Security

解構SRAA安全風險評估及審核服務

KRECENDO HUI

CYBER SECURITY ENGINEER

PROFILE

- Offensive Security Certified Professional (OSCP)
- eLearnSecurity Junior Penetration Tester (eJPT)
- Multiple years working in InfoSec and Cyber Security
- Former security responsible in HKFWS, Langham and Blue cross Insurance
- Experienced in SRAA operation

Security

WHAT IS SRAA?

Consist of 2 parts:

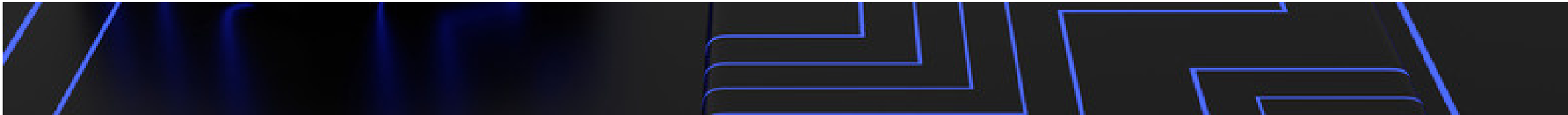
- Security Risk Assessment
- Security Audit

What is Security Risk Assessment?

A Security Risk Assessment (SRA) is the process of identifying and evaluating potential security risks to an organization.

Including:

- **Asset identification** - Identifying critical assets to protect
- **Threat modeling** - Evaluating potential threats to those assets
- **Vulnerability assessment** - Evaluating vulnerabilities that could be exploited
- **Risk analysis** - Estimating risk levels based on threats, vulnerabilities, and impact
- **Recommendations** - Providing recommendations to mitigate high risk issues



