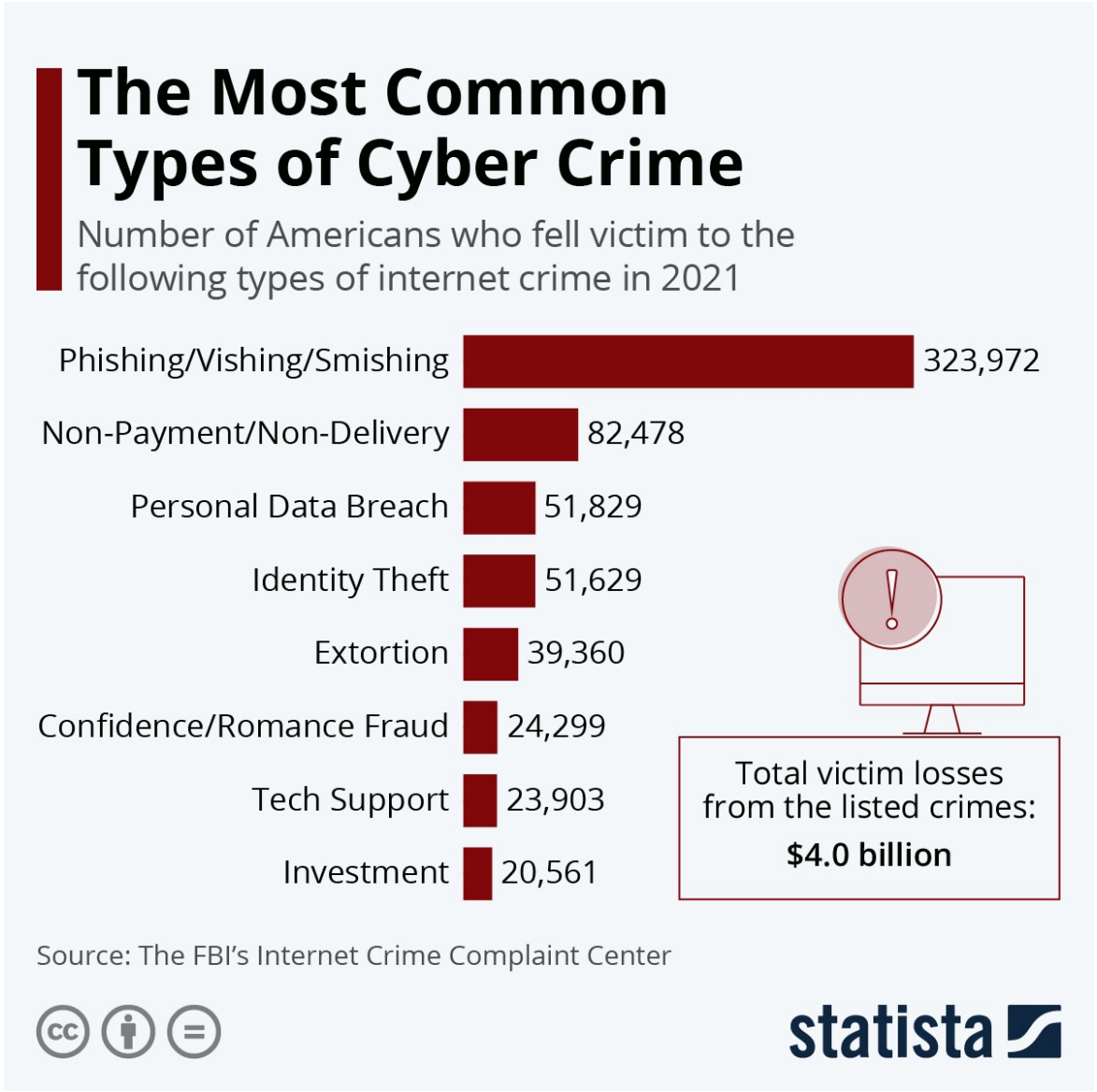
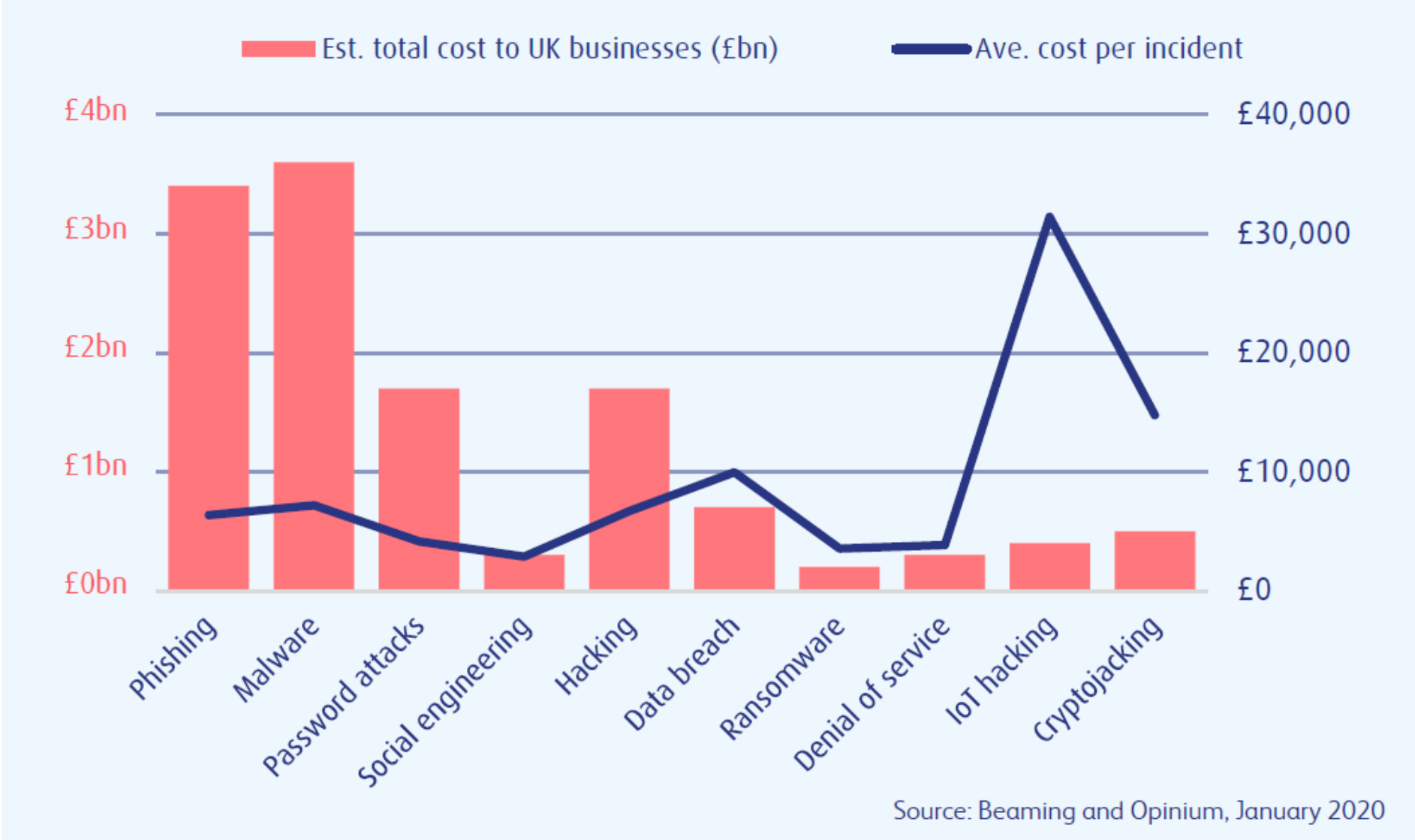
IT RISK

