

ISMS KPI Workshop

정보보호경영시스템 성과지표 도출 및 성과측정 워크숍



By BSI Korea

shape the future



1. Measurement의 이해

What is a measurement or metric?

- ❑ The term metric is used for an individual measurement, which may be represented by a single number, a list, table or chart.
- ❑ A group of metrics is used to build a report, usually with supporting text.

Why needed?

Famous saying and truths about measurement

- ✓ If you don't measure it, you can't manage it
- ✓ If you don't measure it, you can't improve it
- ✓ If you don't measure it, you probably don't care
- ✓ If you can't influence it, then don't measure it

ISO 27001 requirements

4.2.2 Implement and operate the ISMS

C) **Define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results (see 4.2.3 C)**

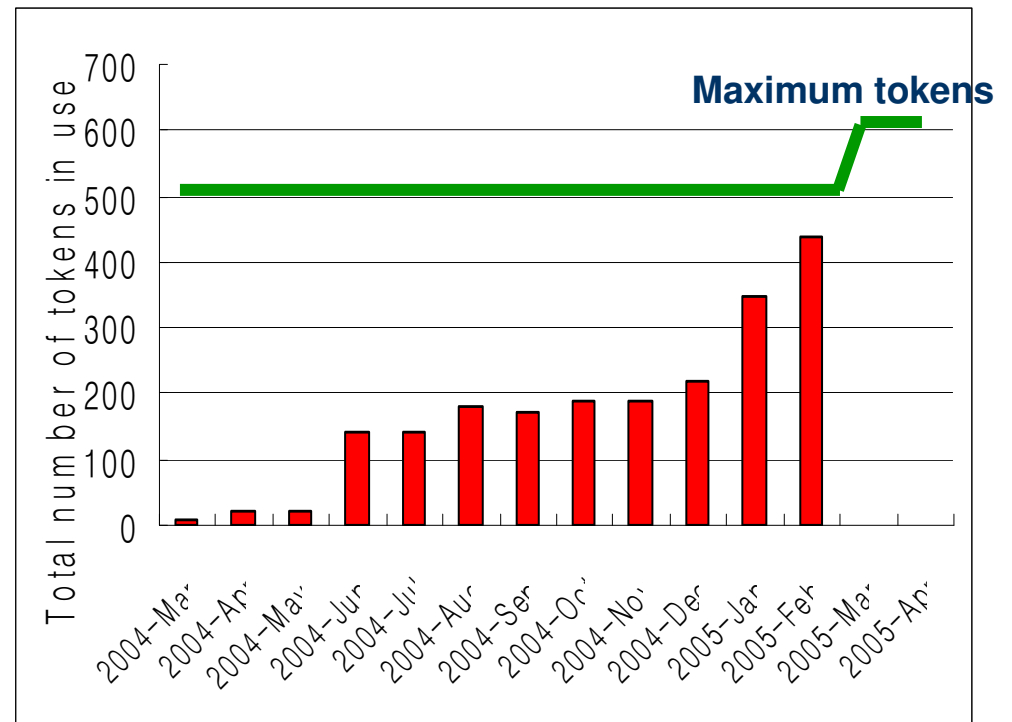
4.2.3 Monitor and review the ISMS

b) Undertake **regular reviews** of the effectiveness of the ISMS (including meeting ISMS policy and objectives, and review of security controls) taking into account results of security audits, incidents, **results from effectiveness measurements** suggestions and feedback from all interested parties.

C) **Measure the effectiveness of controls to verify that security requirements have been met**

Types of metrics

- ❑ **Reactive metrics** show what has happened, particularly from the predominantly reactive processes or controls, such as incident management.
- ❑ **Proactive metrics** give advance warning of events that if left unmanaged could impact the service
- ❑ **Forward schedule metrics** show planned activities, i.e. those activities that are not just predictable but which are intentional.



