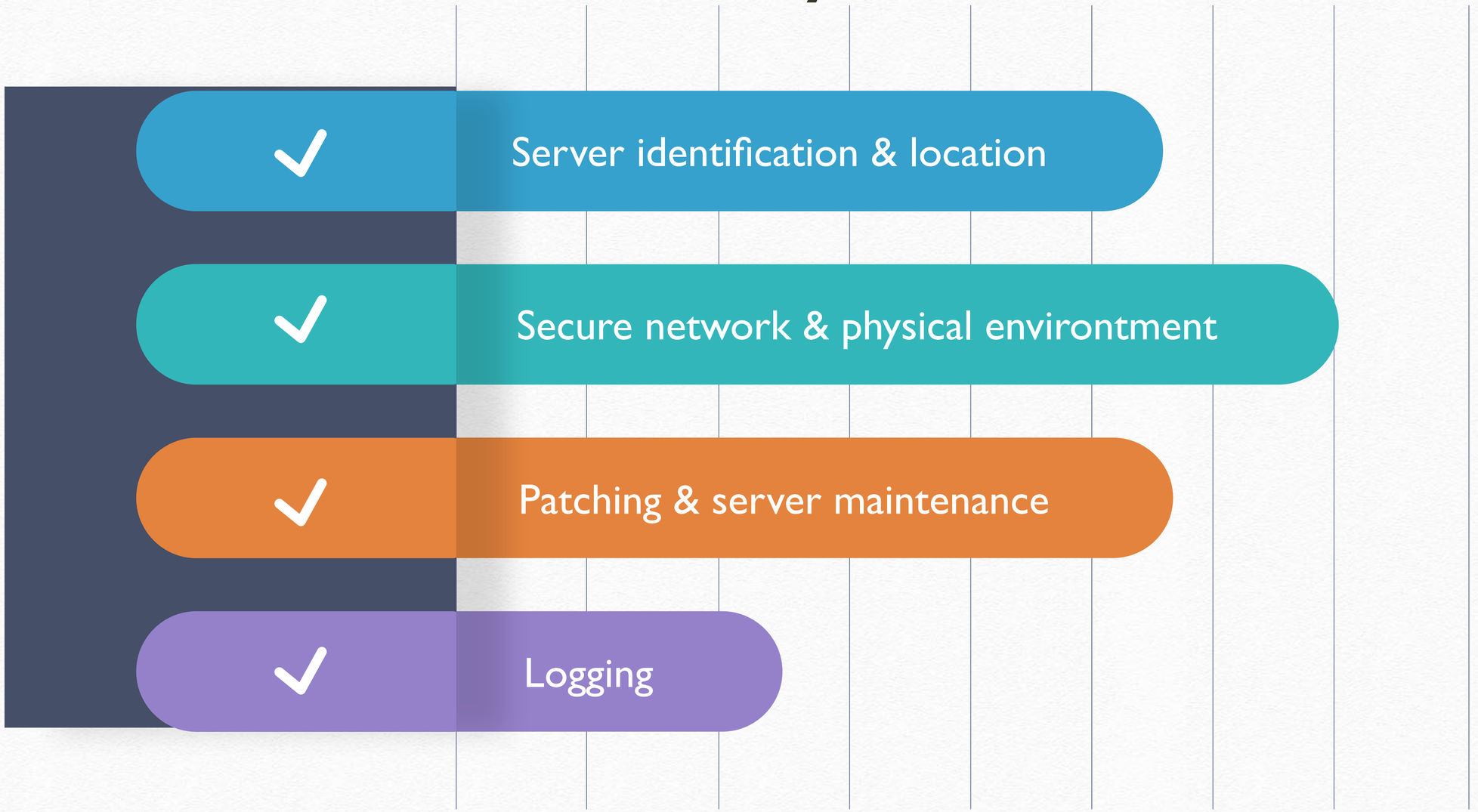
Risk Assessment

- Fisik
- Aplikasi
- Sistem operasi
- Jaringan