Dr. Muhammad Said Hasibuan


The Most Common Types of Cyber Crime
Number of Americans who fell victim to the following types of internet crime in 2021
Phishing/Vishing/Smishing 323,972
Non-Payment/Non-Delivery 82,478
Personal Data Breach 51,829
Identity Theft 51,629
Extortion 39,360
Confidence/Romance Fraud 24,299
Tech Support 23,903
Investment 20,561
Total victim losses from the listed crimes:
$4.0 billion
Source: The FBI's Internet Crime Complaint Center
statista

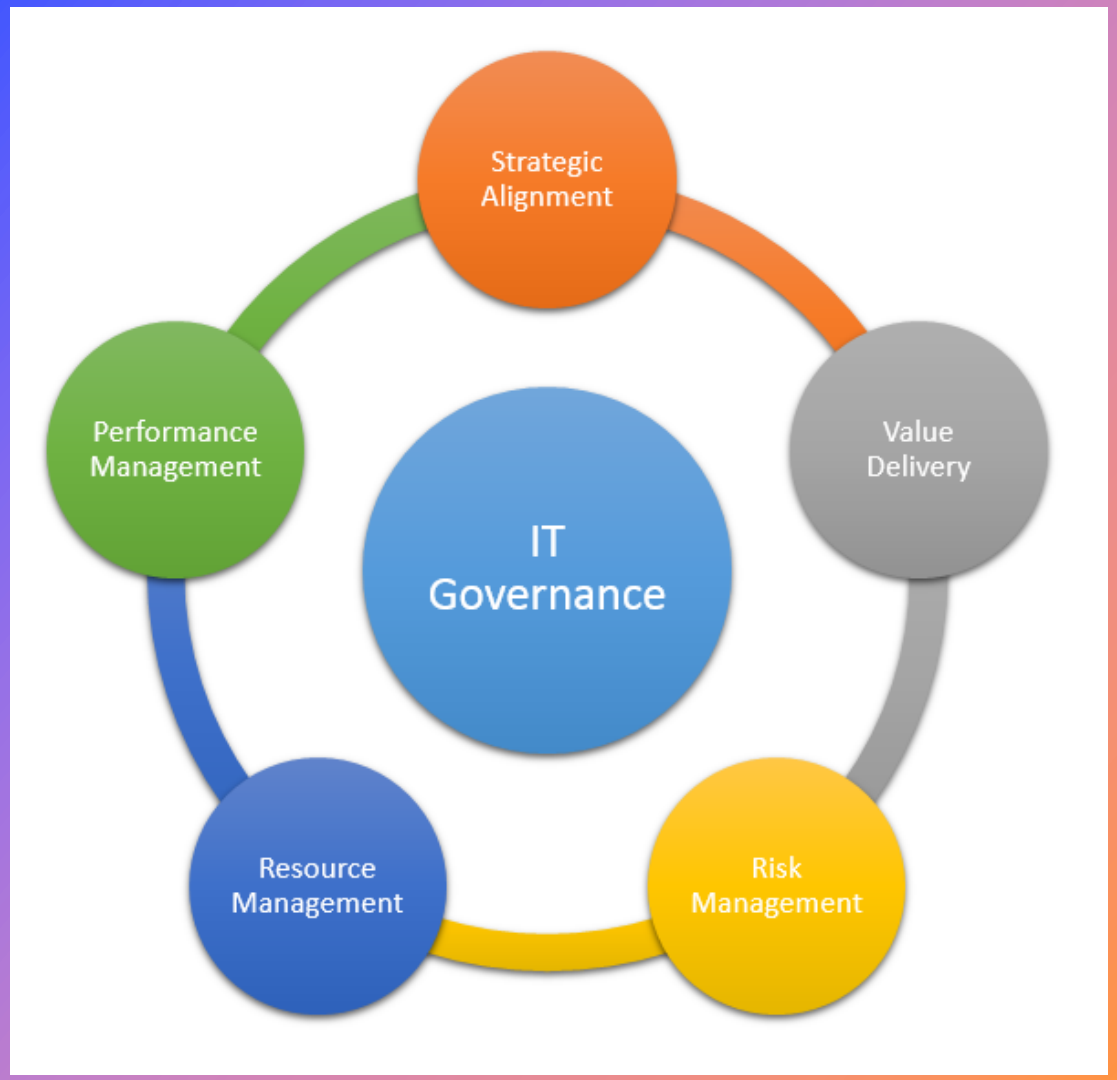

Est. total cost to UK businesses (£bn)
Ave. cost per incident
£4bn
£3bn
£2bn
£1bn
£0bn
£40,000
£30,000
£20,000
£10,000
£0
Phishing
Malware
Password attacks
Social engineering
Hacking
Data breach
Ransomware
Denial of service
IoT hacking
Cryptojacking
Source: Beaming and Opinium, January 2020

