Implementing Administrative Operational Controls

Dr. Lyron H. Andrews
CISSP/CCSP/SSCP/CRISC/CISM/CCSK

https://www.profabula.com/whyprofabula

Overview

Review prominent administrative controls for ITSM

Apply administrative controls to physical and logical cloud security

Information Technology Service Management (ITSM)

ISO/IEC 20000-1:2018 (SMS)

Service Management System

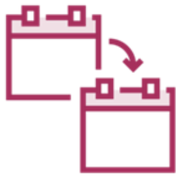
ITIL v4

Information Technology Infrastructure Library

ISO/IEC 20000-1:2018 SMS Overview

Customer and provider connection

Agnostic and independent



One part of many

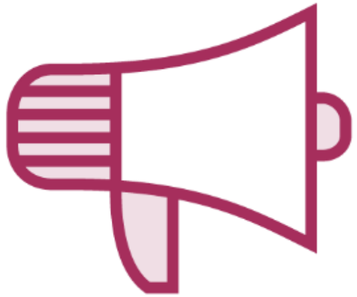
Elements of ISO/IEC 20000-1:2018

Organization context

Leadership

Program planning

Elements of ISO/IEC 20000-1:2018



Support for SMS

Operational planning

Relationship and agreement

Elements of ISO/IEC 20000-1:2018

Supply and demand

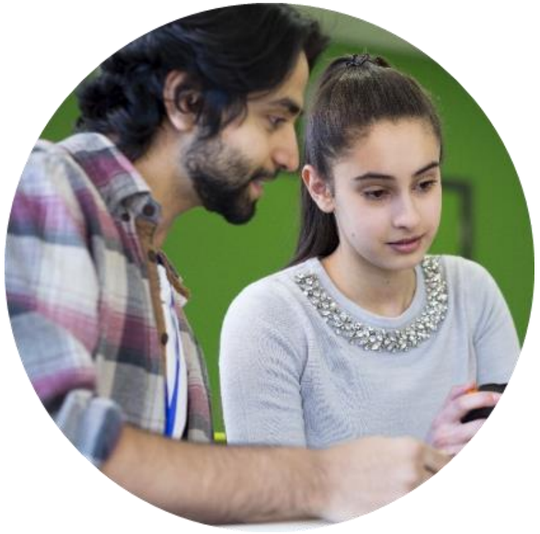
Performance evaluation

Improvement

ITIL v4 - Four Dimensions

Organizations and people

Information and technology



Partners and suppliers

Value streams and processes

Primary Elements of ITIL v4

Service value chain

Practices

Guiding principles

Governance

Continual improvement

ITSM Basics

Change Management

Incident Management

Release Management

Configuration Management

Deployment Management

Patch Management

Implementing Change Management

Did you enjoy attending your last change management meeting?

Are you impatiently waiting to attend your next one?

What makes change management so undesirable?

“The practice of ensuring that changes in an organization are smoothly and successfully implemented and that lasting benefits are achieved by managing the human aspects of the changes.”

Change Management (ITIL Foundation - v4 definition)