- Security token usage and planned increases

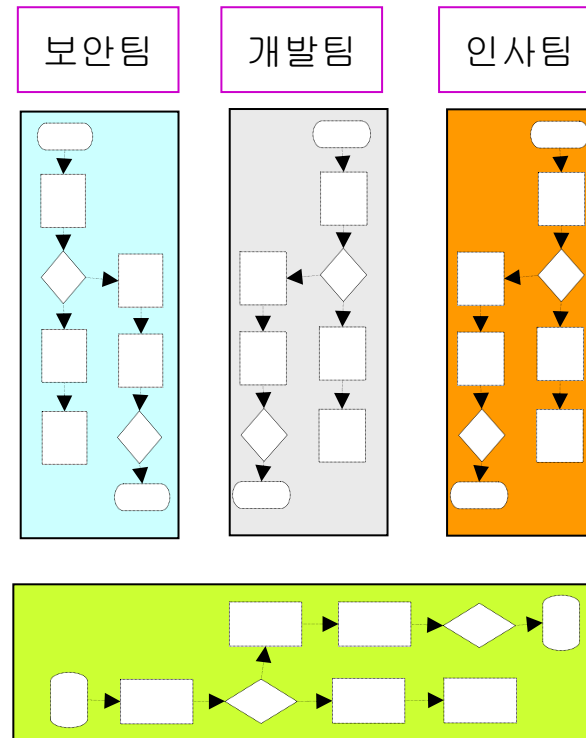
Types of metrics

❑ Metrics independent on other processes

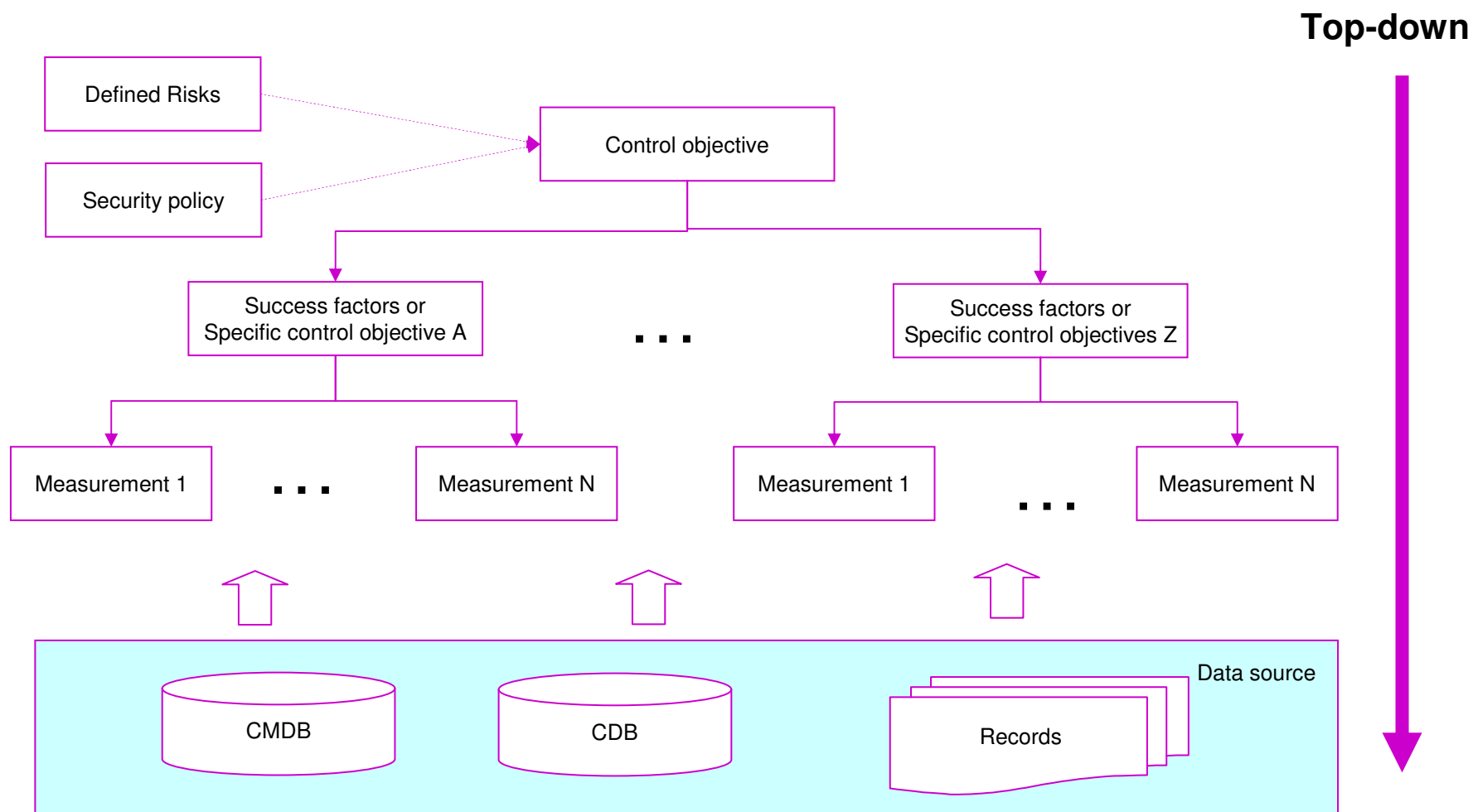
보안 조직에 의해 전적으로 운영되는 security controls의 measurement. 구현이 상대적으로 쉽다.