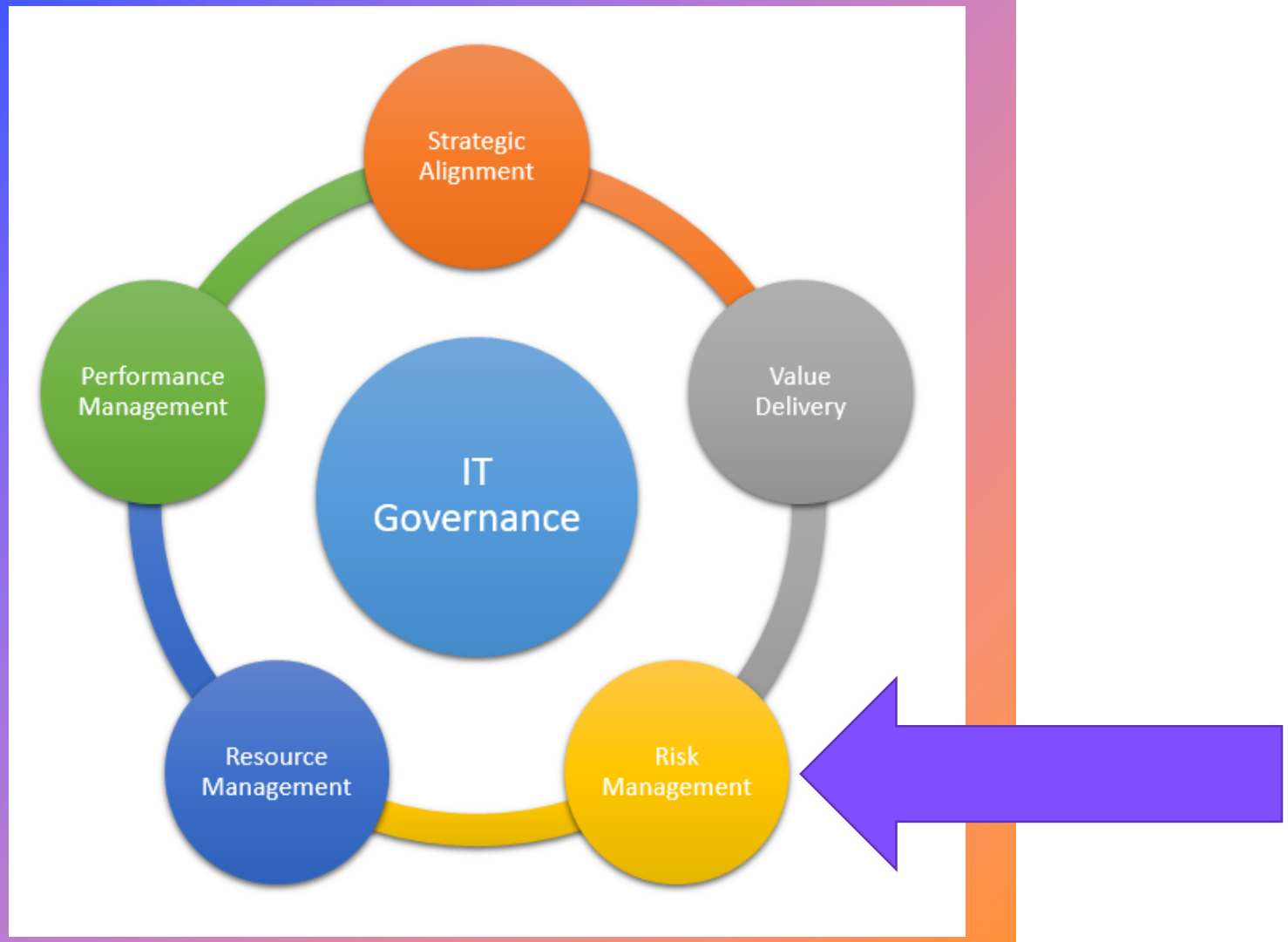
Definition

- Information Security is defined as the set of mechanisms, techniques, measures, and administrative processes employed to protect IT assets from unauthorized access, (mis)appropriation, manipulation, modification, loss, or (mis)use and from unintentional disclosure of data and information embedded in these assets.

Definition

- The Oxford English Dictionary definition of risk is as follows: ‘a chance or possibility of danger, loss, injury or other adverse consequences’ and the definition of at risk is ‘exposed to danger’.
- The Institute of Risk Management (IRM) defines risk as the combination of the probability of an event and its consequence.
- Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations’ missions.


