(ISC)² Italy Chapter

Effective Cloud Governance

Ruoli, Interfaccia, Indicatori

Paolo Ottolino CISSP-ISSAP CISM CISA ISO/IEC 27001 OPST PRINCE2 PMP ITIL

SECURITY 10 ANNI SUMMIT

(ISC)²
Italy Chapter

Agenda

1. Introduzione ed Obiettivi
2. IT Governance: Interfacce
3. Cloud IT: Governance Indicators
4. Cloud Governance: Indicators & Implementation

SECURITY 10 ANNI SUMMIT

(ISC)²
Italy Chapter

Introduzione ed Obiettivi 1/2

L'IT si sta evolvendo nel Cloud, sia privato sia pubblico, in forma di servizi IT. Allo scopo di poter continuare a gestire l'IT (e per non pagare eventuali suoi malfunzionamenti), c'e' bisogno di istruire un nuovo sistema di IT Governance, capace di indirizzare:
- ruoli differenti: Acquirer and Provider
- misurazioni accurate: Indicators
- chiare penalizzazioni/scontistiche: Contracts

La sessione presenta il modello "Effective Cloud Governance", costruito sui seguenti concetti:
1) "If You Can’t Measure It, You Can’t Manage It" [Peter Drucker]
2) L'Acquirer deve accrescere il commitment del Provider, attraverso la definizione di opportuni Service Level anche nel contratto di servizi
3) entrambi Acquirer and Provider devono condividere il modello di IT Governance model (cfr. NIST Cybersecurity framework 1.1, ID.SC-3)

