Security Risk Assessment and Audit

(SRAA)

Service White Paper

SCS | 开源服务

数据无价 安全有价

What is SRAA?

SRAA (Security Risk Assessment and Audit) is an ongoing information security practice process to identify and resolve security issues. Aims to systematically identify, analyze and assess potential cybersecurity risks in an organization's information infrastructure, prioritize risks and make recommendations for mitigation or remediation. The core goal is to enhance the organization’s cybersecurity protection capabilities and prevent cyber threats through continuous risk management and compliance audits.

SRAA = SRA (Security Risk Assessment) + SA (Security Audit). The two practices can be performed separately, but the security audit must be performed after the security risk assessment is implemented.

Who need SRAA?

Government departments and critical infrastructure

Key industries such as finance, medical care, energy, education and government departments.

Government-funded organizations (NGOs/NPOs)

Involving scenarios such as new system launch or major upgrades.

Any organization concerned with information security

Private institutions,catering companies,technology companies,etc.

Differences between SRA and SA

Security Risk Assessment	Security Audit
The identification of threat and vulnerabilities, evaluation of the levels of risk involved, and determination of an acceptable level of risk and corresponding risk mitigation strategies.	The process ascertains the effective implementation of security measures against the departmental IT security policies, standards, and other contractual or legal requirements.
Focus on the risk perspective, assessment areas not necessarily related to security policies and standards.	Focus on the compliance perspective, assess against security policies, standards or other pre-defined criteria.
It can be a self-assessment by B/D or completed by an independent third party.	Must be completed by an independent third party.

Why need SRAA?

1.Compliance requirements

Verify that the current departmental or system's information security measures comply with the Hong Kong Digital Policy Office (DPO) policies and specific standards to reduce the risk of legal penalties or reputational damage.

2. Risk identification and control

Comprehensively identify potential information security risks and weak links at the department or system level, and strengthen the security of the department's internal information system based on professional rectification suggestions and measures to ensure smooth business operations.

3. Continuous improvement

By conducting SRAA on a regular basis, we continuously identify new risks and take timely measures to improve the security status. This mechanism of continuous improvement helps to maintain and improve the level of information security. of the organization.

How you support us in SRAA?

Sign the project authorization agreement

Fill out the SRAA Questionnaire

Assign a dedicated staff for contact

Provide necessary access to systems or equipment and ensure that recovery plans and incident handling procedures are prepared before testing

Our advantages

As a professional team deeply engaged in the field of data compliance and cybersecurity in Hong Kong, as well as an independent third-party auditor, we strictly follow the DPO's specifications and guidelines to provide services.

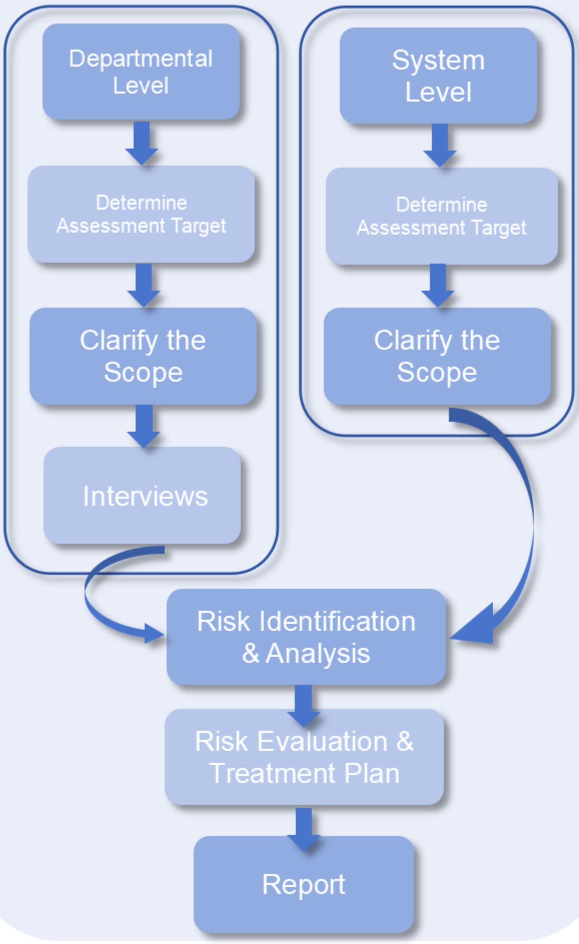
For organizations that require the timeliness of assessment, we rely on efficient and strict implementation capabilities, combined with technical testing and regulatory analysis, to provide the dual guarantee of "technical specifications" to ensure comprehensive information security risk management and control and help customers meet compliance requirements.

About SRA

SRA is a systematic process that aims to identify, analyze and evaluate the customer's existing security risks and then develop appropriate mitigation measures to reduce the risks to an acceptable level. SRA has two separate levels, namely Departmental Level and System Level.

The assessment can be carried out at two levels depending on the situation.

How SRA works?


Departmental Level
Determine Assessment Target
Clarify the Scope
Interviews
System Level
Determine Assessment Target
Clarify the Scope
Risk Identification & Analysis
Risk Evaluation & Treatment Plan
Report

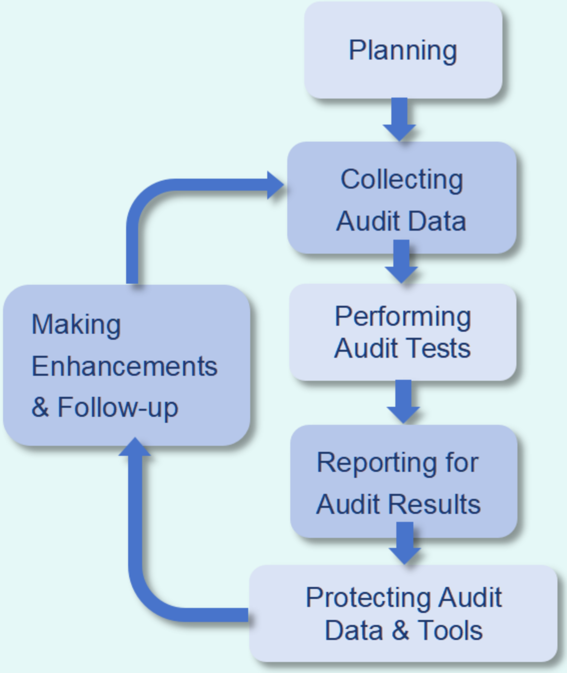
About SA

SA verifies the compliance and effectiveness of customers' existing security controls, policies and technical configurations and identifies potential deficiencies or areas for improvement.

SA verifies that security measures comply with policies and standards through continuous inspections.

Evaluate the effectiveness of safeguards to ensure they are implemented and meet legal and compliance requirements.

How SA works?


Planning
Collecting Audit Data
Performing Audit Tests
Reporting for Audit Results
Protecting Audit Data & Tools
Making Enhancements & Follow-up

SRA output

- Security Risk Assessment Report
- Risk Treatment Plan
- System Risk Register

SA output

- Security Audit Report

Shenzhen Open Source Cybersecurity Services Company Limited.

Email: mareketing@scssec.com

Website: www.scssec-hk.com

Address: Room 2901, Huafeng Building, No.6006 Shennan Road,
Futian District, Shenzhen

Copyright Statement and Confidentiality Agreement