Strategic Alignment
Value Delivery
Risk Management
Resource Management
Performance Management
IT Governance


Strategic Alignment
Value Delivery
Risk Management
Resource Management
Performance Management
IT Governance

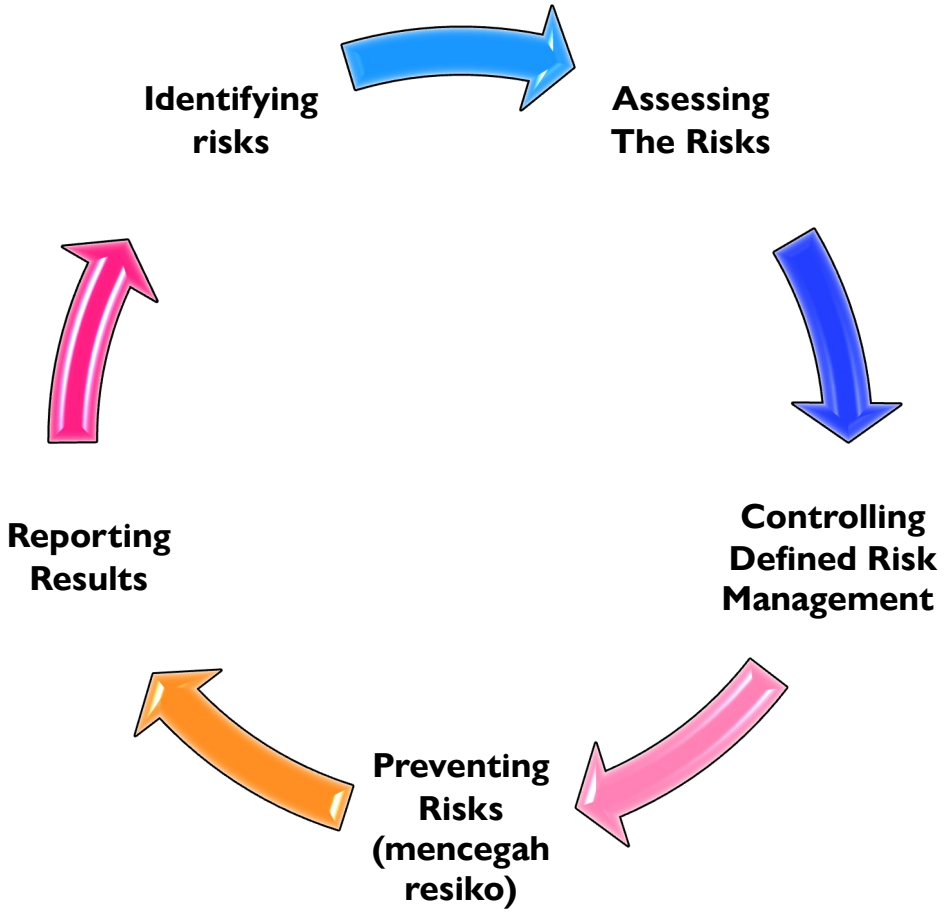
IT Aset

- Desktops PCs and laptops
- Mobile devices and wireless networks (e.g., PDAs, Wi-Fi/Bluetooth devices)
- Application servers, mainframes
- Mail servers
- Web servers Database servers (data warehouses, storage) as well as the entire universe of corporate data, records, memos, reports, etc.
- Network elements (switches, routers, firewalls, appliances, etc.)
- PBXs, IP-PBXs, VRUs, ACDs, voicemail systems, etc.
- Mobility (support) systems (Virtual Private Network nodes, wireless e-mail servers, etc.)

Definition

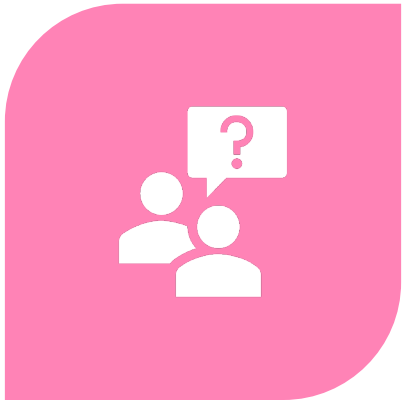
- Perera et al. (2014) defined the management of risks as a systematic approach to the identification, assessment, evaluation, and ranking of the associated risks followed by the allocation of the necessary resources to monitor, control, and minimise any adverse impacts of undesirable events.

IT Risk Management Lifecycle



CATEGORY RISK

HAZARD (OR PURE) RISKS;



CONTROL (OR UNCERTAINTY) RISKS;

OPPORTUNITY (OR SPECULATIVE) RISKS

The Computer Crime and Intellectual Department of Justice defines :

- **Confidentiality.** A breach of confidentiality occurs when a person knowingly accesses a computer without authorization or exceeding authorized access. Confidentiality is compromised when a hacker views or copies proprietary or private information, such as a credit card number or trade secret.
- **Integrity**. A breach of integrity occurs when a system or data has been accidentally or maliciously modified, altered, or destroyed without authorization. For example, viruses and worms alter the source code in order to allow a hacker to gain unauthorized access to a computer system.
- **Availability**. A breach of availability occurs when an authorized user is prevented from timely, reliable access to data or a system. An example of this is a denial of service (DoS) attack.

Confidentiality

Melakukan Klasifikasi Akses:

internal use only (hanya digunakan di lingkungan internal perusahaan),

public (biasanya disebarkan melalui *website* atau media sosial perusahaan), dan

confidential (sangat rahasia, contohnya data-data terkait planning, finansial, business process, dll).

Ancaman aspek *confidentiality*

password strength (lemahnya *password* yang digunakan, sehingga mudah ditebak ataupun di-*bruteforce*).

malware (masuknya virus yang dapat membuat *backdoor* ke sistem ataupun mengumpulkan informasi *pengguna*).

social engineering (lemahnya *security awareness* pengguna dimana mudah sekali untuk 'dibohongi' oleh *attacker*, yang biasanya adalah orang yang sudah dikenalnya).

