Information and Communications Security SS 22
Guest Lecture 3
Security Management

28th June 2022, Frankfurt

Michael Schmid
michael.schmid@m-chair.de
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de

Speaker

Michael Schmid (Dipl. Inf., MBA, CISM, ITIL, BSIG §8a, ISO Lead Auditor)

- since 2012 deputy CISO @Hubert Burda Media Holding KG
- since 2017 PhD student @m-chair
- since 2017 founder and board member of AUDEG - Deutsche Auditoren eG
- University Lecturer & Scientific Reviewer
- > 15 years experience in the field of IT / Information Security
- areas of focus: ISMS, IT Compliance & Governance and Risk Management
- active participation in (inter)national committees: UPKRITIS, ISACA, GI & RMA

Agenda

I. Introduction Security Management
II. Information Security Management System
III. Risk Management
IV. Business Continuity & Incident Management
V. Information Security Measurement
VI. Literature

Agenda

I. **Introduction Security Management**
II. Information Security Management System
III. Risk Management
IV. Business Continuity & Incident Management
V. Information Security Measurement
VI. Literature

I. Introduction Security Management

Security Management, what is Security Management?

To understand the main purpose of Security Management we need to look at both Security and Management in their individual roles and current descriptive meanings in the industries of today.

Security

Security of today is very different from what it was perceived at the turn of the 20th Century. Security is constantly evolving to meet the requirement of tackling the ever evolving 'Threat' and the needs of the organisation. It is not only for the purposes of the commercial industry as it also interacts with the public on a daily basis.

I. Introduction Security Management

Management

The word Manage comes from the Italian maneggiare [maned'dZa:re] (to handle, especially tools), which derives from the Latin word manus (hand). The French word ménagement [menaʒmã] influenced the development in meaning of the English word management in the 17th and 18th centuries.

Management is a word commonly used to describe a position of responsibility in the Business, Political, Cultural or Social industries.

There are various definitions of management, yet the industry standard is simply defined as a process of getting the task completed efficiently with and through other people in accordance with the organisations policies and objectives.

I. Introduction Security Management

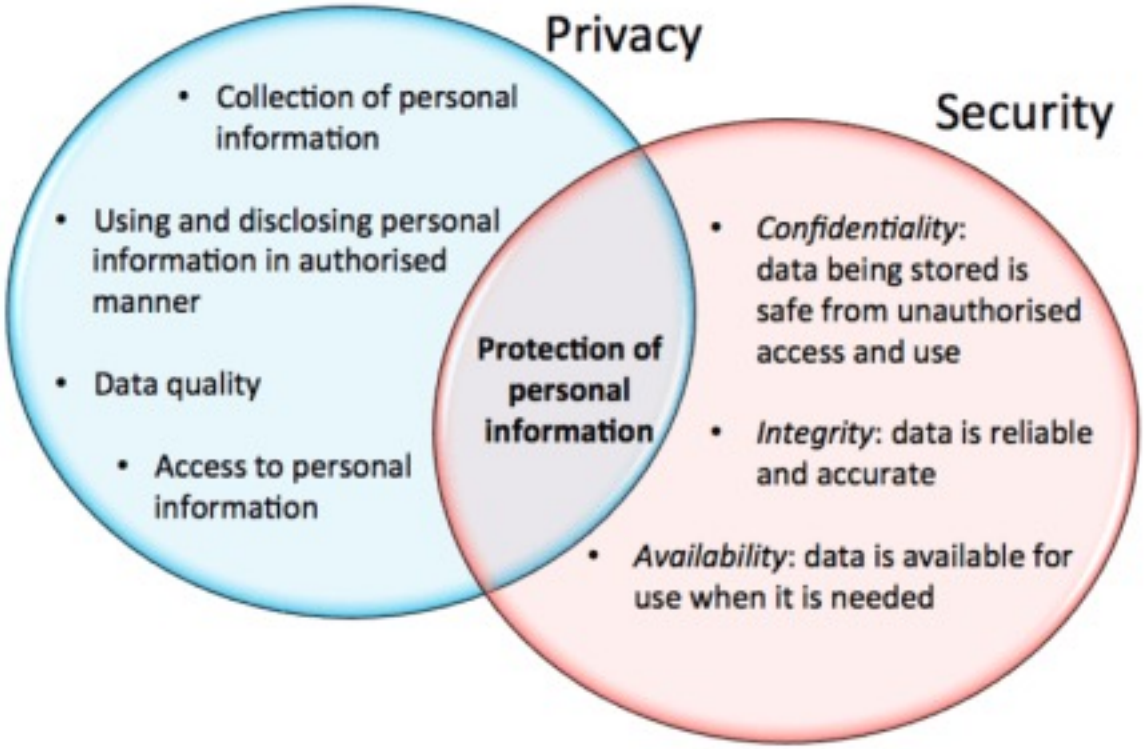
What is the main purpose of Security Management?

One of the main tasks to be completed upon appointment is to carry out a full risk assessment of the threat the organisation is exposed to. This includes the following:

- Internal practices & procedures – This includes examining the organisations activities from recruitment to how the organisations records are kept in compliance with the new GDPR regulations, as well as how it conducts its day to day business.
- Physical risks to premises – Conducted by assessing the plans for the premises and evaluating the points of entry, not just the normal entrance points but those subject to risk to be entered through illegally i.e. a ground floor window.
- External risks – There are wide ranging factors involved when assessing the external risks. The location, building, current criminal activities within the area as well as the surrounding environment and accessibility of the location.

I. Introduction Security Management

Privacy vs. Security



Source: davidfroud.com

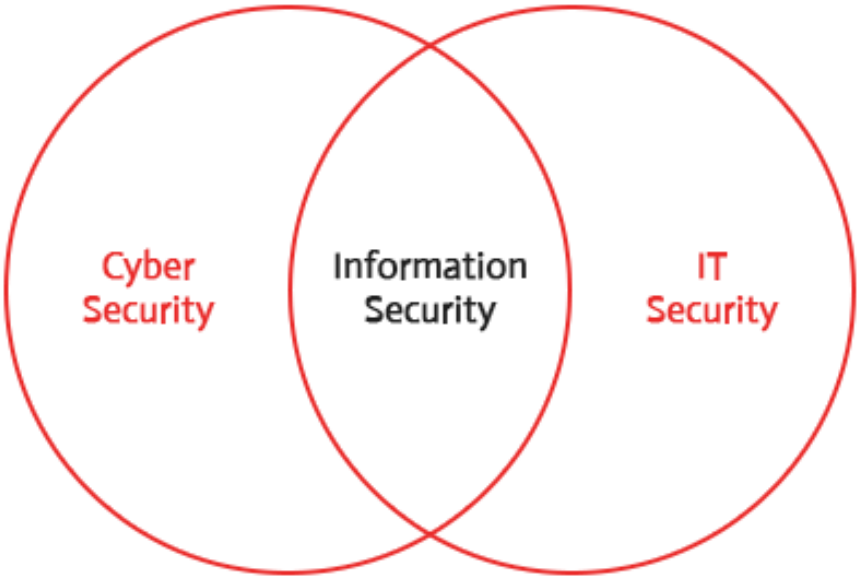
I. Introduction Security Management

CIA vs. Information security?