❑ Metrics dependent on other processes

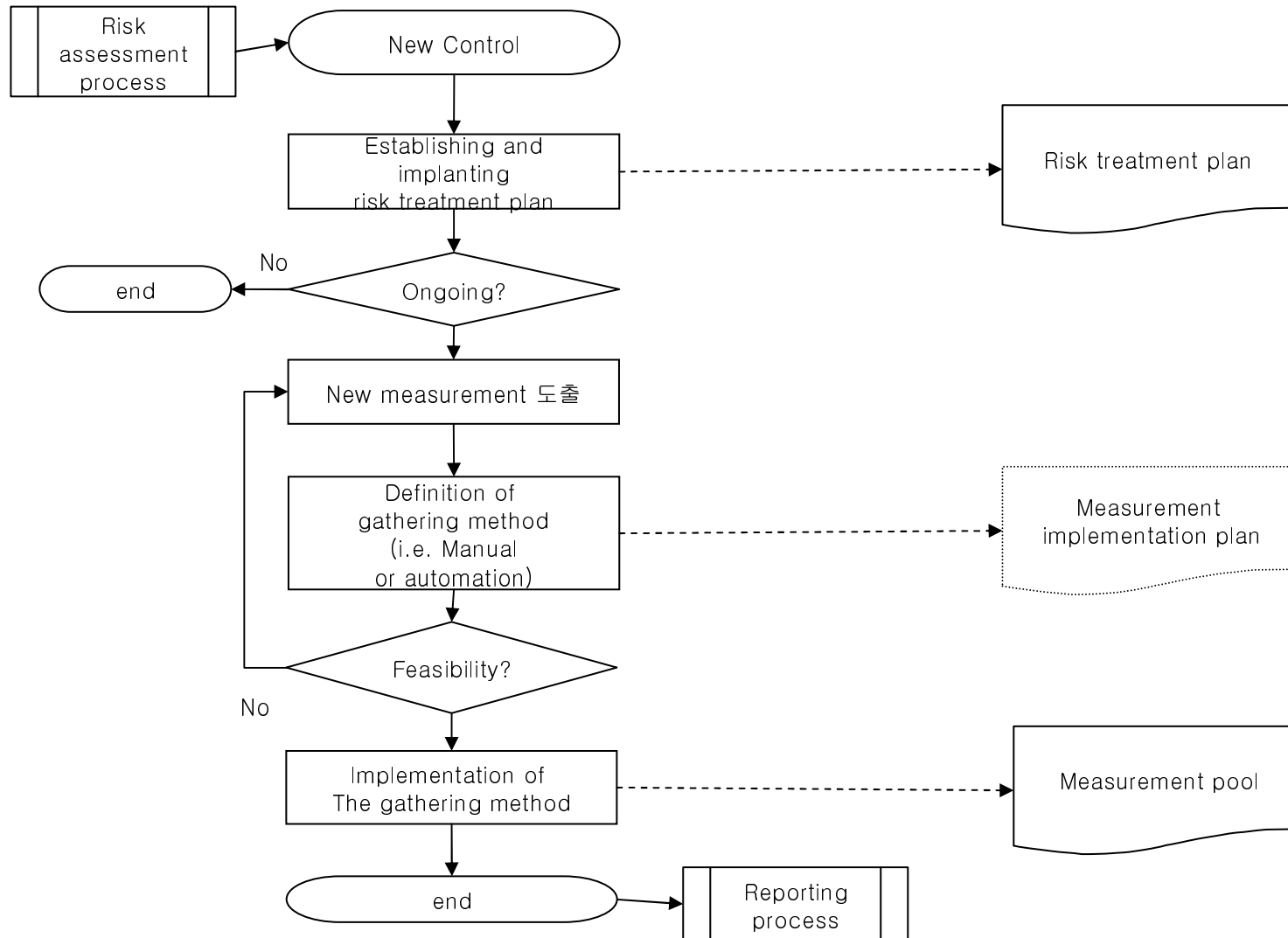
다른 조직이 소유권을 가지고 있는 프로세스와 관련된 measurements. 보안 조직은 타 프로세스에 필요한 보안 통제와 measurement의 요구를 반영해야 함. 타 조직의 프로세스 목표와 특성을 충분히 이해하고 해당 프로세스의 목적을 보장하면서 원하는 Measurement를 구현할 수 있는 방안을 마련해야 함. 해당 프로세스 Owner의 sponsorship이 없으면 실패할 가능성이 큼.