Bagaimana menjamin Confidentiality

- Enkripsi merupakan sebuah teknik untuk mengubah file/data/informasi dari bentuk yang dapat dimengerti (*plaintext*) menjadi bentuk yang tidak dapat dimengerti (*ciphertext*), sehingga membuat *attacker* sulit untuk mendapatkan informasi yang mereka butuhkan. Enkripsi harus dilakukan pada level media penyimpanan dan transmisi data.

Capaian Integrity

menerapkan ***strong encryption*** pada media penyimpanan dan transmisi data.

menerapkan ***strong authentication*** dan ***validation*** pada setiap akses file/akun login/action yang diterapkan. Authentication dan validation dilakukan untuk menjamin legalitas dari akses yang dilakukan.

menerapkan ***access control*** yang ketat ke sistem, yaitu setiap akun yang ada harus dibatasi hak aksesnya. Misal tidak semua memiliki hak akses untuk mengedit, lainnya hanya bisa melihat saja.

Availability

- Faktor kesengajaan

Faktor kesengajaan bisa dari serangan *Denial of Service* (DoS), *malware*, maupun *hacker/cracker*.

- Faktor *accidental* (kecelakaan).

hardware failure (rusak atau tidak berfungsi dengan baiknya *hardware* tersebut), konsleting listrik, kebakaran, banjir, gempa bumi, dan bencana alam lainya.

Bagaimana memastikan tercapainya aspek *availability*,

disaster recovery plan (memiliki cadangan baik tempat dan *resource*, apabila terjadi bencana pada sistem)

redundant hardware (misal memiliki banyak *power supply*)

RAID (salah satu cara untuk menanggulangi *disk failure*)

data backup (rutin melakukan backup data)

Risk management encompasses three processes

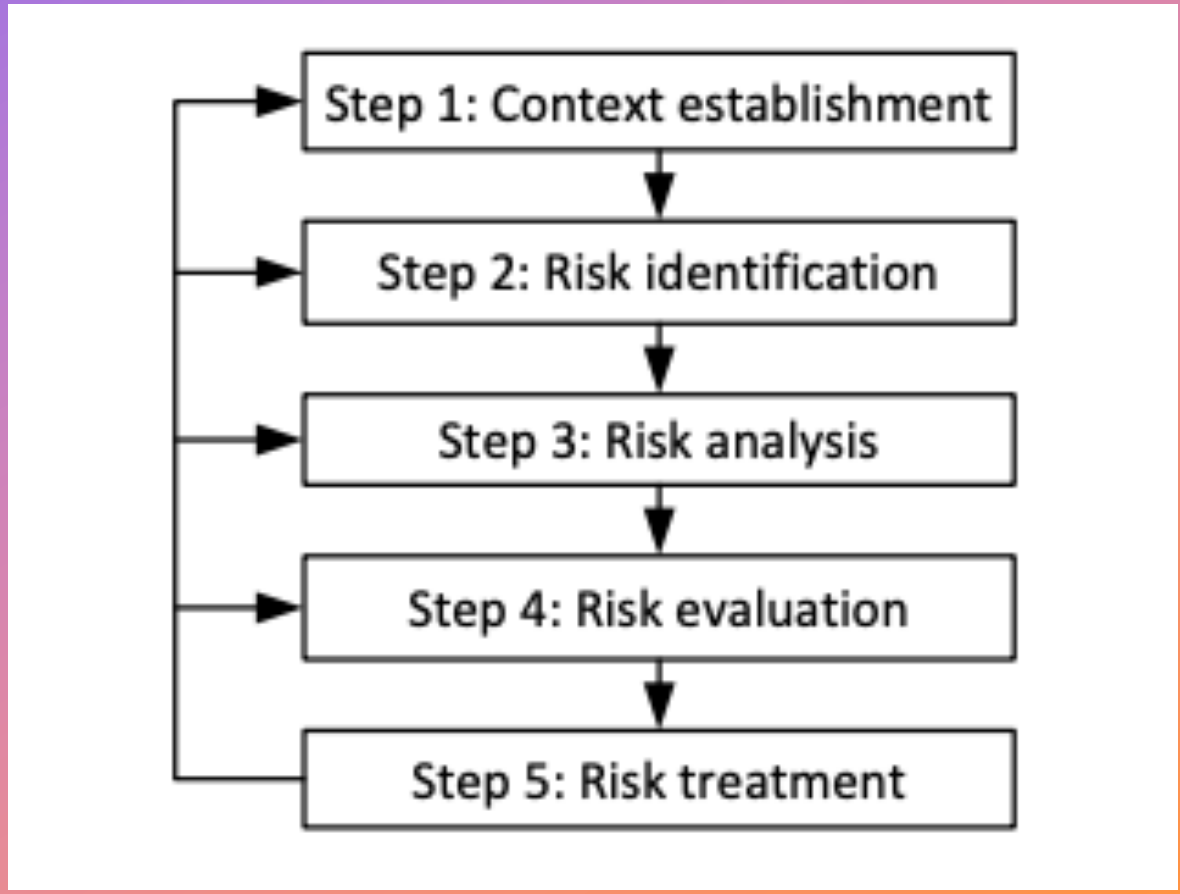
Risk assessment

Penilaian resiko *(risk assessment)* merupakan proses awal di dalam metodologi manajemen resiko. Secara lebih spesifik sejak dikeluarkannya COSO *Internal Control Integrated Framework*, *risk assessment* dengan tegas dianggap sebagai salah satu komponen dari sistem *internal control* (Woods; 2007).