Source: comtact.co.uk

I. Introduction Security Management

Cyber vs. Information vs. IT Security



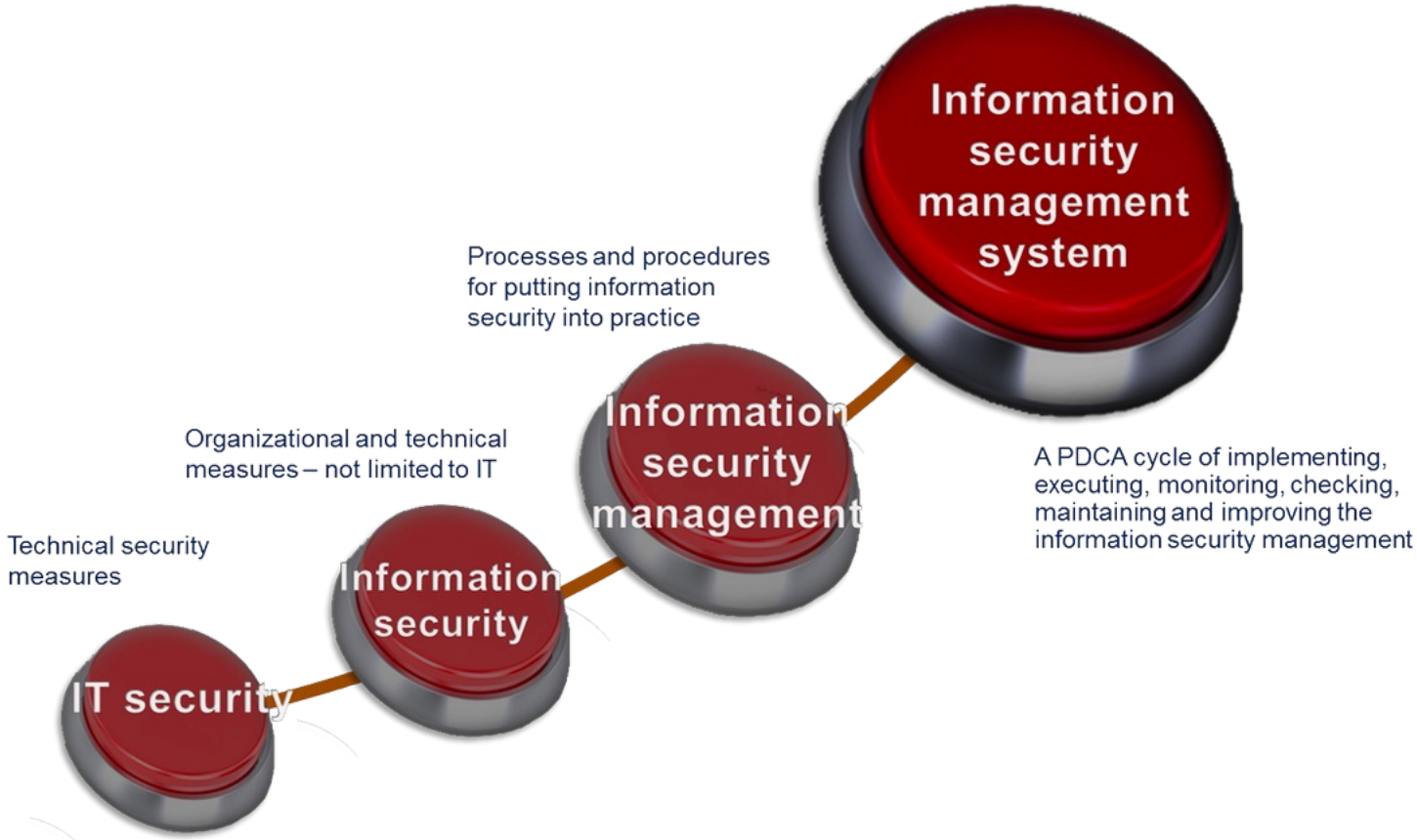
Source: businessbeam.com

Agenda

I. Introduction Security Management
II. Information Security Management System
III. Risk Management
IV. Business Continuity & Incident Management
V. Information Security Measurement
VI. Literature

II. Information Security Management System

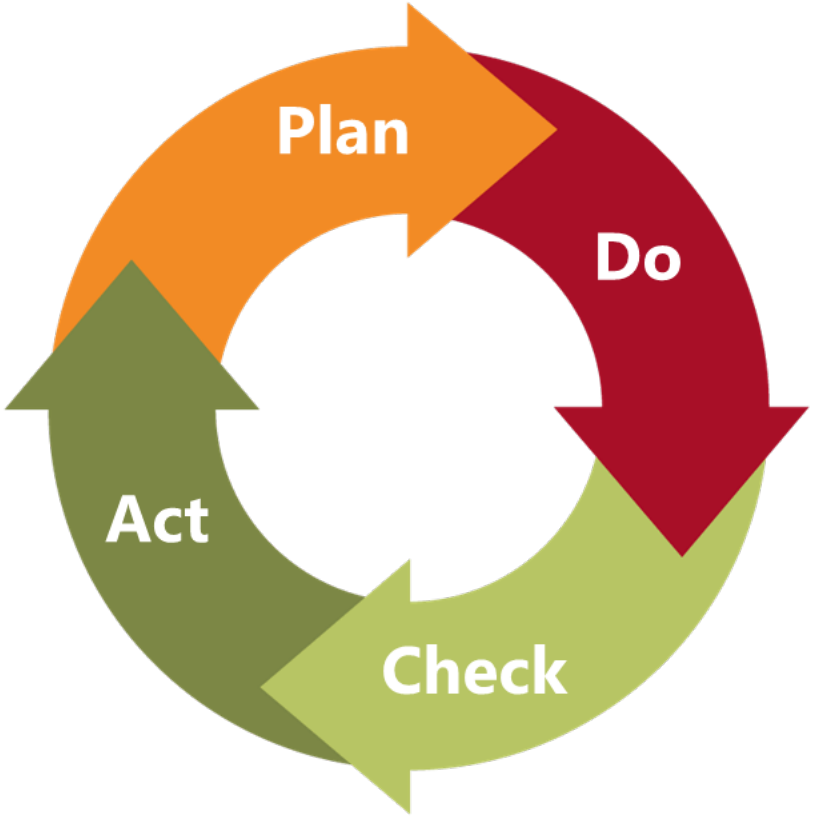
From IT security to an Information security management system



