CISSP Domain 6 — Security Assessment and Testing

Domain 6 — Security Assessment and Testing

Real User Monitoring or RUM captures all transactions of all users of a website or application. Also called **End-User Experience Monitoring.**

Synthetic Performance Monitoring or **Proactive Monitoring** uses external agents running scripted transactions. It's meant to simulate typical uesrs.

Website Monitoring uses simulated transactions to perform HTTP requests to test availability and performance. These can specialize in database transactions or TCP port availability.

Dynamic versus Static Testing

Dynamic testing runs the system under test.

Static testing analyzes the system without running it.

KPI vs KRI

Key Performance Indicators or KPI are about past events.

Key Risk Indicators or KRI are about the possibility or probability of risk in the future.

DR vs BC

Business Continuity tries to prevent the outage, or mitigate impact.

Disaster Recovert tries to rapidly return to a pre-disaster state.

SOC (formerly SAS 70, now SSAE) = auditing reports

Type 1 evaluates the **design.**

Type 2 evaluates the design *and* **effectiveness.**

- **SOC 1** = mainly for financial auditors and investors
  - SOC 1 **Type 1** report = auditor's opinion on accuracy and completeness of management's description of the system or service, as well as suitability of the **design** of controls.
  - SOC 1 **Type 2** report = Type 1 **plus** audit of **effectiveness** of those controls **over a declared period**(typically 6 or 12 months)
- **SOC 2** = report for IT staff, regulators, and business partners, all of whom should have sufficient knowledge to use the details, addressing any of the five Trust Services:
  - Security (mostly access control)
  - Availability
  - Processing Integrity (complete, accurate, timely, authorized)
  - Confidentiality
  - Privacy

  Same **Type 1 / Type 2** distinction.
- **SOC 3** = just a summary report of SOC 2, pass or fail, for current or potential customers

	Type 1 Auditor's opinion on accuracy and completeness of management's description of the system, plus suitability of the system's **design.**	**Type 2** Type 1 *plus* an audit of the**effectiveness** of those controls over a declared period, usually 6 or 12 months.
SOC 1 Report for financial auditors and investors.		
SOC 2 Report for IT staff, regulators, and business partners. investors.		

SOC 3 A pass/fail summary of SOC 2, brochure-type content for current or potential customers.		

Intended recipients of SOC 2 should have sufficient knowledge to use the details, address any of the five Trust Services:

- Security (mostly access control)
- Availability
- Processing Integrity (is it complete, accurate, timely, authorized)
- Confidentiality
- Privacy