Types of Security Risk Assessment

1) Vulnerabilities Scanning

2) Penetration testing

- Black box, grey box, white box

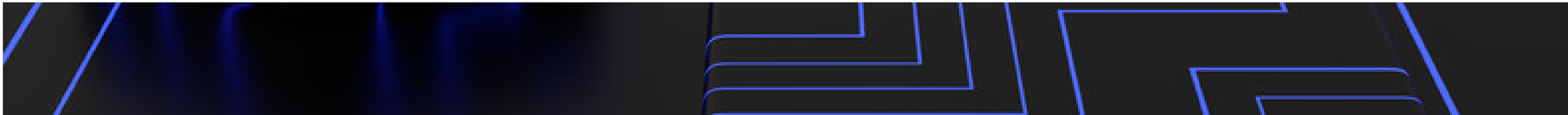
3) Cloud Security Risk Assessment

4) Network Security Risk Assessment

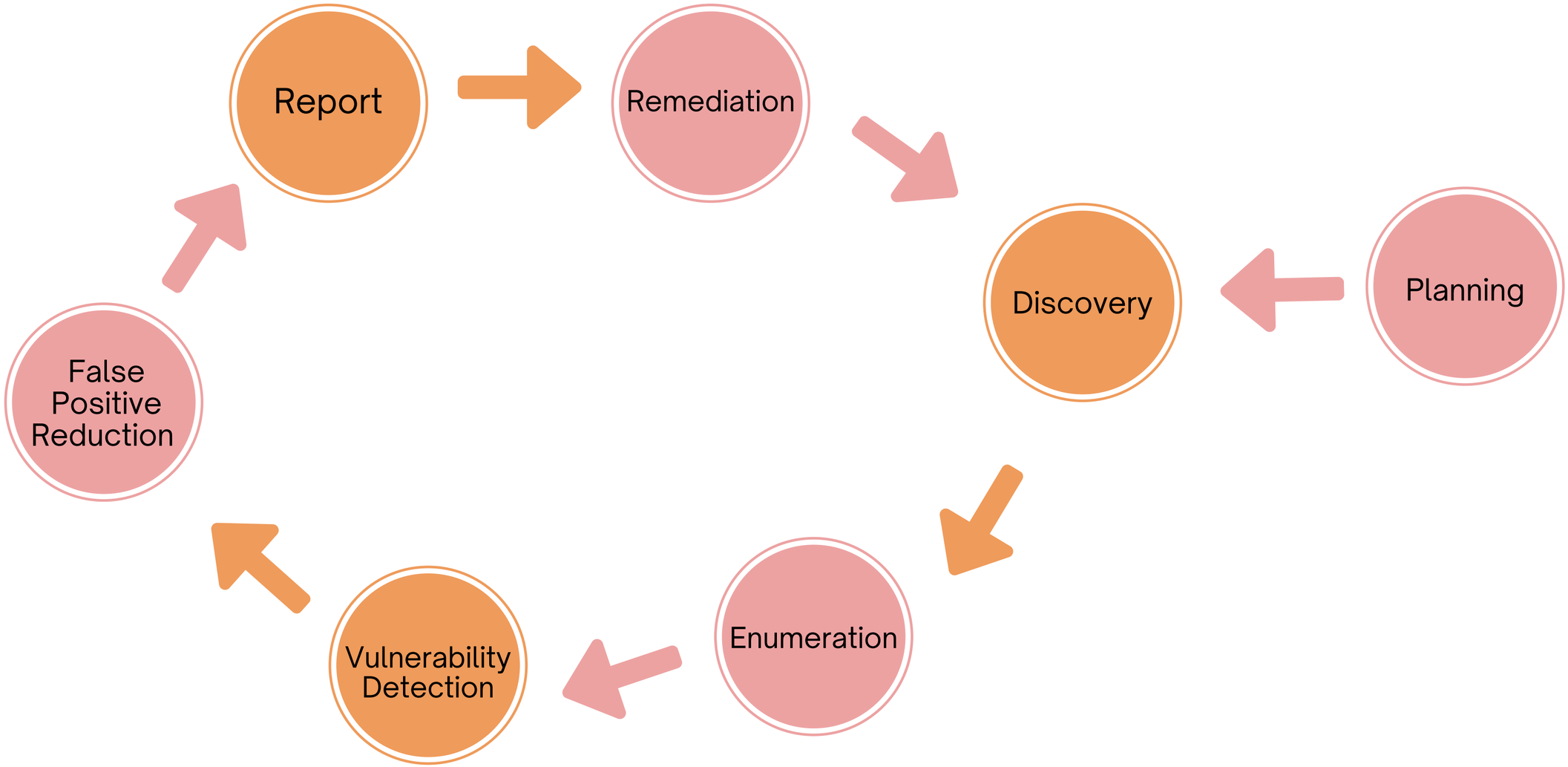
5) Mobile Application Risk Assessment

6) Code Review

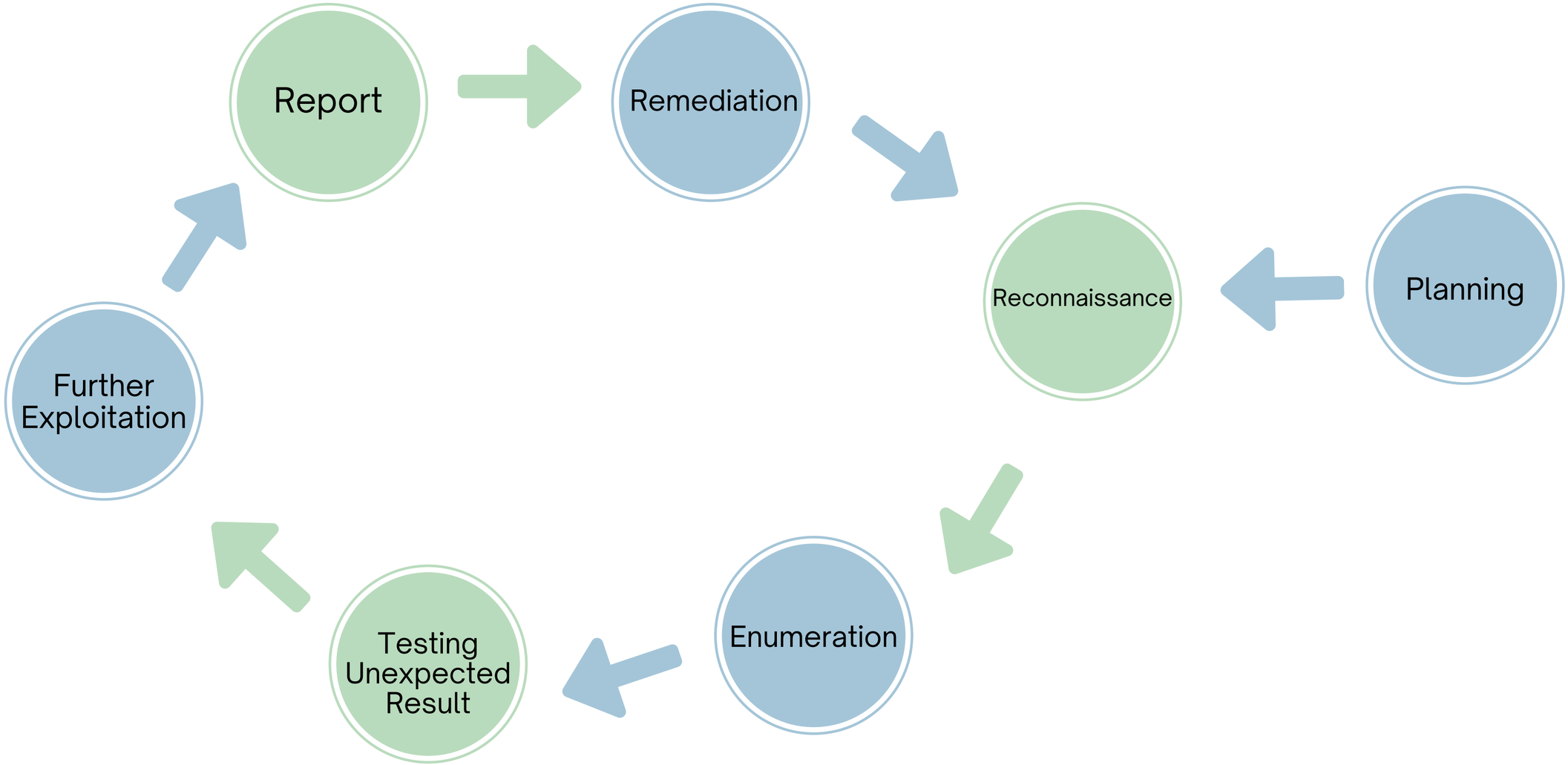
7) Application Programming Interface (API) Risk Assessment