Source: it-pillars.com

II. Information Security Management System

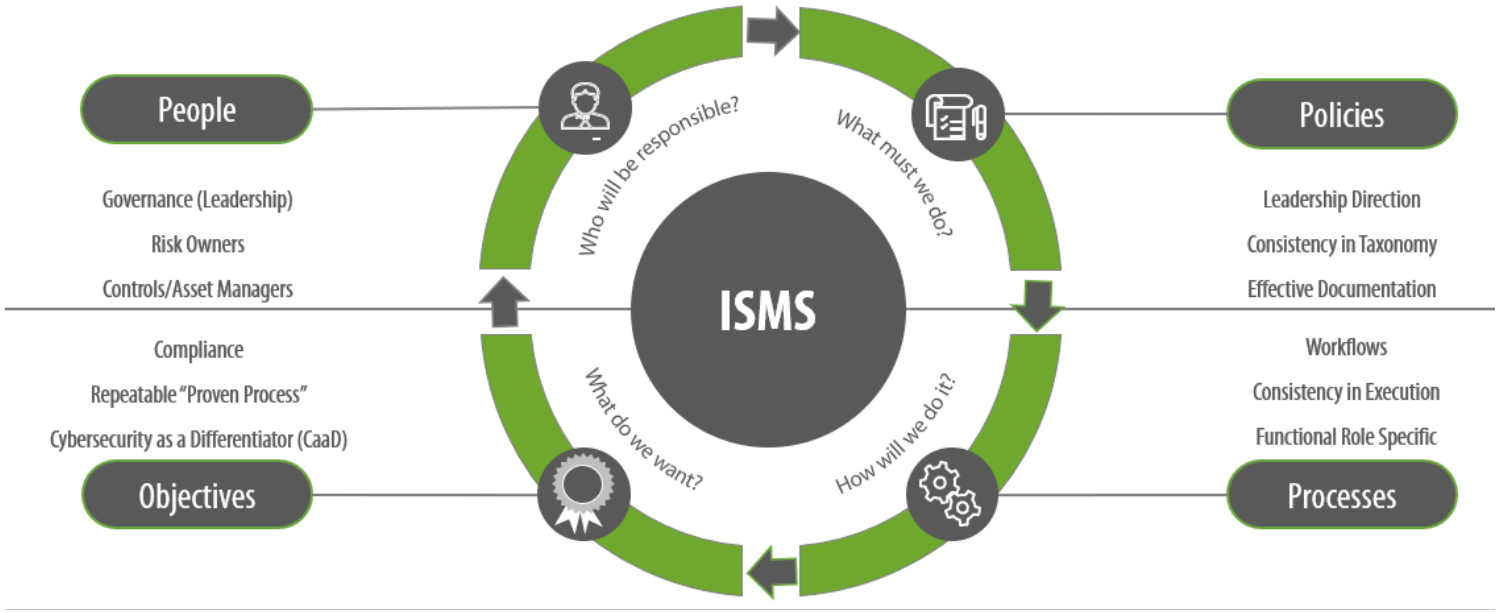
PDCA or Demin circle



Source: glauxsoft.com

II. Information Security Management System

Information **S**ecurity **M**anagement **S**ystem (ISMS)



Source: cyberintsolns.com

II. Information Security Management System

Governance, **R**isk management and **C**ompliance (GRC)

Source: softexpert.com

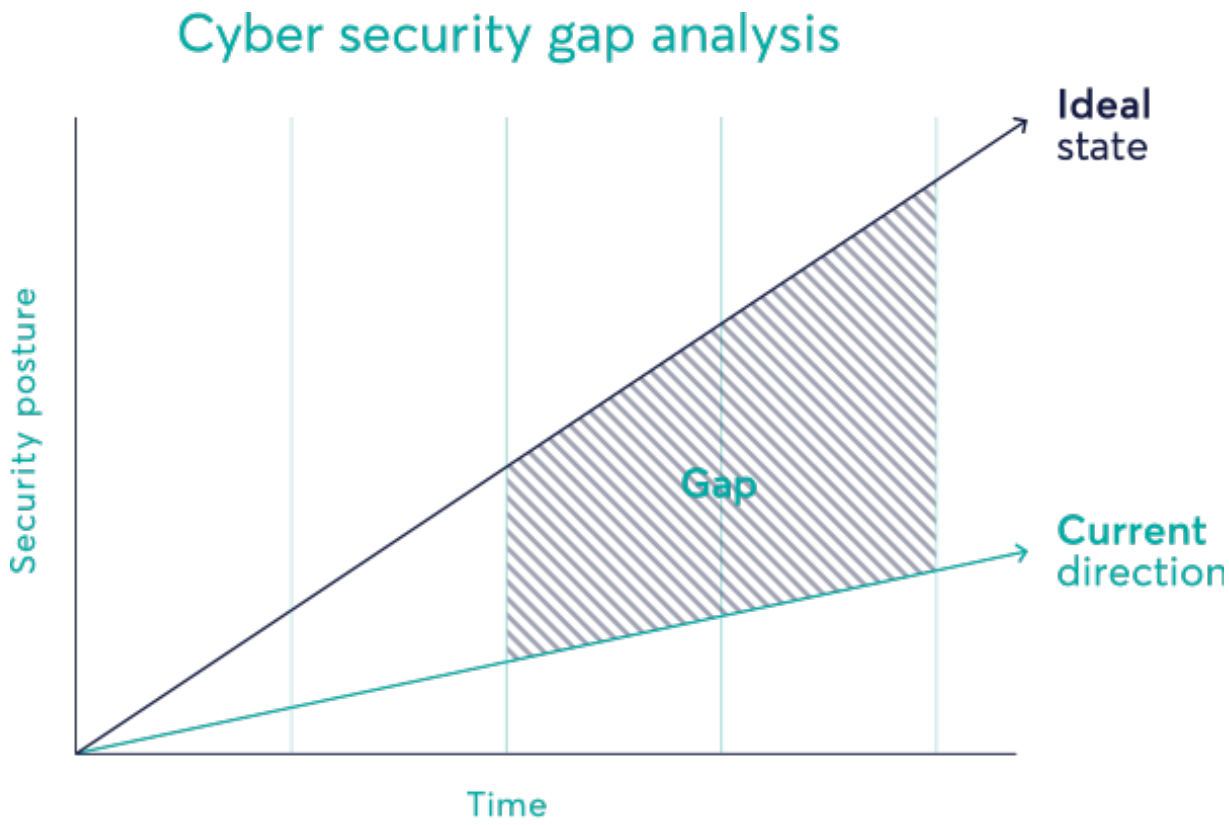
II. Information Security Management System

ISO/IEC 27001:2013 is the internationally recognised management system standard for information security.

Source: caveonix.com

II. Information Security Management System

A **gap analysis** helps determine the steps required to reach your ideal cyber security posture.