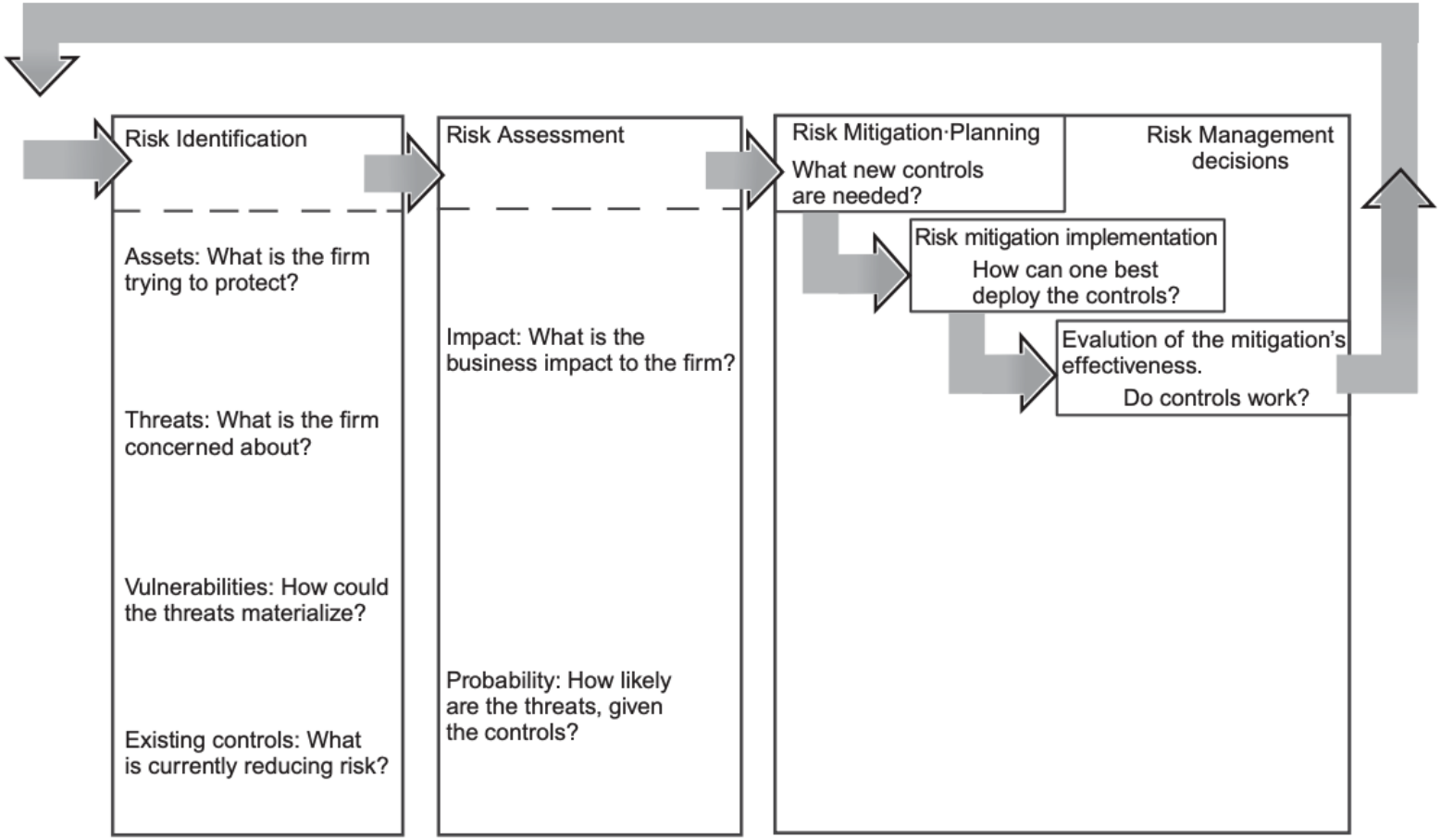
Risk mitigation,

Evaluation and assessment.