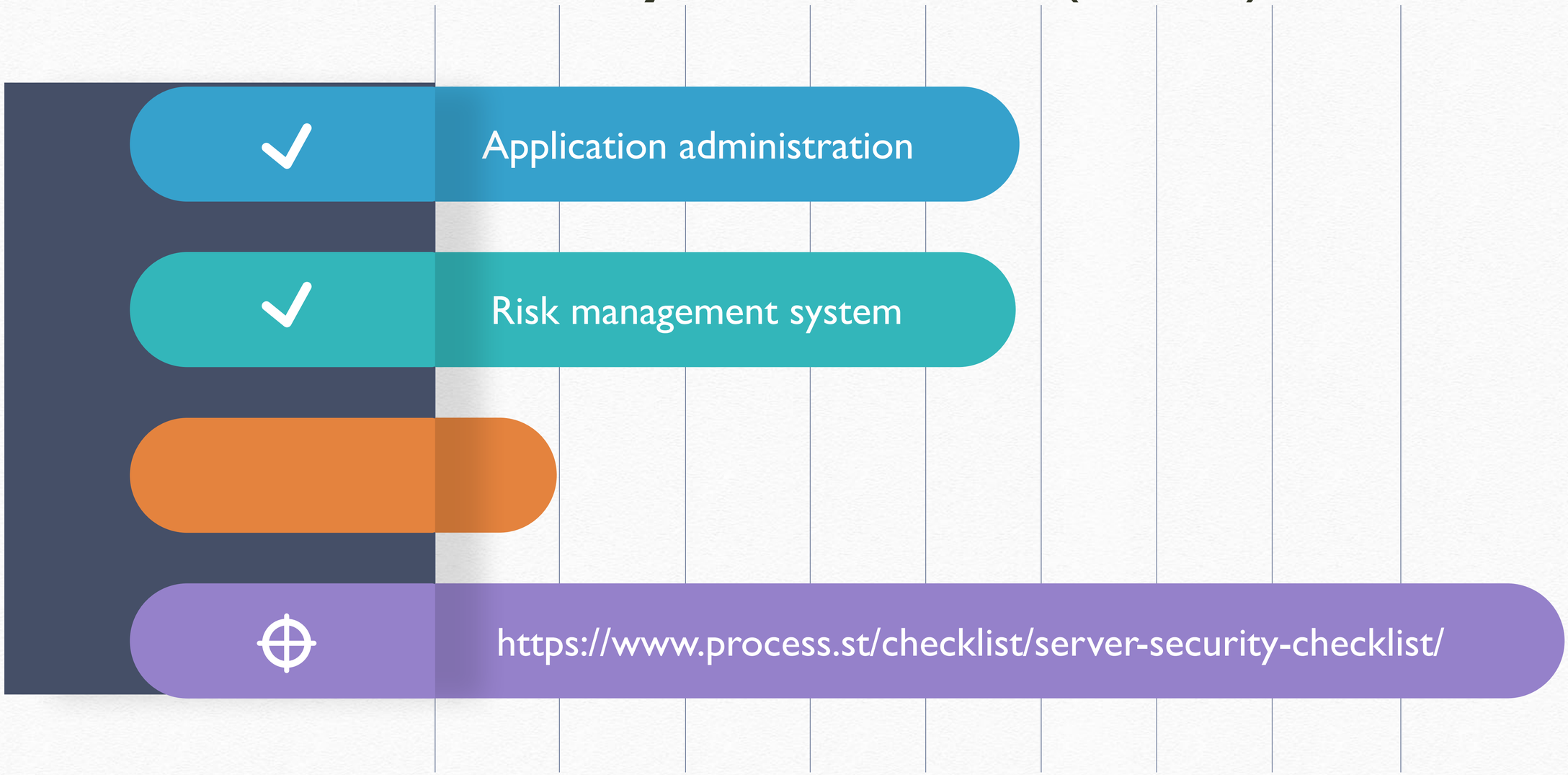
http://www.exinfm.com/excel%20files/IT%20RISK%20ASSESMENT%20TEMPLATE.xls