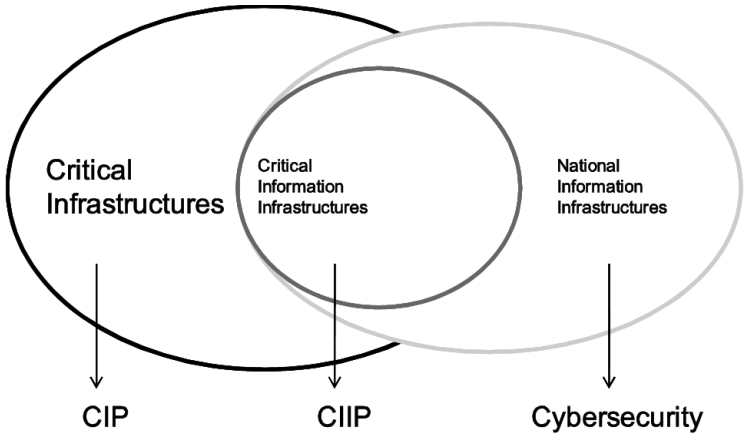


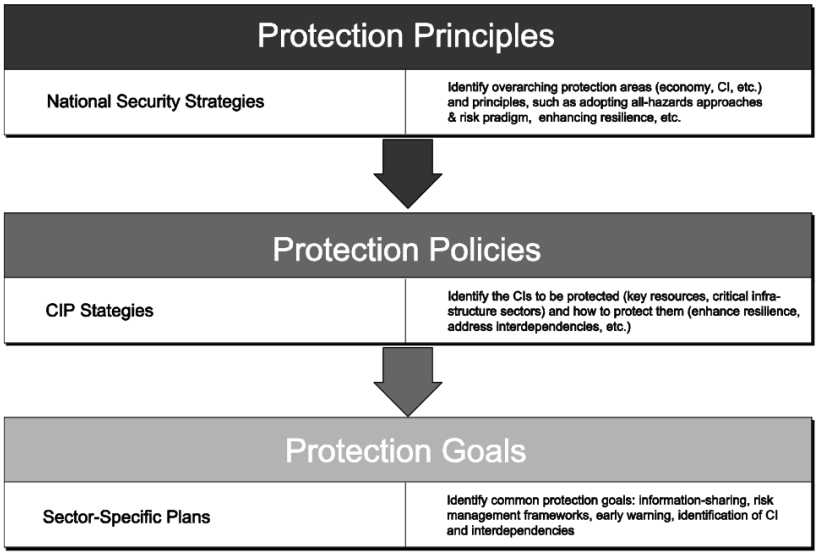
Source: csisgroup.com

II. Information Security Management System

Regulatory requirements in Germany that enforce security management

- **C**ritical **I**nformation **I**nfrastructures **P**rotection (CI(I)P) discover key issues, developments, and trends in order to make recommendations about strategy making in the field of CIIP.





Source: springer.com

II. Information Security Management System

German IT Security Law "1.0"

- Amending act, no codification of IT security
- Entered into force on 25th July 2015
- Amended various existing laws:
  - Act on the Federal Office for Information Security (BSIG)
  - Atomic Energy Act (EnWG)
  - Telemedia Act (TMG)
  - Telecommunications Act (TKG)
  - Act on the Federal Criminal Police Office (BKAG)
- Mostly referring on the protection of Critical Infrastructures, but also including a general extension of power of the BSI according to Sec. 7 BSIG (warnings), Sec. 7a BSIG (examination of IT security)
- Concretization of the scope of application through the BSI-Kritis Regulation, referring to Critical Infrastructures which are defined by certain thresholds in numbers: Energy, Health, ICT, Transport&Traffic, Media, Water, Finance&Insurance, Food, State&Administration

Agenda

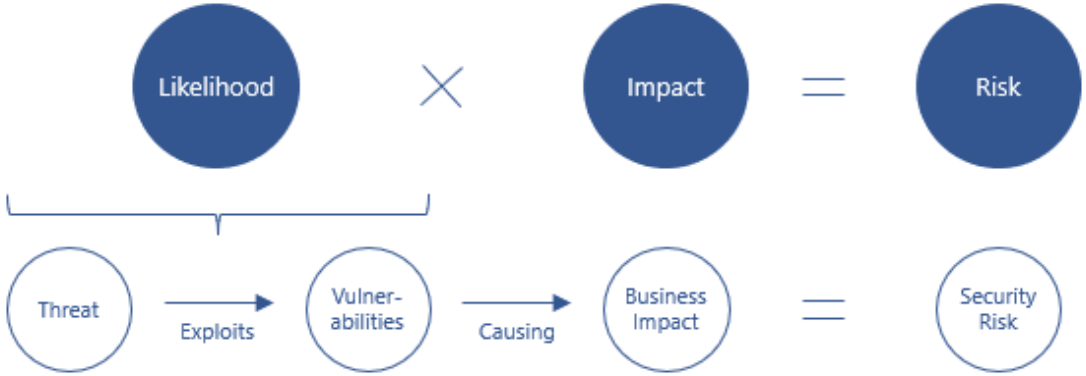
I. Introduction Security Management
II. Information Security Management System
III. Risk Management
IV. Business Continuity & Incident Management
V. Information Security Measurement
VI. Literature

III. Risk Management

Source: pngitem.com

Risk management

Risk is expressed as a combination of the likelihood of an event occurring and the impact on the business expressed in the equation:



Source: b-advisory.ch

III. Risk Management

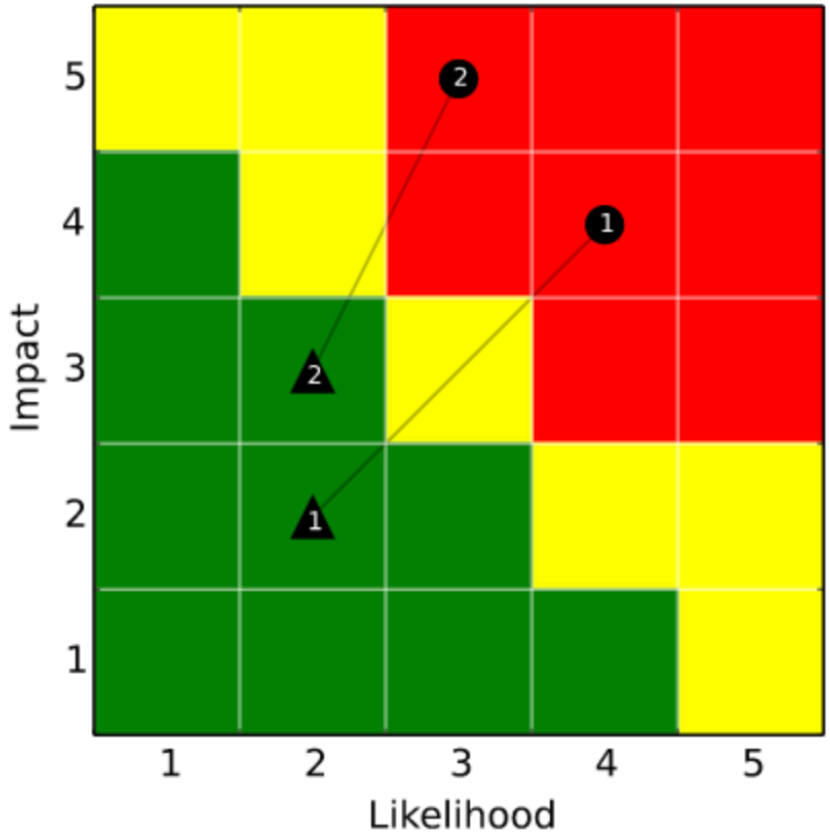
Risk matrix

Impact	rare	unlikely	possible	likely	certain
catastrophic	Low Med	Medium	Med High	High	High
critical	Low	Low Med	Medium	Med High	High
moderate	Low	Low Med	Medium	Med High	Med High
minor	Low	Low Med	Low Med	Medium	Med High
neglectable	Low	Low	Low Med	Medium	Medium