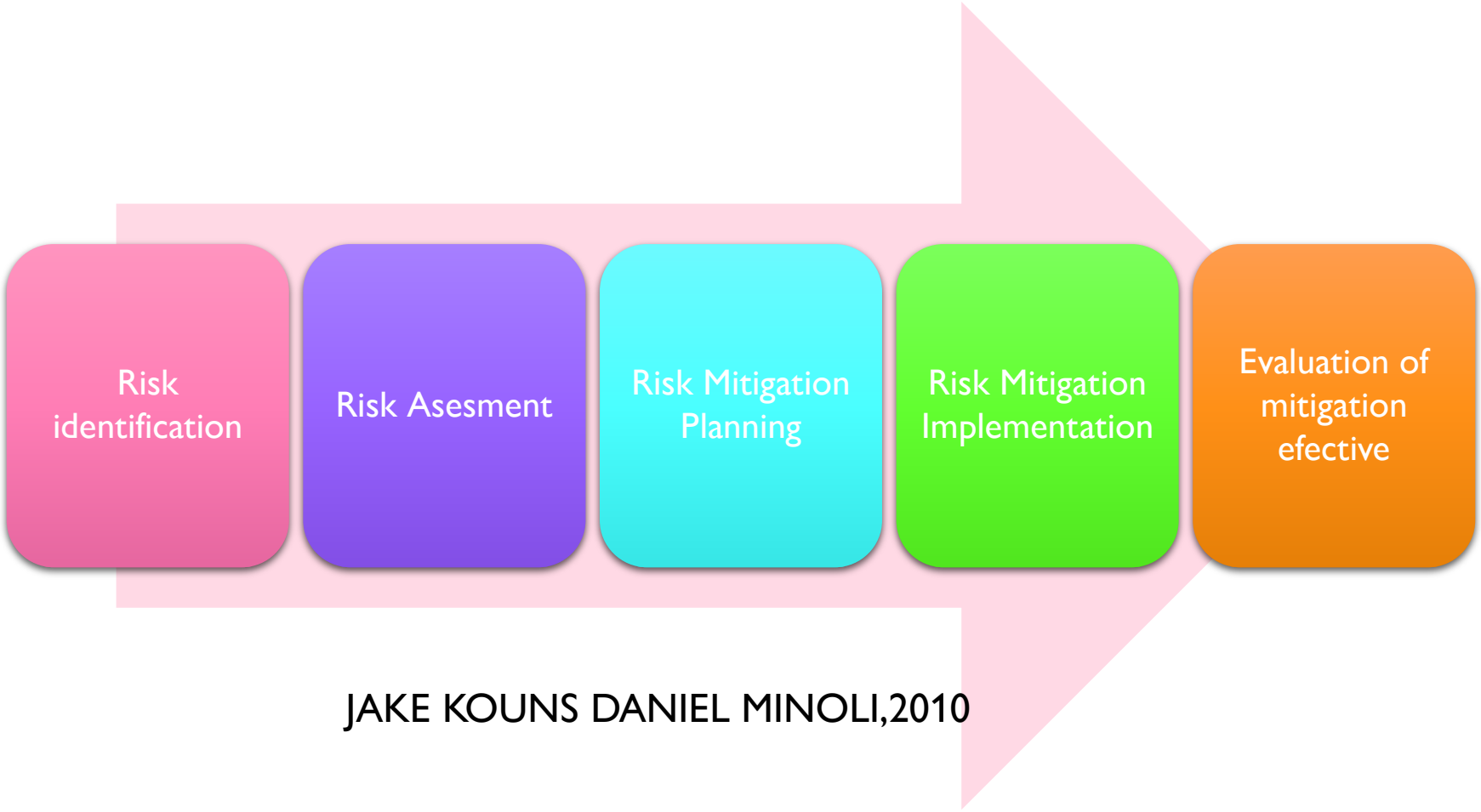
RISK ASESSMENT PROCESS



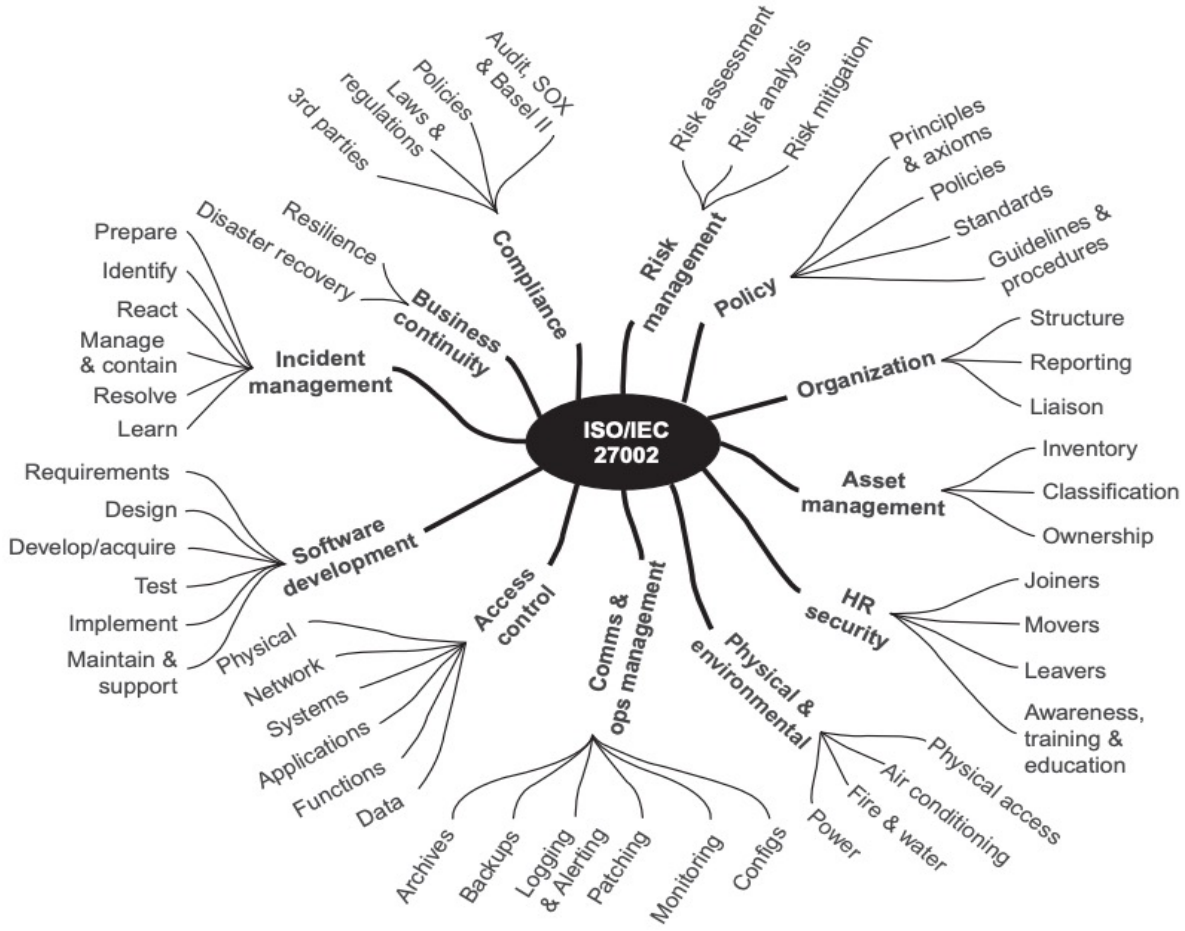
Risk management process as defined in this text.