SECURITY 10 ANNI SUMMIT

(ISC)² Italy Chapter

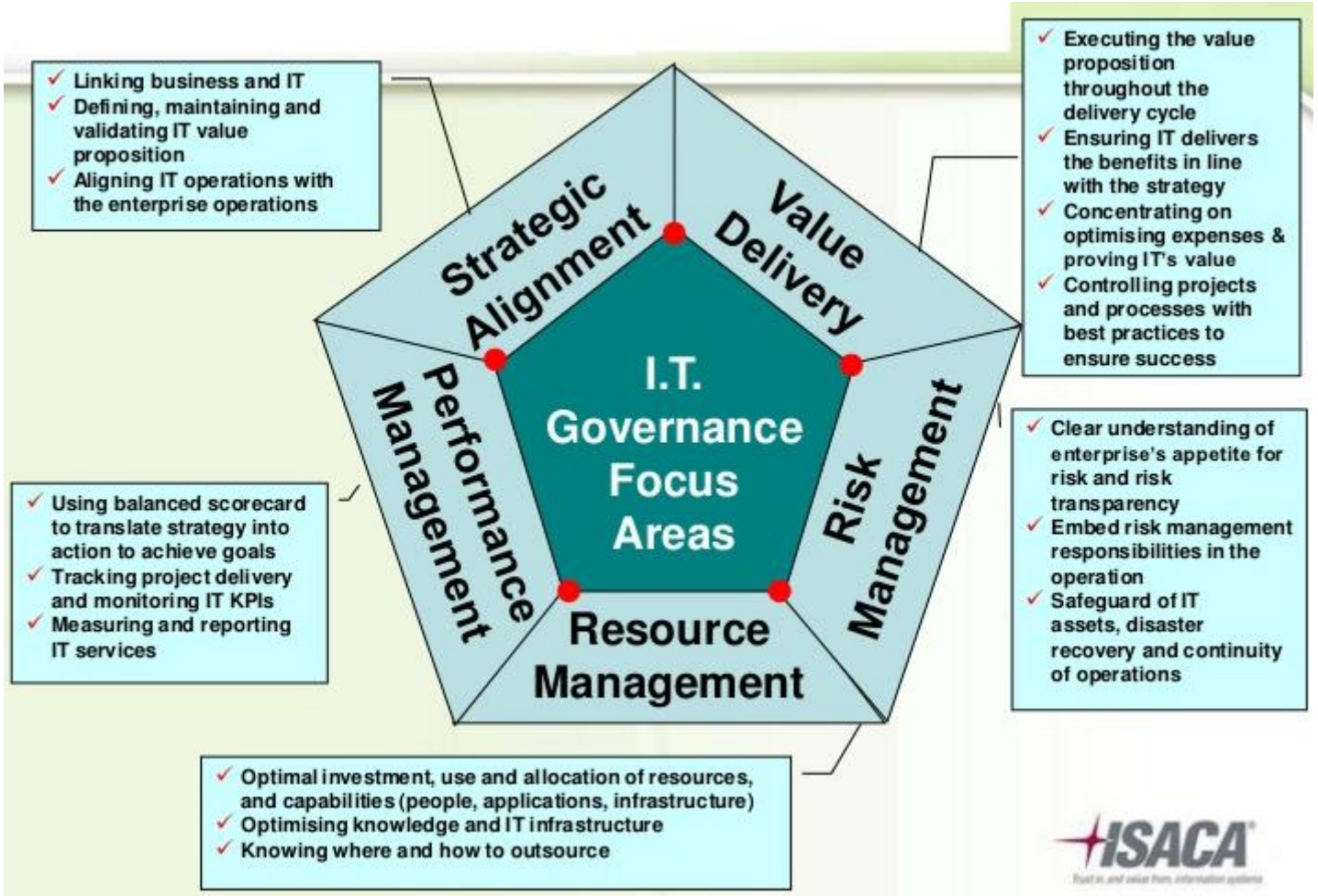
Introduzione ed Obiettivi 2/2

Un Effective Cloud Governance Model deve essere basato su indicatori, divisi per fasi (es. quelle del CobiT), ruoli ed indicatori:

Cycle	Customer	Provider	Indicators	Description
Direct	Appraise	Assess	KPI	Required Efficiency
Create	Validate	Design	KGI	Attended Goals
Protect	Manage	Implement	KRI	Risk Level
Execute	Control	Execute	SLA	Service Level
Monitor	Govern	Maintain	KMI	Service Direction

IT Governance: fast recap 1/2