Likelihood

Source: b-advisory.ch

Risk matrix with and without measures

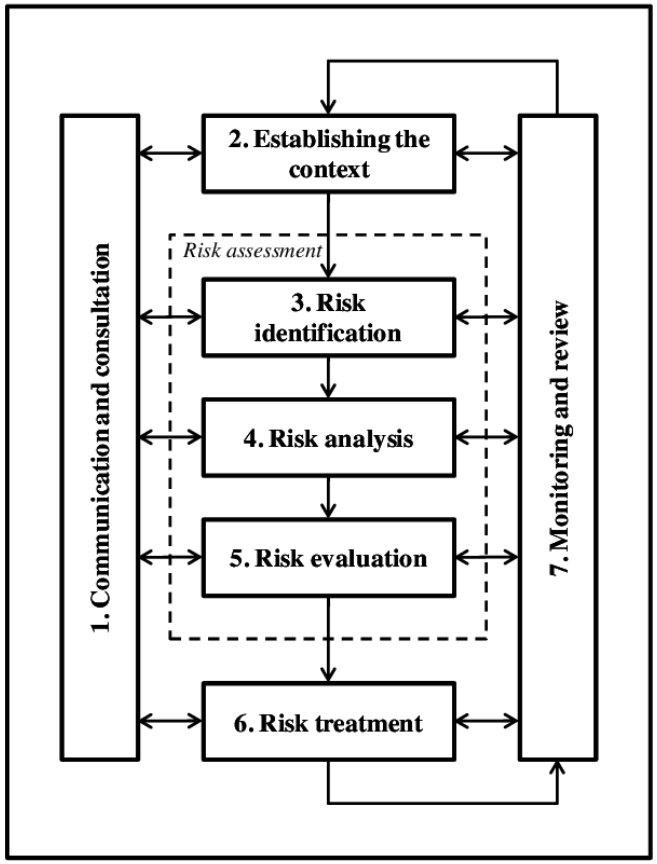


Source: b-advisory.ch

III. Risk Management

ISO 31000:2018 – provides principles and generic guidelines on managing risks faced by organizations

Risk management process

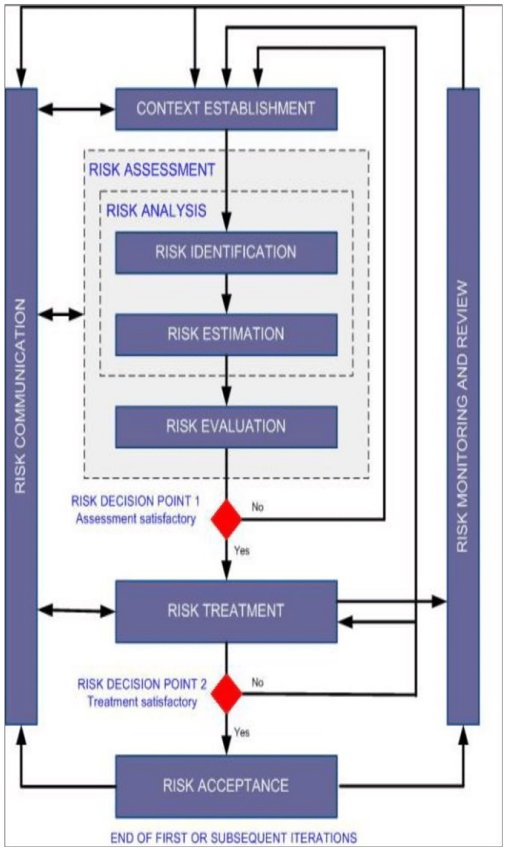


Source: ISO.org

III. Risk Management

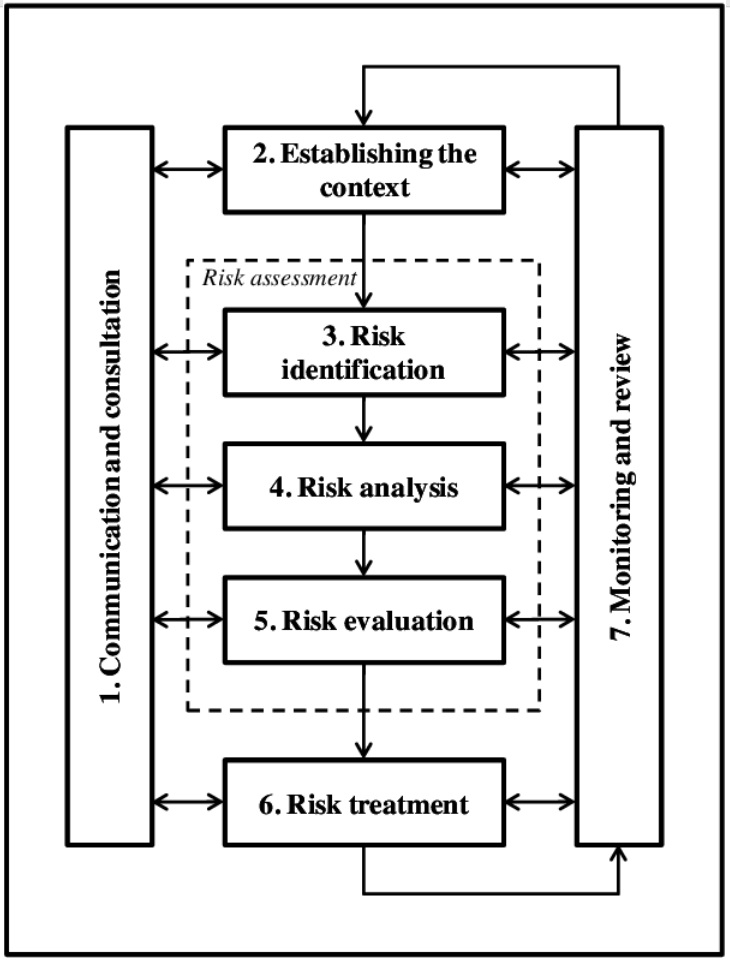
ISO/IEC 27005:2018 - provides guidelines and techniques for managing **information** security risks

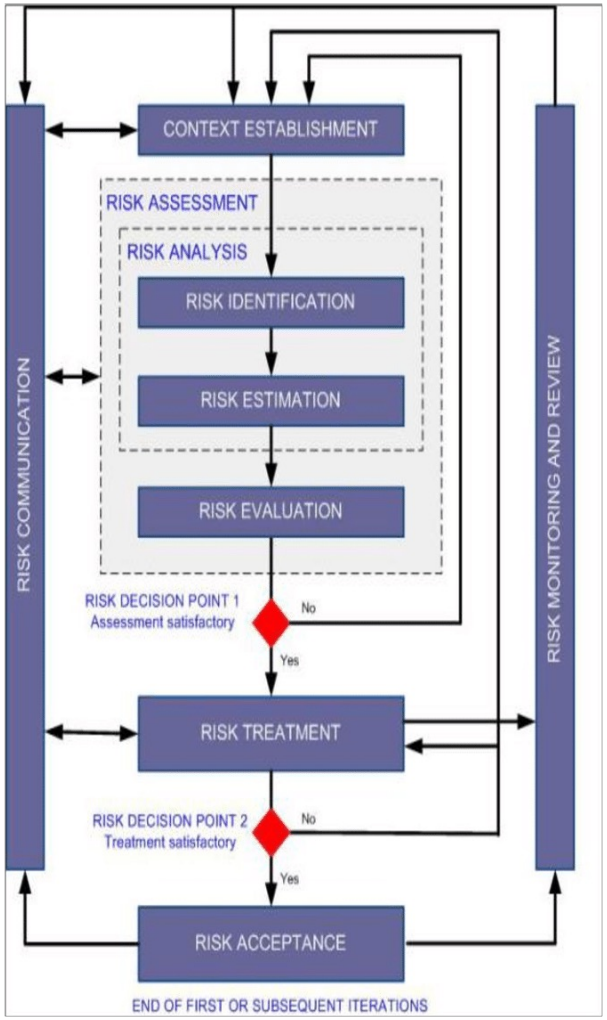
Risk management process



Source: ISO.org

III. Risk Management





Source: ISO.org

III. Risk Management

Risk treatment options

1. Avoidance You can choose not to take on the risk by avoiding the actions that cause the risk.

2. Reduction You can take mitigation actions that reduce the risk. For example, wearing a life jacket when you swim.

3. Transfer You can transfer all or part of the risk to a third party. The two main types of transfer are insurance and a company may choose to transfer a collection of project risks by outsourcing the project.