Server security checklist



Server security checklist (cont)

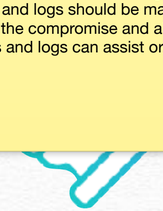
Server security checklist (cont)



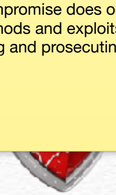
Simplicity—Security mechanisms (and information systems in general) should be as simple as possible. Complexity is at the root of many security issues.
Fail-Safe—If a failure occurs, the system should fail in a secure manner, i.e., security controls and settings remain in effect and are enforced. It is usually better to lose functionality rather than security.
Complete Mediation—Rather than providing direct access to information, mediators that enforce access policy should be employed. Common examples of mediators include file system permissions, proxies, firewalls, and mail gateways.
Open Design—System security should not depend on the secrecy of the implementation or its components.
Separation of Privilege—Functions, to the degree possible, should be separate and provide as much granularity as possible. The concept can apply to both systems and operators and users. In the case of systems, functions such as read, edit, write, and execute should be separate. In the case of system operators and users, roles should be as separate as possible. For example, if resources allow, the role of system administrator should be separate from that of the database administrator.
Least Privilege—This principle dictates that each task, process, or user is granted the minimum rights required to perform its job. By applying this principle consistently, if a task, process, or user is compromised, the scope of damage is constrained to the limited resources available to the compromised entity.
Psychological Acceptability—Users should understand the necessity of security. This can be provided through training and education. In addition, the security mechanisms in place should present users with sensible options that give them the usability they require on a daily basis. If users find the security mechanisms too cumbersome, they may devise ways to work around or compromise them. The objective is not to weaken security so it is understandable and acceptable, but to train and educate users and to design security mechanisms and policies that are usable and effective.
Least Common Mechanism—When providing a feature for the system, it is best to have a single process or service gain some function without granting that same function to other parts of the system. The ability for the Web server process to access a back-end database, for instance, should not also enable other applications on the system to access the back-end database.
Defense-in-Depth—Organizations should understand that a single security mechanism is generally insufficient. Security mechanisms (defenses) need to be layered so that compromise of a single security mechanism is insufficient to compromise a host or network. No “silver bullet” exists for information system security.
Work Factor—Organizations should understand what it would take to break the system or network’s security features. The amount of work necessary for an attacker to break the system or network should exceed the value that the attacker would gain from a successful compromise.
Compromise Recording—Records and logs should be maintained so that if a compromise does occur, evidence of the attack is available to the organization. This information can assist in securing the network and host after the compromise and aid in identifying the methods and exploits used by the attacker. This information can be used to better secure the host or network in the future. In addition, these records and logs can assist organizations in identifying and prosecuting attackers.

ion

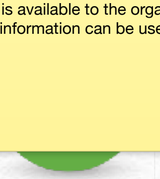
IST 800-123)