IT Governance using ITGI Framework



(ISC)² Italy Chapter

IT Governance: fast recap 2/2

IT Governance Life Cycle

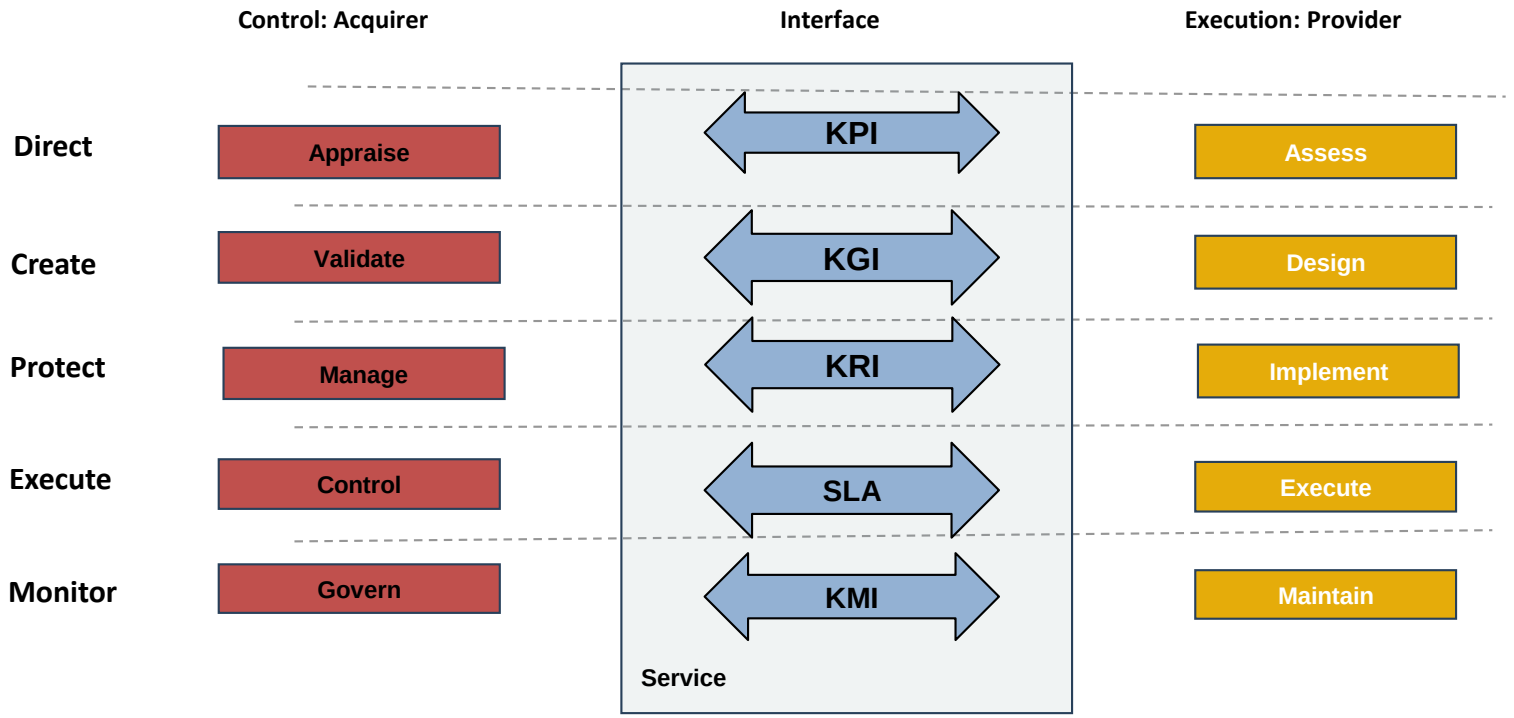
Governance Objective	Direct	Create	Protect	Execute	Monitor
IT Governance Focus Area	Strategic Alignment	Value Delivery	Risk Management	Resources Management	Performance Management
COBIT / VAL IT Contribution	• Business – IT Goals • Outcomes indicators	• Control Objectives • Process and Maturity Models • Management Practices and performance metrics			• ICT Balanced Scorecard • Assurance Guide