4. Acceptance Risk acceptance, also known as risk retention, is choosing to face a risk. In general, it is impossible to pro enjoy an active life without choosing to take on risk.

Agenda

I. Introduction Security Management
II. Information Security Management System
III. Risk Management
IV. Business Continuity & Incident Management
V. Information Security Measurement
VI. Literature

IV. Business Continuity & Incident Management

Business **C**ontinuity **M**anagement (BCM)

Source: Accenture

IV. Business Continuity & Incident Management

Business **C**ontinuity **M**anagement **S**ystem (BCMS)

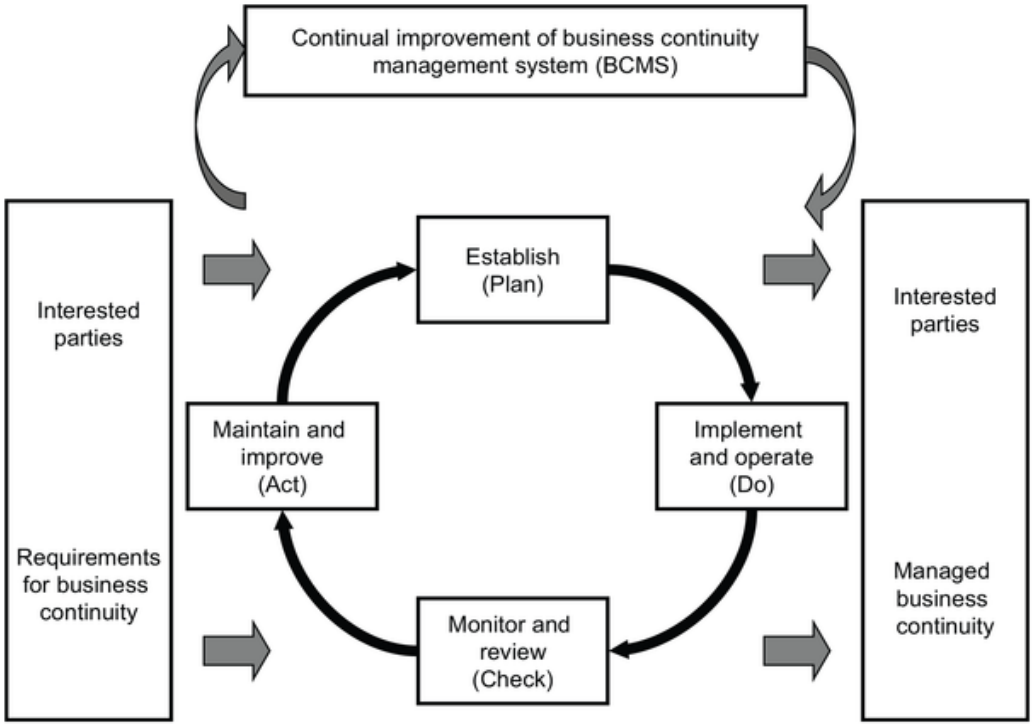
1. Incident Management Plan (IMP)
2. Incident Communication Plan (ICP)
3. Disaster Recovery Plan (DRP)
4. Business Continuity Plan (BCP)
5. Test, Maintain and Review
6. Awareness & Training

Source: preparedex.com

IV. Business Continuity & Incident Management

ISO 22301:2019 - specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise

BCM process



Source: ISO.org

IV. Business Continuity & Incident Management

Business **I**mpact **A**nalysis (BIA)

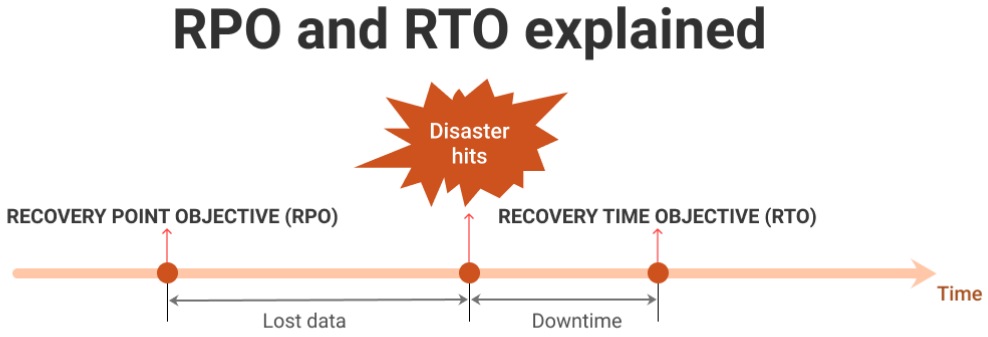
A BIA is a process that allows us to identify critical business functions and predict the consequences a disruption of one of those functions would have. It also allows us to gather information needed to develop recovery strategies and limit the potential loss.

Completing a BIA will assess the risks of a disaster on the organization. It will allow for each department within your organization to explain and discuss how an unexpected event would affect their business function. This will then help your organization prioritize specific functions through the use of Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO).

IV. Business Continuity & Incident Management

Recovery **P**oint **O**bjective **(RPO)** describes the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan's maximum allowable threshold or "tolerance".