Components of Change Management

Policy

Initiation

Activities

Plan

Improve

Engage

Design and transition

Obtain/build

Deliver and support

Change Management Activities

Standard

Normal

Emergency

Types of Change

Configuration Management Goals

Identify new items

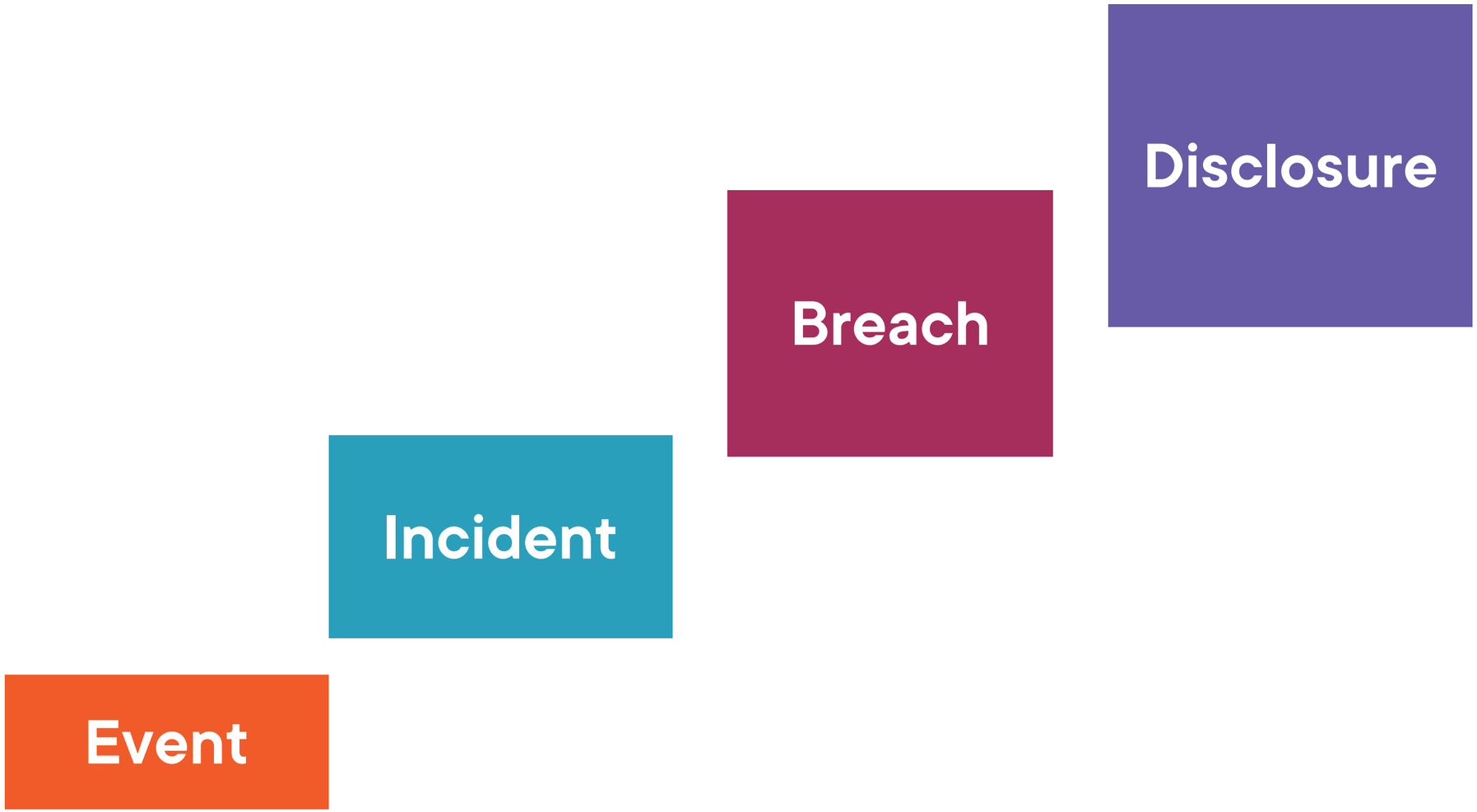
Update changes

Verify accuracy

Audit nonconformity

Implementing Incident and Problem Management

Incidents – Relative to Other Occurrences



Incident Management Essentials

Minimize negative impact

Logged and resolved

Prioritization and classification

Impact

Urgency

Priority

Incident Classification and Prioritization

ISO/IEC 20000-1:2018 Incident Management

Recorded

Prioritized

Escalated

Resolved

Closed

CMU/SEI Incident Management Capability

Prepare

Protect

Detect

Respond

Sustain

Availability, Capacity, and Service Level Management

Service-level Agreements (SLAs) Basic

Writing from provider's perspective

Works as compensation tool

Uptime vs. availability

ISO/IEC DIS 19086-1:Cloud (SLA) Framework

Part 1:

Overview and concepts

Part 2:

Metrics

Part 3:

Core requirements

SLA Elements

Accessibility

Availability

Capacity

Elasticity

Service monitoring

Roles and responsibilities

SLA Elements

Service resilience/fault tolerance

Audits, certifications, attestations

Changes to features

Response time

Termination of services

Service Level Management Guidelines

Target alignment

Data-driven evidence

Continuous reviews

Catalogue alignment

Requirements documented

Service metrics

Manage Communications with Relevant Parties

“Openness Principle: There should be a general policy of openness about developments, practices, and policies with respect to personal data.”

Organization for Economic Cooperation and Development

“Cloud service providers must inform customers where their data resides, disclose the use of subcontractors to process PII and make clear commitments about how that data is handled.”

ISO/IEC 27018:2019 Protection of Personal Data in the Cloud

A data controller “must be able to demonstrate that personal data are processed in a transparent manner in relation to the data subject.”

General Data Protection Regulation

Maintenance schedule

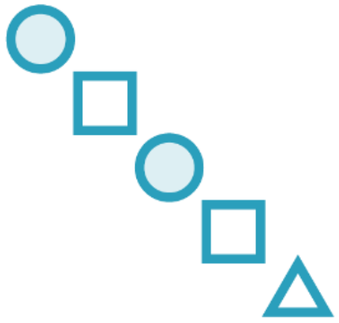
Personal data breach

Transparency report

Transparency Concerns

Implementing Release, Deployment, and Patch Management

Release, Deployment, and Patch Management

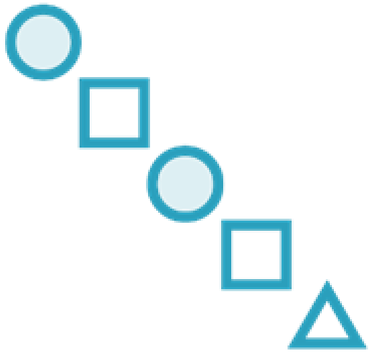


Release management

Deployment management

Patch management

Release Management



Variable nature of releases

Effort before and after release

Stages of release

Deployment Management

New or changed items moved to live environments

Contrast with release management

Various approaches

Patch Management

Designed to rectify issues with existing systems

Organizations must consider risks

Primary considerations of process

Continuous Integration/Continuous Delivery (CI/CD)

Development team focus

Small and frequent

Building, packaging, testing

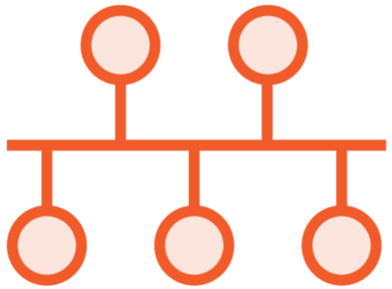
Multi-tiered integration

Integrated controls

Mutable vs. Immutable Environments

Mutable	Immutable
VMs managed like servers	VMs are not preserved when out of date
Changes over weeks/days	Changes over hours/minutes
Partial automation	Full automation

Function as a Service (Serverless Architecture)



Microservices

Containers

Summary

Where in the administrative control space can your organization improve?

What administrative controls are most important for success in your cloud consumption strategy?

Up Next:
Manage Security Operations