SECURITY 10 ANNI SUMMIT

(ISC)² Italy Chapter

IT Governance: Interfacce 1/2

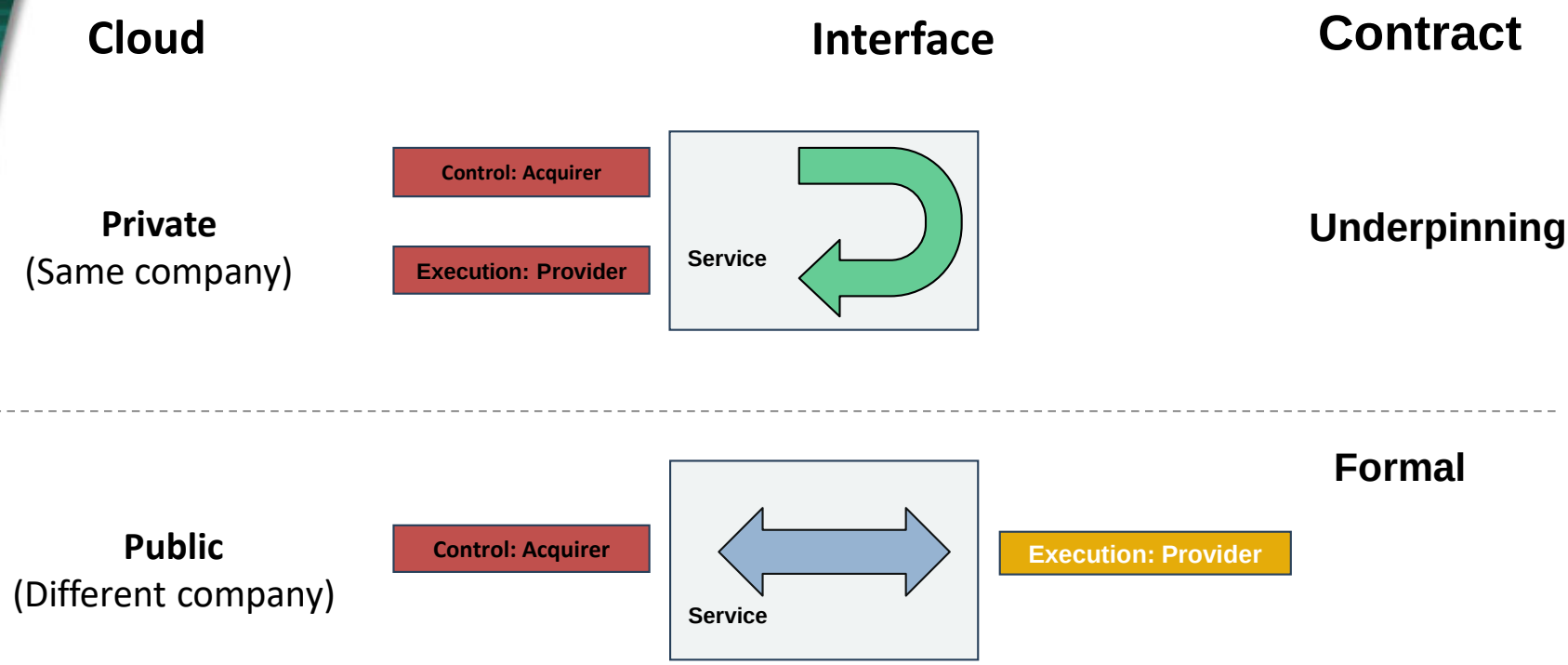
Governance Phases & Indicator Types



SECURITY 10 ANNI SUMMIT

IT Governance: Interfacce 2/2

Interface Types



Cloud IT Governance: metrics 1/3

Approach to Indicator Identification

- Issue: Metrics are needed to know what you need to focus on
- Problem: *You don't know what you don't know!*
- Goal: Metrics must be focused on specific things you want to measure