Flow of Vulnerability Scanning

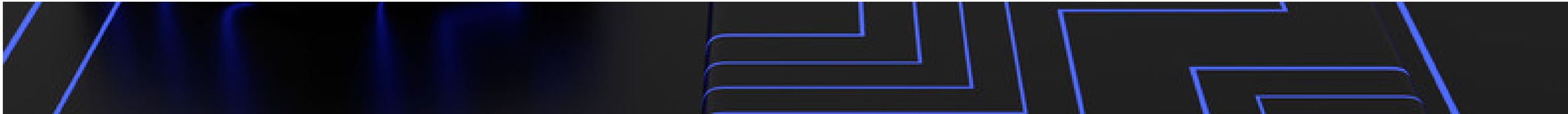


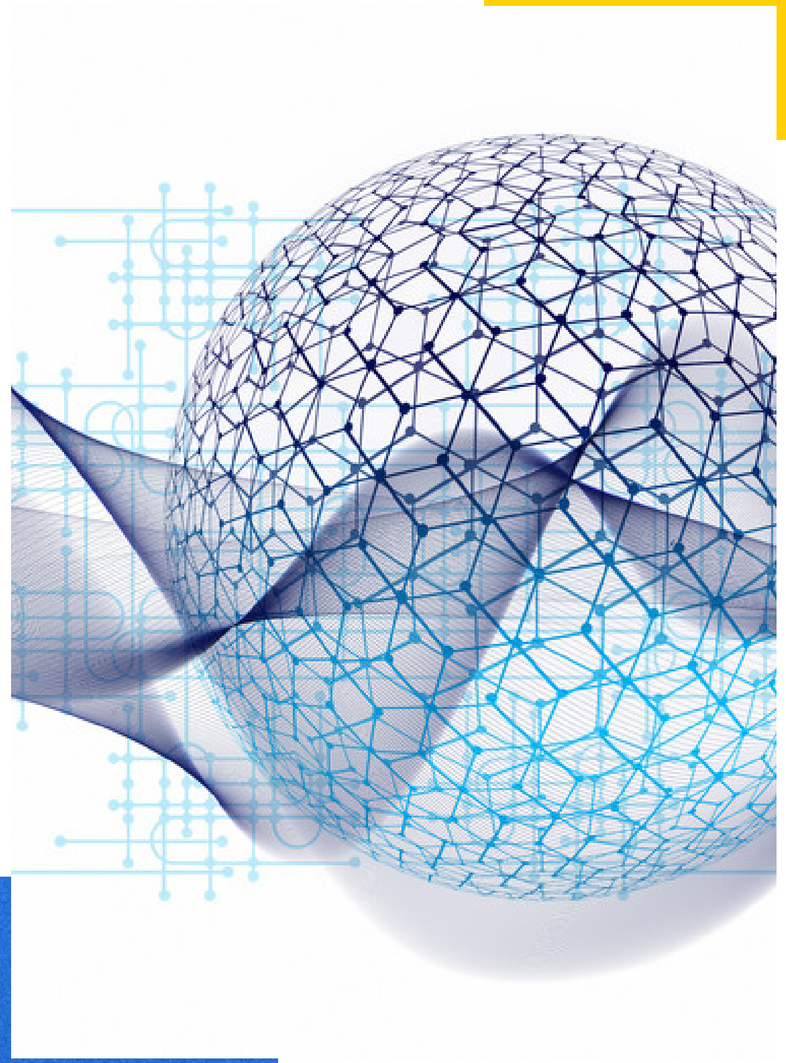
Flow of Penetration Testing



Security Risk Assessment Standard

- OWASP Web Testing Guideline
- OWASP Mobile Testing Guideline
- The Common Vulnerability Scoring System (CVSS)
- The Penetration Testing Execution Standard(PTES)





WHAT IS SECURITY AUDIT?

A Security Audit (SA) is a more in-depth evaluation of the security of a system or organization.

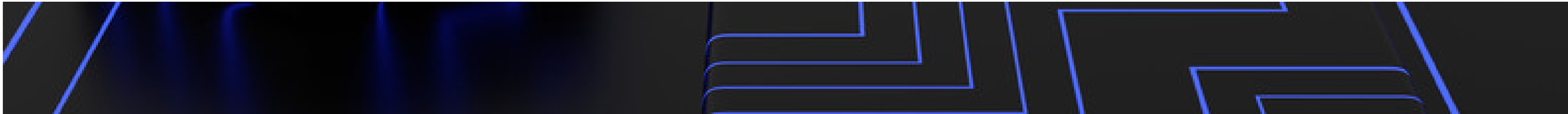
Including:

- Examining security controls
- Assessing system configurations and patching
- Reviewing access controls
- Testing for vulnerabilities
- Evaluating compliance with security policies and standards
- Interviewing employees (i.e. project owner, it staff)
- Providing recommendations for improvement

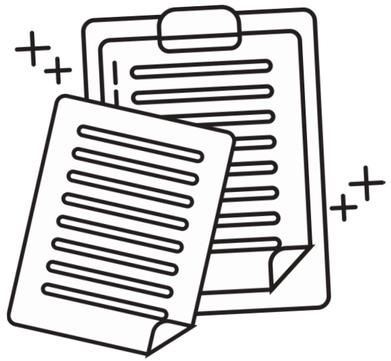
Security

Security Audit Standard

- COBIT - Control Objectives for Information and Related Technology
- NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems
- SOC 2 - Service Organization Control 2 (for service organizations)