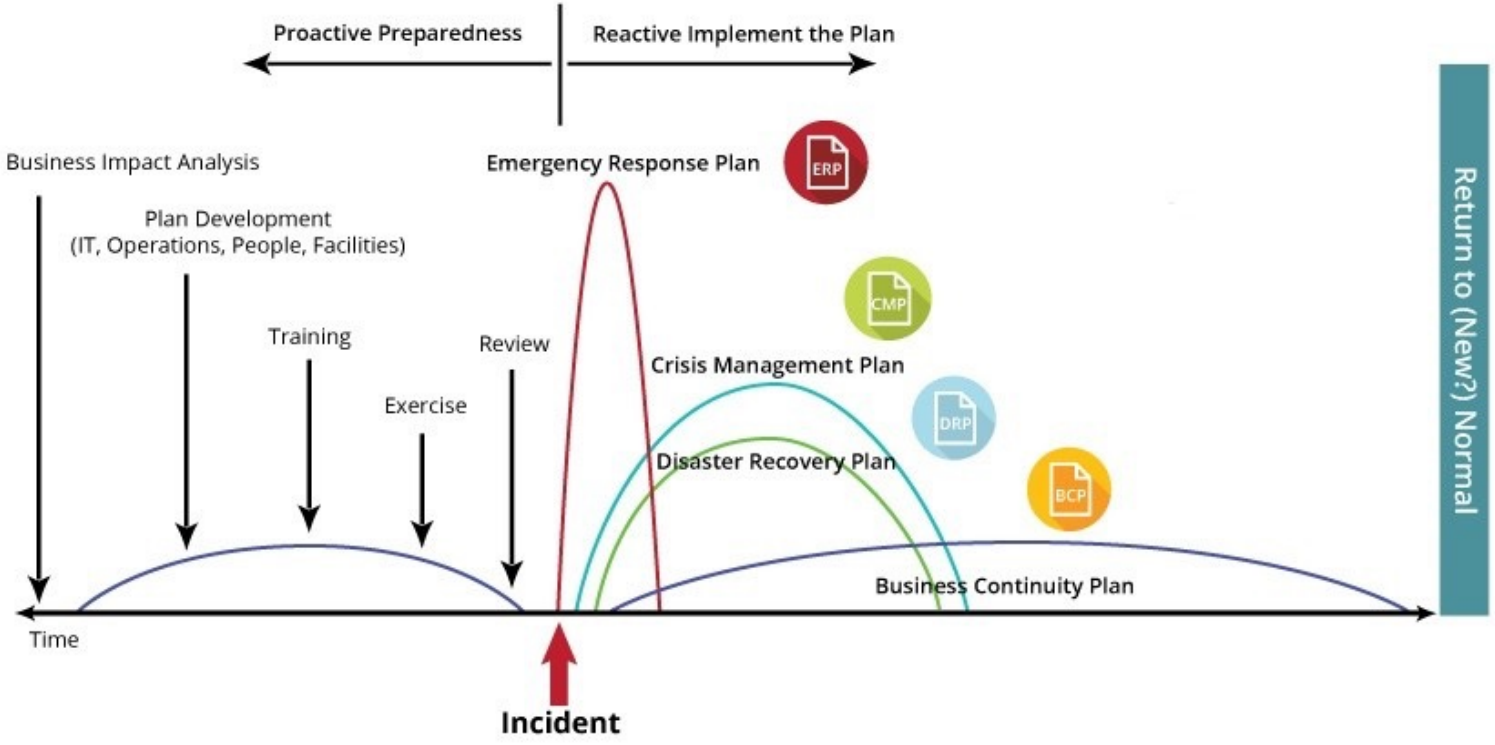
The **R**ecovery **T**ime **O**bjective **(RTO)** is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity. In other words, the RTO is the answer to the question: "How much time did it take to recover after notification of business process disruption?"