(ISC)² Italy Chapter

Cloud IT Governance: metrics 2/3

Approach to Indicator Identification

- ***Keep the metrics reproducible***
  - Develop rigorous, objective definitions
  - Build indicator framework tied to Governance phases
- ***Keep the metrics manageable***
  - Leverage existing automated sources of data
  - Make practical decisions to narrow scope as needed
- ***Keep the metrics verificable***
  - Tie to effective cyber processes
  - Avoid incentivizing covert measurement
- ***Provide an increased level of transparency***

SECURITY 10 ANNI SUMMIT

(ISC)² Italy Chapter

Cloud IT Governance: metrics 3/3

Requirements to Indicator Identification

- ***S. Payne, "A Guide to Security Metrics"***
- ***NIST***
  - ***SP 800-53 Rev 3***
  - ***SP 800-55 Rev 1, Sections 5.0-6.0***
  - ***SP 800-100, Section 7.0 (summarizes 800-55)***
- ***CIS Security Metrics***

SECURITY 10 ANNI SUMMIT

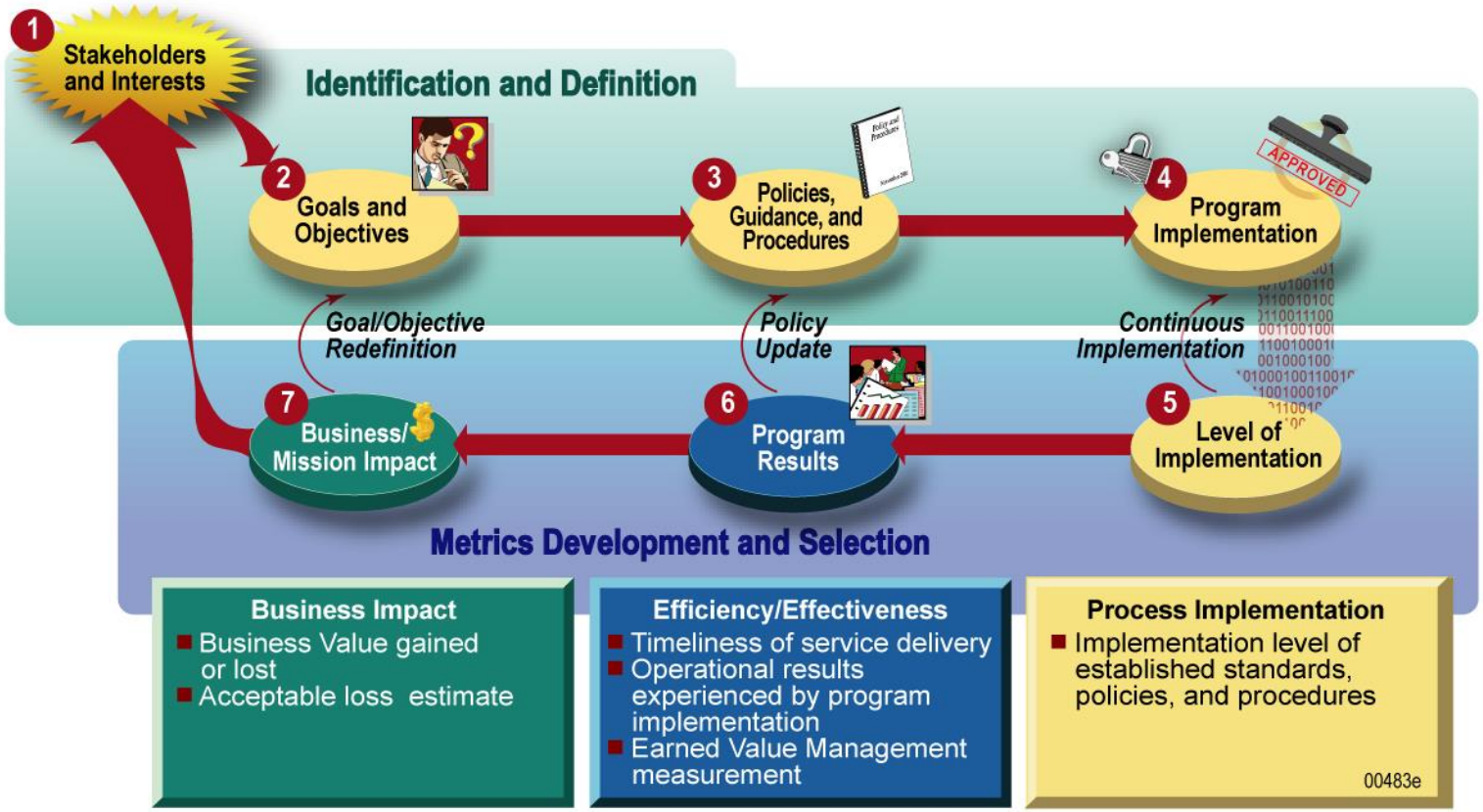
IT Governance: Payne

Seven Steps

1. Define the metrics program goal(s) and objectives
2. Decide which metrics to generate
3. Develop strategies for generating the metrics
4. Establish benchmarks and targets
5. Determine how the metrics will be reported
6. Create an action plan and act on it, and
7. Establish a formal program review/refinement cycle