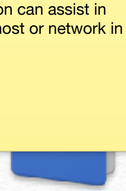
Simplicity



Fail-safe



Complete mediation



Open design

Separation of privilege

Least privilege

Psychological acceptability

Least common mechanism

Defense-in-depth

Work factor

Compromise recording

Testing

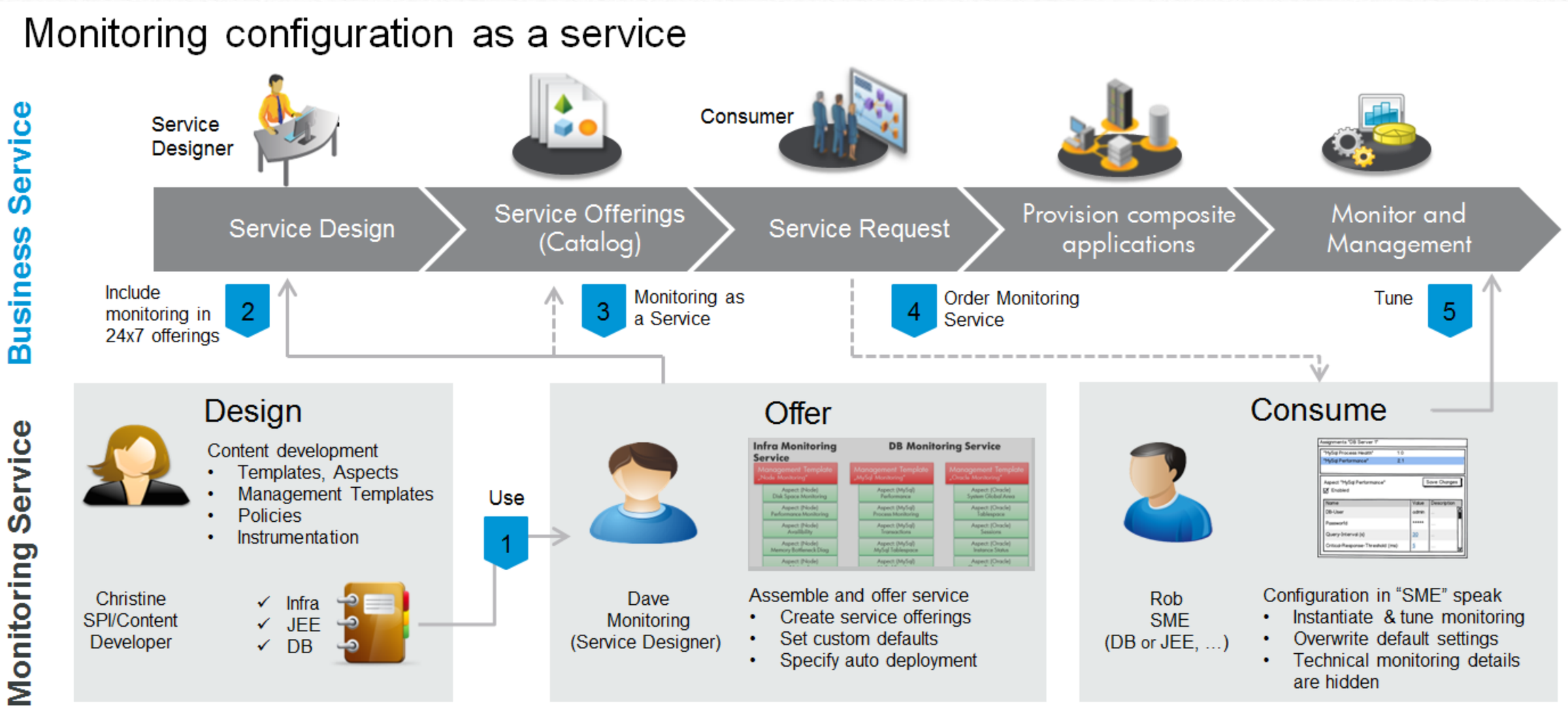
Buat daftar yang akan diuji

Tentukan metode pengujian yang tepat

Gunakan alat bantu yang tepat

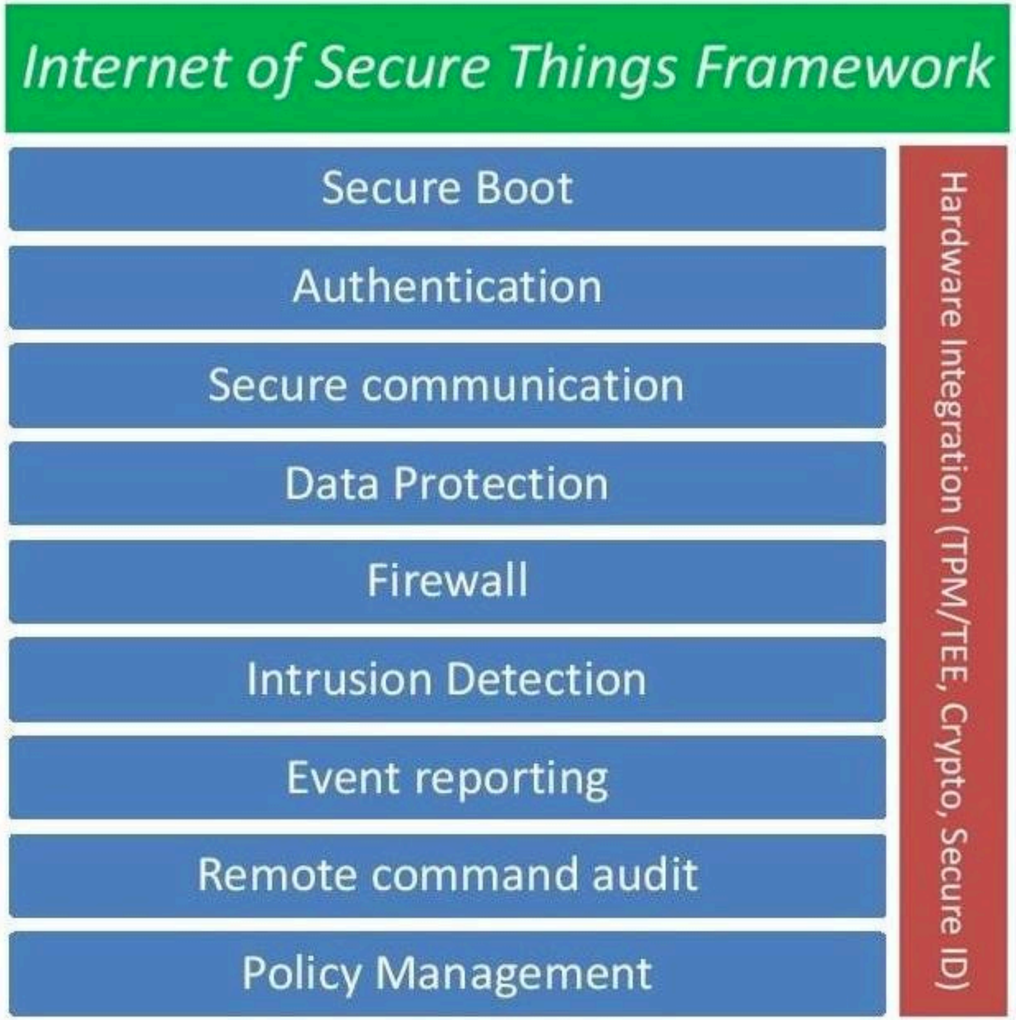
Perbaiki !