Source: msp360.com

IV. Business Continuity & Incident Management

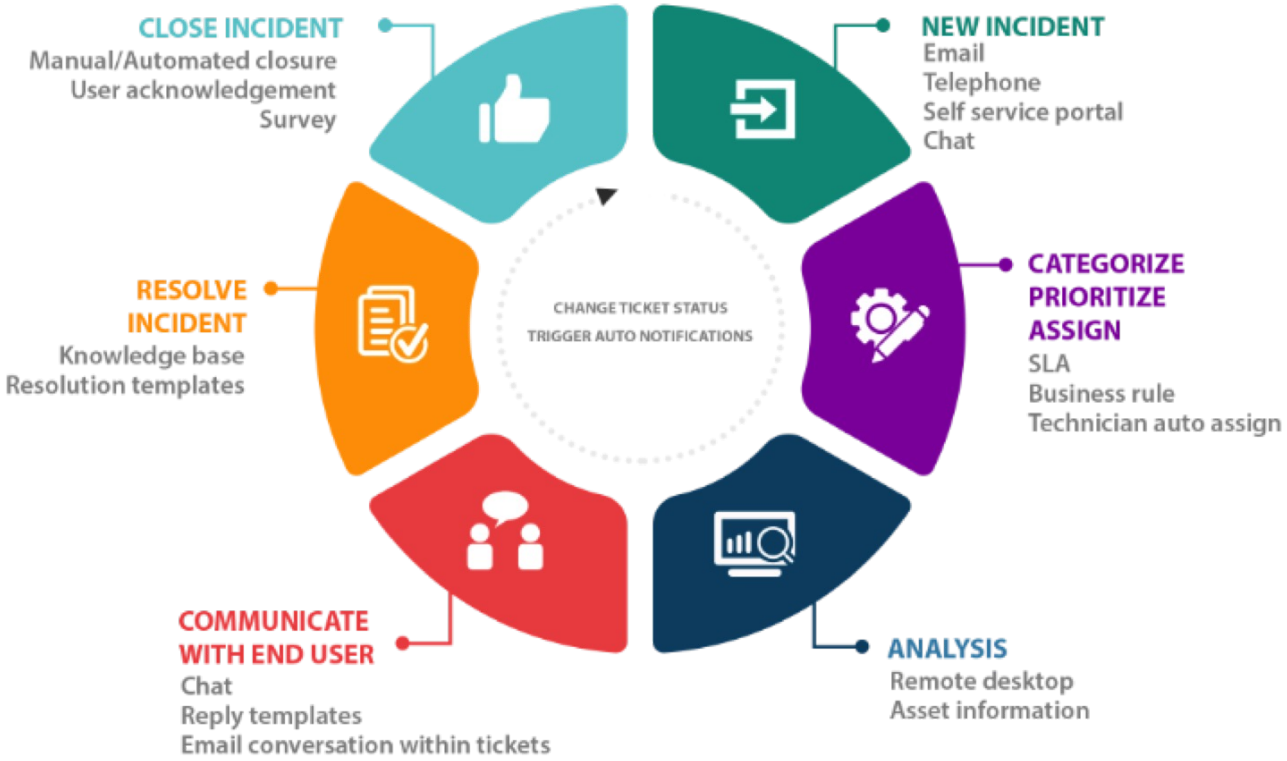
Procedure of a protoypical incident



Source: preparedex.com

IV. Business Continuity & Incident Management

Incident Management



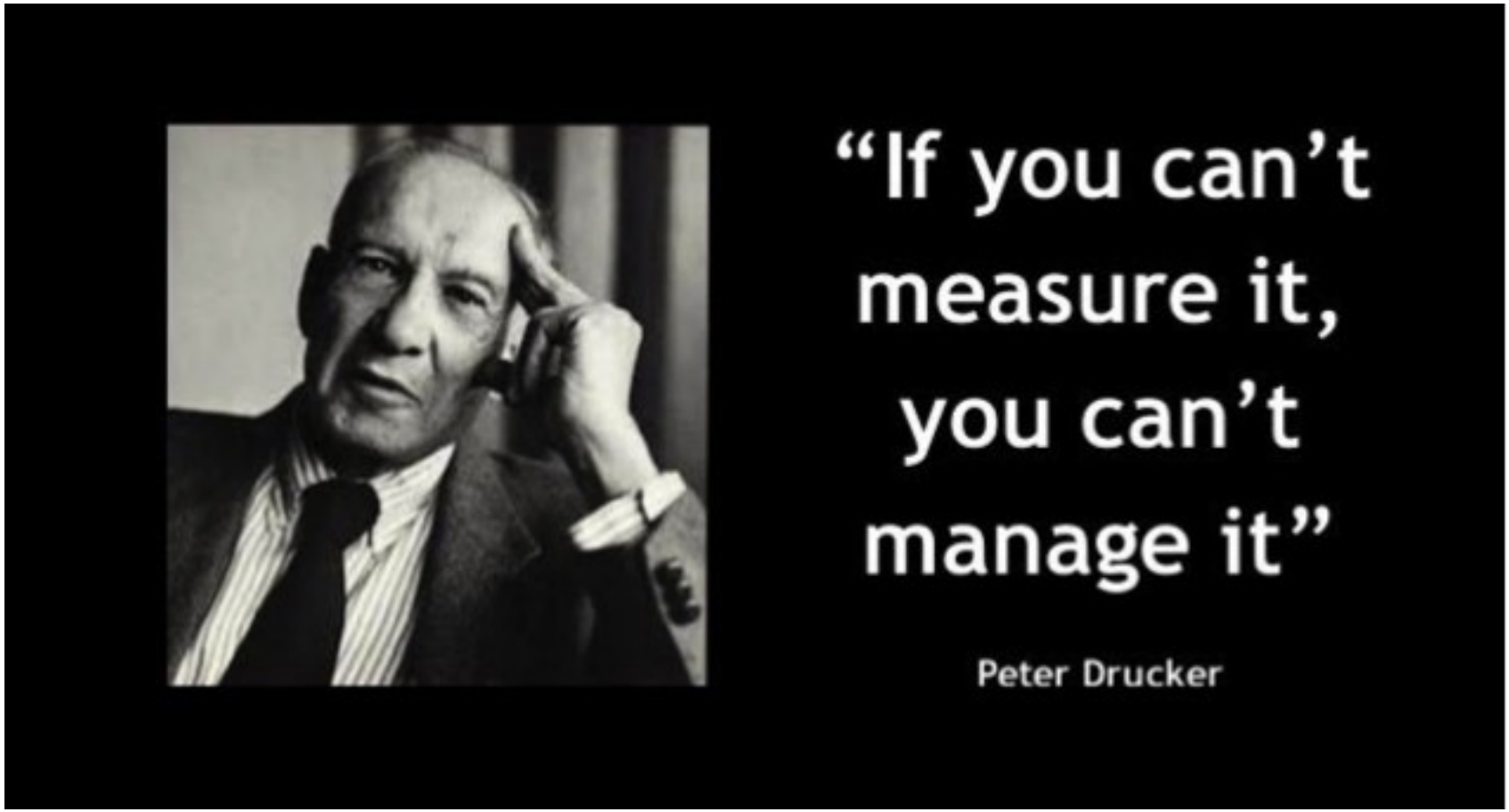
Source: manageengine.com

Agenda

I. Introduction Security Management
II. Information Security Management System
III. Risk Management
IV. Business Continuity & Incident Management
V. Information Security Measurement
VI. Literature

V. Information Security Measurement

Information Security Measurement



Source: busyqueenbee.com

V. Information Security Measurement

Key **P**erformance **I**ndicator (KPI)

Source: adbox24.de

V. Information Security Measurement

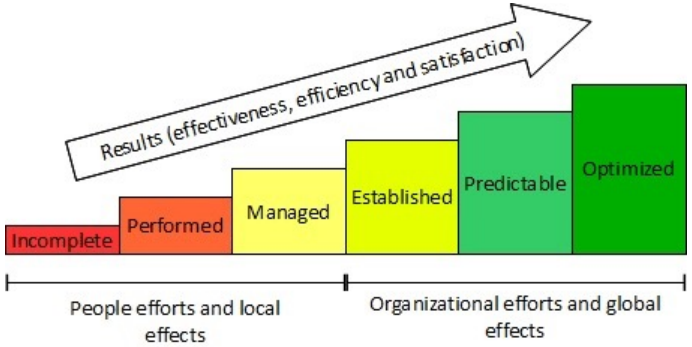
Difference between a metric and an indicator

- A **key performance indicator** is used to measure performance and success.
- A **metric** is nothing more than a number within a KPI that helps track performance and progress.

Source: agencyanalytics.com

V. Information Security Measurement

Maturity model



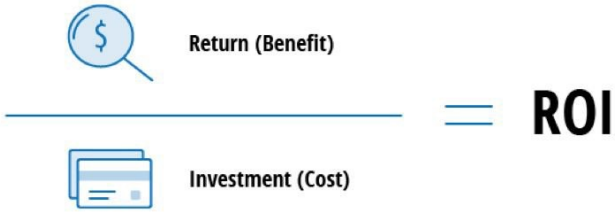
<u>0 – Incomplete:</u> No process implemented or little / no evidence of any systematic achievement of the process purpose
<u>1 – Performed:</u> The process achieves its expected purpose
<u>2 – Managed:</u> The process is implemented in a managed way (planned, monitored, and adjusted) with appropriately established, controlled, and maintained work products
<u>3 – Established:</u> The process is implemented using a defined (standard) process that is capable of achieving the expected outcomes
<u>4 – Predictable:</u> The process operates within defined limits to achieve its expected outcomes
<u>5 – Optimized:</u> The process is continuously improved to meet relevant current and projected enterprise goals

Source: advisera.com

V. Information Security Measurement

Defining ROI and ROSI

Return **O**n **I**nvestment (ROI) is a profitability ratio for a specific investment. It helps you determine whether you should make a purchase or skip it, or how a particular investment has performed to date. The simplest way to calculate ROI is to quantify some kind of "return" or "benefit" and divide it by the "investment" or "cost":



Source: computerweekly.com

V. Information Security Measurement

Defining ROI and ROSI

Return **O**n **S**ecurity **I**nvestment (ROSI) means that by looking at all costs (including those caused by damage from an attack) it can be shown whether and when an investment in information security measures leads to a return on investment or not.

$$\text{ROSI (\%)} = \frac{\text{ALE} * \text{Mitigation Ratio} - \text{Cost of Solution}}{\text{Cost of Solution}}$$

Quantitative Risk Assessment Formula

Annualized **L**oss **E**xpectancy (ALE) =
Single **L**oss **E**xpectancy (SLE) by the **A**nnualized **R**ate of **O**ccurrence (ARO)

$$\text{ALE} = \text{SLE} * \text{ARO}$$

Source: computerweekly.com

Agenda

I. Introduction Security Management
II. Information Security Management System
III. Risk Management
IV. Business Continuity & Incident Management
V. Information Security Measurement
VI. Literature

VI. Literature

- Management of Information Security, M. E. Whitman, H. J. Mattord
- Guide to Disaster Recovery, M. Erbschilde
- Guide to Network Defense and Countermeasures, G. Holden
- Real Digital Forensics: Computer Security and Incident Response, 1/e; Keith J. Jones, Richard Bejtlich, Curtis W. Rose
- Computer Security: Art and Science, Matt Bishop (ISBN: 0-201-44099-7), Addison-Wesley 2003
- Security in Computing, 2nd Edition, Charles P. Pfleeger, Prentice Hall

Chair of Mobile Business & Multilateral Security

Michael Schmid
Goethe University Frankfurt
E-Mail: michael.schmid@m-chair.de
WWW: www.m-chair.de