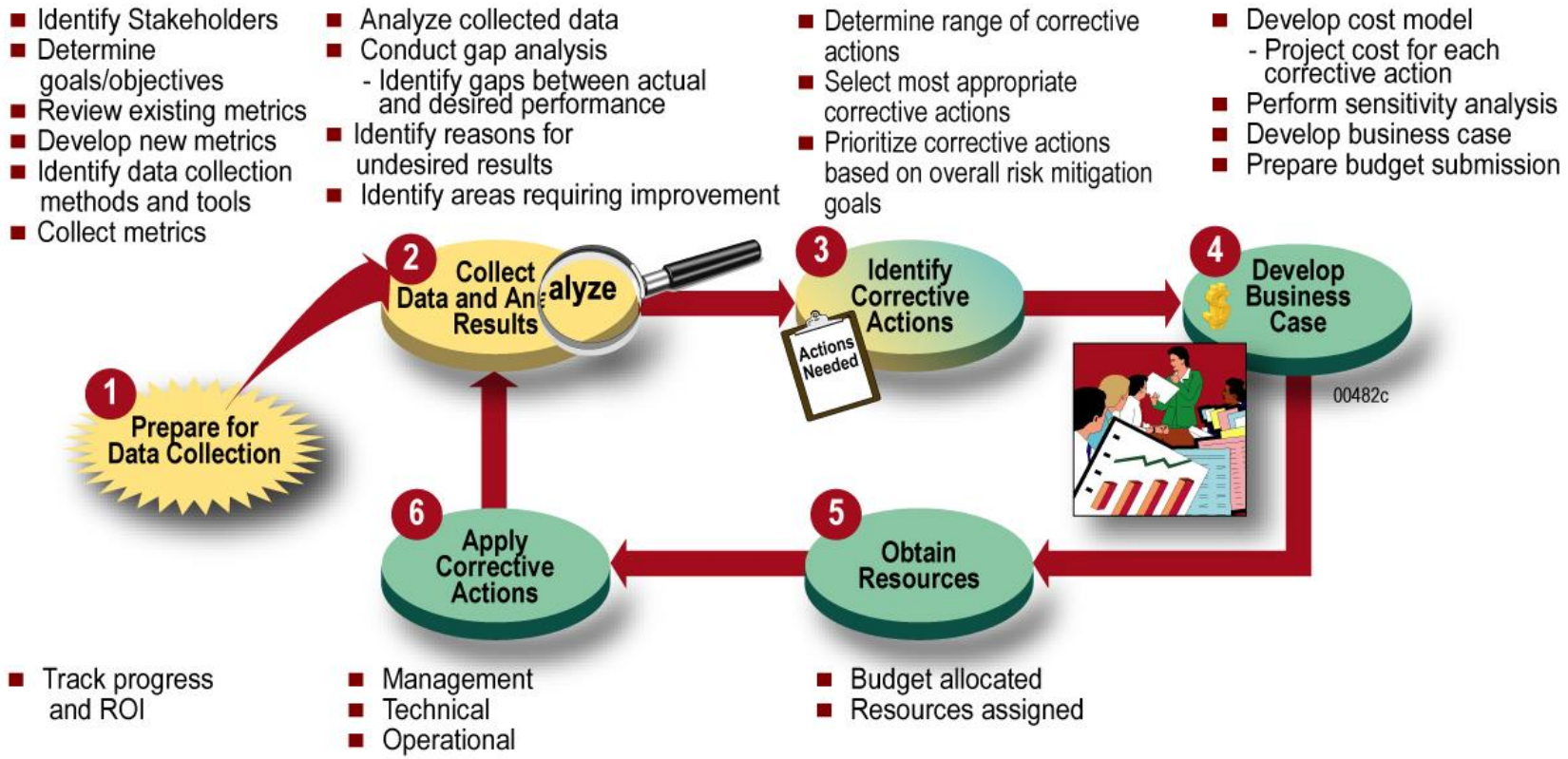
IT Governance: NIST 1/2

Integrated Program



IT Governance: NIST 2/2

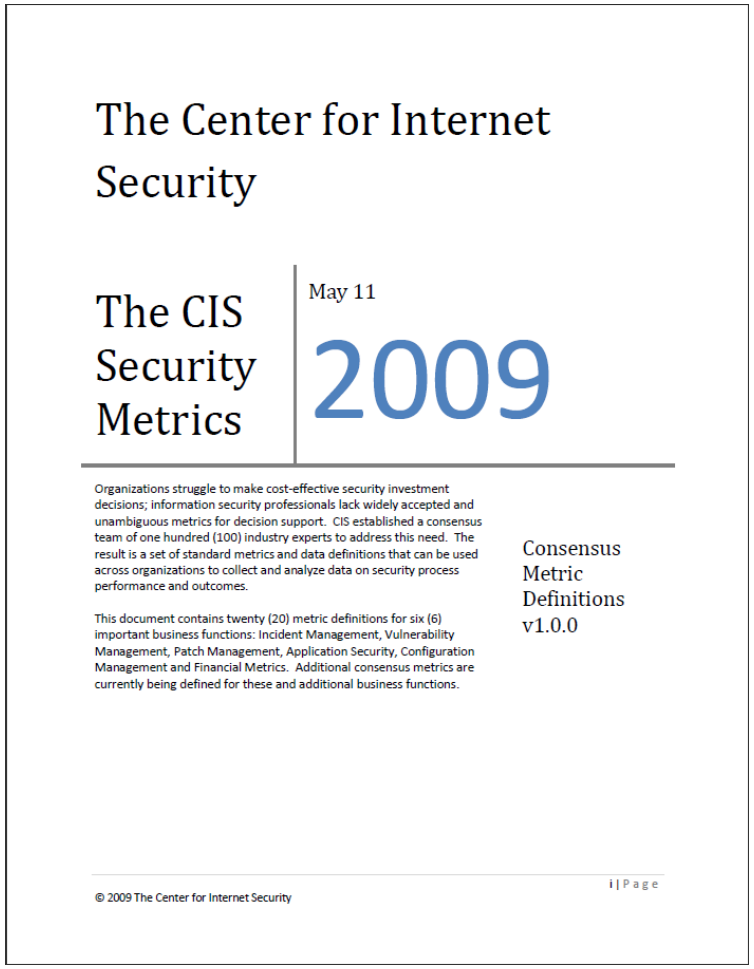
Collecting and Analyzing Data



(ISC)² Italy Chapter

IT Governance: CIS Security Metrics 1/2

Definitions



The Center for Internet Security

The CIS Security Metrics

May 11

2009

Organizations struggle to make cost-effective security investment decisions; information security professionals lack widely accepted and unambiguous metrics for decision support. CIS established a consensus team of one hundred (100) industry experts to address this need. The result is a set of standard metrics and data definitions that can be used across organizations to collect and analyze data on security process performance and outcomes.

This document contains twenty (20) metric definitions for six (6) important business functions: Incident Management, Vulnerability Management, Patch Management, Application Security, Configuration Management and Financial Metrics. Additional consensus metrics are currently being defined for these and additional business functions.

Consensus Metric Definitions v1.0.0

- Well-defined and documented
- Reasonably broad in scope (incident, vulnerability, patch, application, CM, financial)
- Actionable, for the most part
- Not too big (20 metrics)