Monitoring



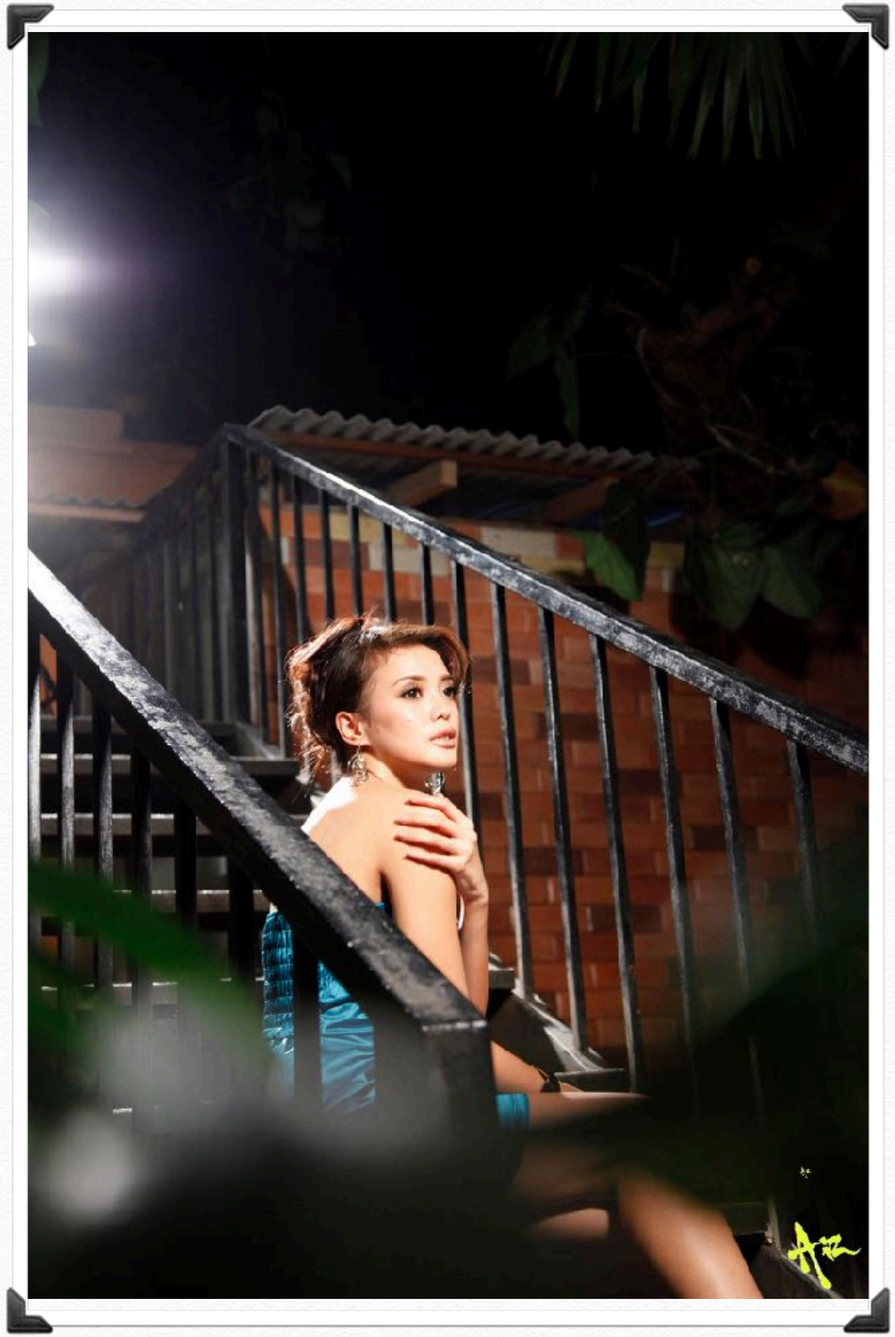
Security Monitoring

Evaluate


Internet of Secure Things Framework
Secure Boot
Authentication
Secure communication
Data Protection
Firewall
Intrusion Detection
Event reporting
Remote command audit
Policy Management
Hardware Integration (TPM/TEE, Crypto, Secure ID)


1
Availability
2
Integrity
3
Confidentiality

Question?



"Aku hanyalah orang biasa, tapi aku ingin membuat seseorang menjadi luar biasa dan istimewa"

Azis Kurniawan

Thank you

CISTECH 2017 - LEMSANEG
azis.kurniawan@lemsaneg.go.id


azis.kurniawan@lemsaneg.go.id

azis.kurniawan@gmail.com


+62 0812-199 00 723


https://www.facebook.com/azispage


aziyzk


@citycrypt

https://www.youtube.com/channel/UCsfuWs2-0Aq8lL1u1fW5g3A


https://github.com/citycrypt

Visit it

- https://www.process.st/checklist/server-security-checklist/#relevant-checklists
- https://security.berkeley.edu/resources/best-practices-how-to-articles
- https://www.htbridge.com/websec/
- https://community.saas.hpe.com/t5/IT-Operations-Management-ITOM/HP-OMi-now-includes-Automation-to-simplify-IT-Monitoring/ba-p/218677?nm#.WSMpq8aB2Ho
- https://www.nap.edu/read/1581/chapter/7#136