Security Risk Audit Questionnaire



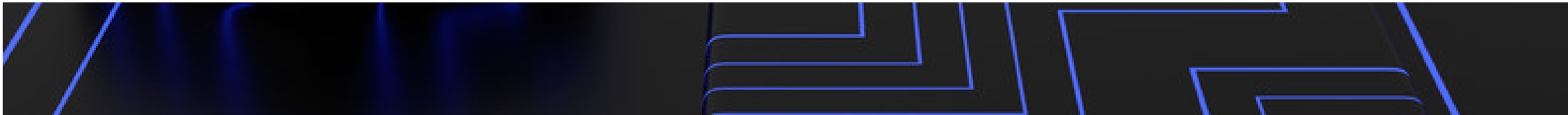
Ref	Auditable Unit	Inherent Risk Rating	Control Environment Indicator	Audit Requirement Rating	Rating*	Frequency
A	**Corporate Governance**					
A.1	Finance	5	3	4	C	Annual
A.2	Legal and Democratic Services	4	4	2	M	Every 3 years
A.3	Human Resources and Organisational Development	5	2	4	C	Annual
A4	Customer Services and Performance	6	3	5	C	Annual
A5	Procurement	5	3	4	C	Annual
B	**Enterprise Planning and Infrastructure**					
B.1.	Asset Management and Operations	4	4	2	M	Every 3 years
B.2	Planning and Sustainable Development	4	2	3	H	Every 2 years
B.3	Economic and Business Development	5	3	4	C	Annual
C	**Education, Culture and Sport**					
C.1	Communities, Culture and Sport	4	4	2	M	Every 3 years
C.2	Schools and Education Establishments	5	2	4	C	Annual
C.3	Educational Development, Policy and Performance	4	4	2	M	Every 3 years
D	**Housing and Environment**					
D.1	Regeneration and Housing Investment	5	5	3	H	Every 2 years
D.2	Housing and community safety	3	3	2	M	Every 3 years
D.3	Environmental Services	3	2	2	M	Every 3 years
E	**Social Care and Wellbeing**					
E.1.	Adult Services	6	4	4	C	Annual
E.2	Children Services	6	4	4	C	Annual
E.3	Older people and rehabilitation	5	5	3	H	Every 2 years

The different between Security Risk Assessment and Audit

Security Risk Assessment	Security Audit
The identification threats and vulnerabilities, evaluation of levels of risk involved, and determination of an acceptable level of risk and risk mitigation strategies	The processes to ascertain the effective implementation of security measures against the departmental IT security policies, standards, and other contractual or legal requirements
Focus on the **risk perspective**	Focus on **compliance perspective**
Key Deliverables: **risk register and risk mitigation measures**	Key Deliverables: **compliance checklist**

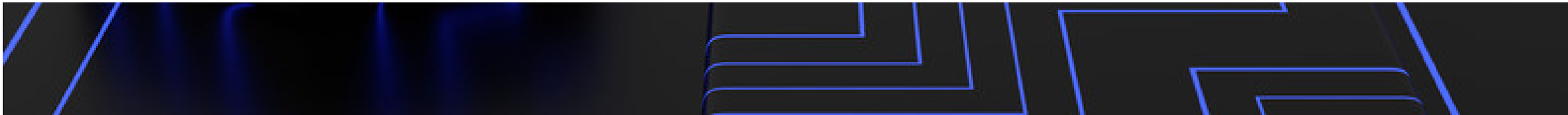
Other Requirement by OGCIO

- Baseline IT Security Policy (S17)
- IT Security Guidelines (G3)
- Practice Guide for Security Risk Assessment & Audit
- Practice Guide for Penetration Testing
- Practice Guide for Information Security Incident Handling



The importance of Security Risk Assessment and Audit

- Requirement from government/funder
- NGOs are high-risk targets
- Security risks are not a concern during the software development cycle
  - Identify and understand the existing vulnerabilities.
- Improve the effectiveness of the existing policy, standards, guidelines and procedures by identifying the inadequacies and examine
- Enhance funder confidence and future cooperate opportunities



Q&A

Security

UD Security

THANK YOU!!

YOUR MOST RELIABLE CYBER SECURITY PARTNER

(852) 2554 7545 (852) 9696 7545 service@ud.hk www.ud.hk