SECURITY SUMMIT

(ISC)² Italy Chapter

IT Governance: CIS Security Metrics 2/2

Functions

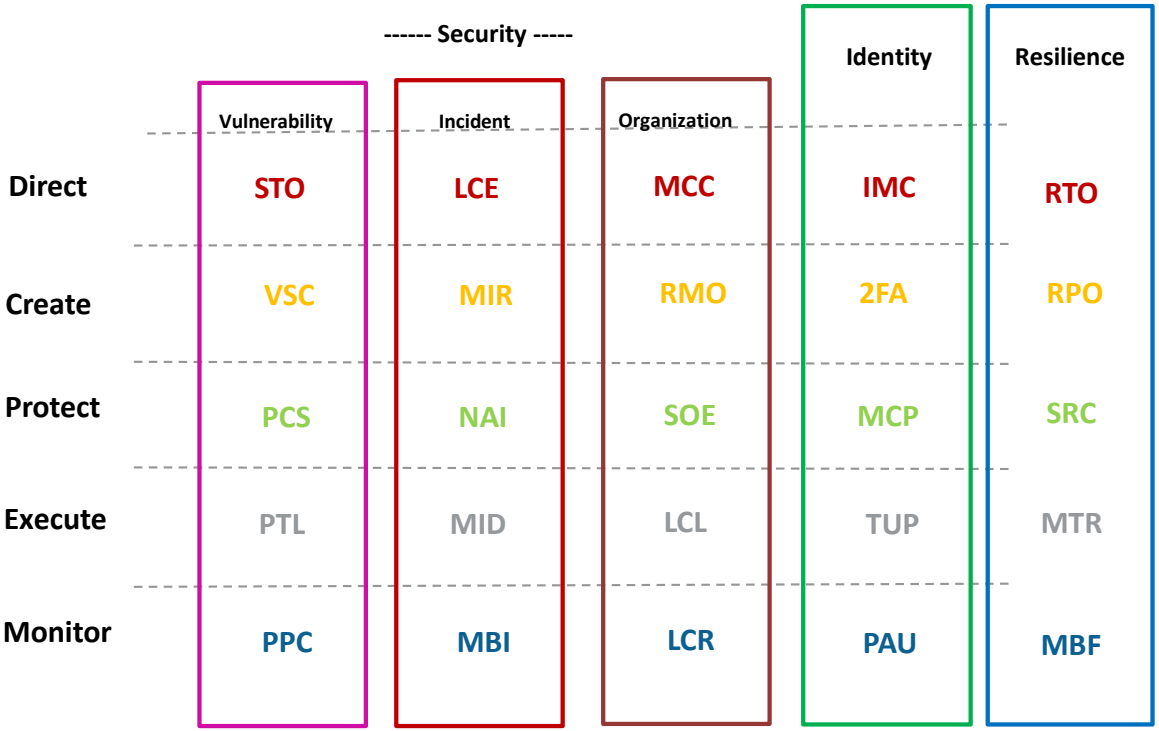
Function	Management Perspective	Defined Metrics	Cloud Governance
Incident Management	How well do we detect, accurately identify, handle, and recover from security incidents?	• Mean Time to Incident Discovery • Number of Incidents • Mean Time Between Security Incidents • Mean Time to Incident Recovery	• MID • NAI • MBI • MIR
Vulnerability Management	How well do we manage the exposure of the organization to vulnerabilities by identifying and mitigating known vulnerabilities?	• Vulnerability Scanning Coverage • Percent of Systems with No Known Severe Vulnerabilities • Mean Time to Mitigate Vulnerabilities • Number of Known Vulnerabilities	• VSC • PCS • PTL • -
Patch Management	How well are we able to maintain the patch state of our systems?	• Patch Policy Compliance • Patch Management Coverage • Mean Time to Patch	• PPC • PCS • PTL
Application Security	Can we rely on the security model of business applications to operate as intended?	• Number of Applications • Percent of Critical Applications • Risk Assessment Coverage • Security Testing Coverage	• - • - • - • VSC
Configuration Management	How do changes to system configurations affect the security of the organization?	• Mean Time to Complete Changes • Percent of Changes with Security Reviews • Percent of Changes with Security Exceptions	• MCC • RMO • SOE
Financial Metrics	What is the level and purpose of spending on information security?	• IT Security Spending as % of IT Budget • IT Security Budget Allocation	• - • -

SECURITY 10 ANNI SUMMIT

(ISC)² Italy Chapter

IT Governance Implementation 1/7

Governance Indicators by Areas



SECURITY 10 ANNI SUMMIT

(ISC)² Italy Chapter

IT Governance Implementation 2/7

Governance Indicators about Security (Vulnerability)

------ Security -----

Vulnerability

Security Testing Objectives (STO) how much time from one pen test to another

Vulnerability Scan Coverage (VSC) percentage of system VA is performed upon

Platform Compliance Score (PCS) percentage of system configuration meeting best-practice standards

Patch Latency (PTL) time between a patch's release and your successful deployment of that patch

Patch Policy Compliance (PPC) percentage of system patching meeting patch policy

(ISC)² Italy Chapter

IT Governance Implementation 3/7

Governance Indicators about Security (Incident)

------ Security -----

Incident

Log Correlation Effectiveness (LCE) percentage of incidents identified by correlation

Mean Time for Incident Recovery (MIR) time from incident discovery to recovery

Number of Annual Incident (NAI) how many incident per year

Mean Time for Incident Discovery (MID) time occurring from incident and its discovery

Meantime Between Incident (MBI) incident rates: how often these occur

SECURITY SUMMIT

(ISC)² Italy Chapter

IT Governance Implementation 4/7

Governance Indicators about Security (Organization)

------ Security -----

Organization

Meantime to Complete Change (MCC) how much time from change issue to implementation

Risk Management Objective (RMO) percentage of suggested countermeasure implemented

Security Objective Exception (SOE) percentage of change with exception

Log Collection Latency (LCL) delay from event and trasmission of log to central SIEM