Design guidelines



Implementation procedure



Reporting process

- measurement를 정기적으로 취합, 분석, 리포팅하는 프로세스
- 리포팅의 정기적인 주기 및 비정기적인 주기 결정
- measurement의 timeliness 고려
- audience에 따른 활동
- 다른 프로세스와의 관계(e.g. 특정 measure의 경우 내부 감사의 결과를 input으로 받는 경우가 있음)

Sample measurement

Risk	Risk ID: R20060316-0001, Very High(9) “SQL injection을 통한 고객 개인 정보 유출의 위험”
Selected controls	A.12.2.1 Input data validation A.12.5.1 Change control procedures
Control objectives	Data input to applications shall be validated to ensure that this data is correct and appropriate The implementation of changes shall be controlled by the use of formal change control procedure
Success factors	“개발 변경 프로세스의 테스트 과정에서 SQL injection 취약점이 반드시 제거 되도록 보장”
Measurement	SQL injection 검증이 실행된 개발 요청 건의 비율(%)
설명	어플리케이션 개발 건 중 SQL injection 검증이 실행되었는지를 확인하는 measurement.
측정방법	개발 테스트 결과에 SQL injection 검증 여부가 포함되어 있는지를 매월 보안 담당자가 확인함. 운영으로 이관된 모든 개발 요청 건에 대비해 비율을 환산, 모든 대내외 웹 어플리케이션에 대해 모두 적용. 어플리케이션 별로 분류하여 리포팅
측정주기	월 단위
Data source	변경 관리 시스템내의 테스트 기록

Sample measurement- cont'

Target value	>90
Danger value	<60
Possible value	0-100
제약사항	현재 개발 요청의 분류 항목에 '입력 필드 포함' 여부가 포함되어 있지 않아 객관적으로 입력 필드가 포함되어 있는 지를 확인하기가 어려움. 향후 변경관리 시스템을 개선할 예정임.

Sample measurement- cont'