Log Correlation (LCR) average number of correlation rule per system

SECURITY SUMMIT 10 ANNI

(ISC)² Italy Chapter

IT Governance Implementation 5/7

Governance Indicators about Identity

Identity

Identity Management Coverage (IMC) proportion of account (privileged and unprivileged) vaulted and managed

Two Factor Authentication percentage (2FA) percentage of user that should use 2FA for accessing the systems

Meantime to Certified Privileged Account (MCP) time a Privileged Account is certified

Time for User Provisioning average (TUP) how long a new user waits to get access to the resources they need

Privileged Account average per User (PAU) amount of «duties» owned by a user (SoD)

SECURITY SUMMIT

IT Governance Implementation 6/7

Governance Indicators about Resilience

Resilience

Recovery Time Objective (RTO) maximum time needed for recover the service

Recovery Point Objective (RPO) time the transaction occurred before accident could not be recovered

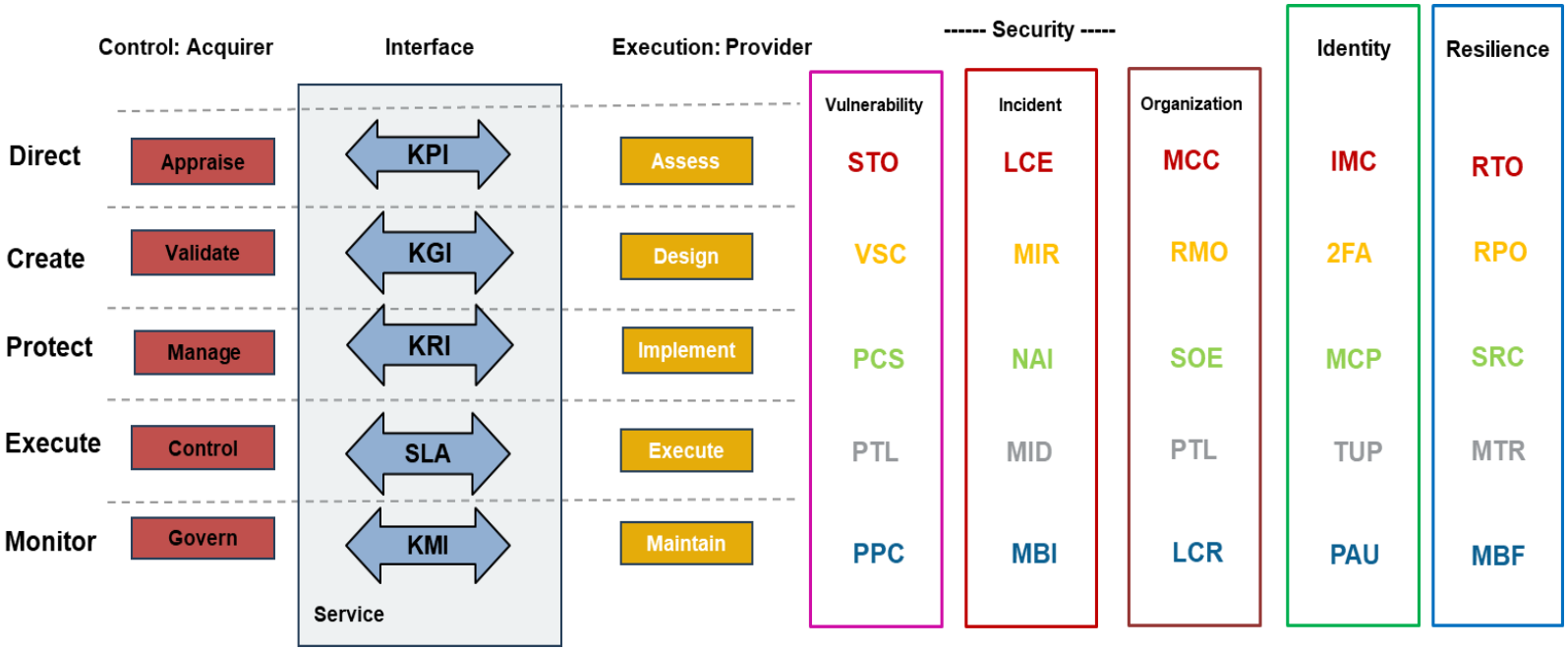
System Recovery Coverage (SRC) percentage of systems covered by BC/DR

Meantime To Repair (MTR) average time to recover the service

Meantime Between Failure (MBF) average time from a failure to another one

IT Governance Implementation 6/7

Putting all Together



(ISC)² Italy Chapter

Grazie!

Paolo Ottolino CISSP-ISSAP CISM CISA ISO/IEC 27001 OPST PRINCE2 PMP ITIL
paolo.ottolino@isc2chapter-italy

SECURITY 10 ANNI SUMMIT