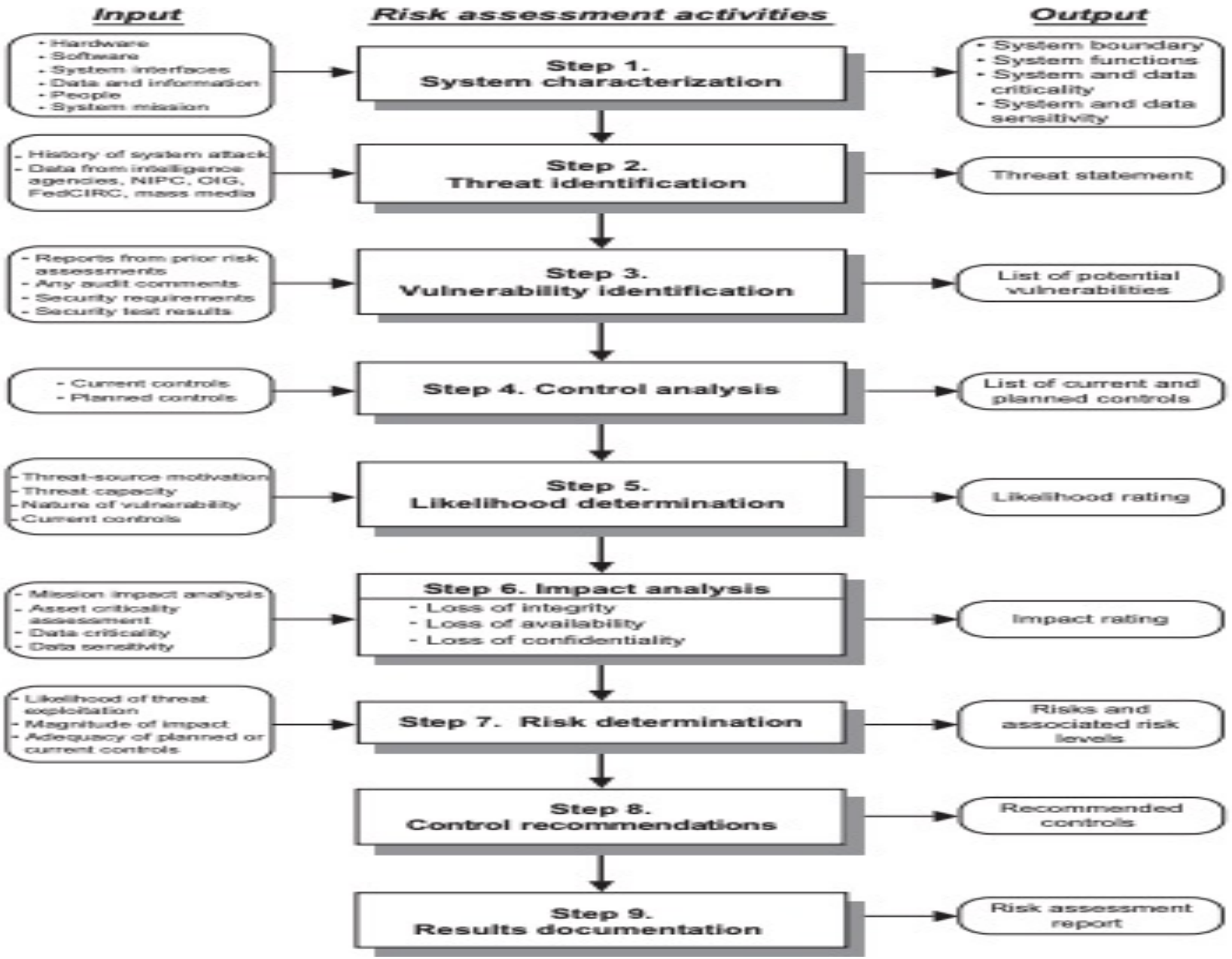


identification of threats



JAKE KOUNS DANIEL MINOLI,2010


ISO/IEC 27002
Compliance
Audit, SOX & Basel II
Policies
Laws & regulations
3rd parties
Risk management
Risk assessment
Risk analysis
Risk mitigation
Policy
Principles & axioms
Policies
Standards
Guidelines & procedures
Organization
Structure
Reporting
Liaison
Asset management
Inventory
Classification
Ownership
HR security
Joiners
Movers
Leavers
Awareness, training & education
Physical & environmental
Physical access
Air conditioning
Fire & water
Power
Comms & ops management
Configs
Monitoring
Patching
Logging & Alerting
Backups
Archives
Access control
Physical
Network
Systems
Applications
Functions
Data
Software development
Requirements
Design
Develop/acquire
Test
Implement
Maintain & support
Incident management
Prepare
Identify
React
Manage & contain
Resolve
Learn
Business continuity
Resilience
Disaster recovery


Input
Risk assessment activities
Output
• Hardware
• Software
• System interfaces
• Data and information
• People
• System mission
Step 1.
System characterization
• System boundary
• System functions
• System and data criticality
• System and data sensitivity
- History of system attack
- Data from intelligence agencies, NIPC, CIG, FedCIRC, mass media
Step 2.
Threat identification
Threat statement
- Reports from prior risk assessments
- Any audit comments
- Security requirements
- Security test results
Step 3.
Vulnerability identification
List of potential vulnerabilities
- Current controls
- Planned controls
Step 4. Control analysis
List of current and planned controls
- Threat-source motivation
- Threat capacity
- Nature of vulnerability
- Current controls
Step 5.
Likelihood determination
Likelihood rating
- Mission impact analysis
- Asset criticality assessment
- Data criticality
- Data sensitivity
Step 6. Impact analysis
- Loss of integrity
- Loss of availability
- Loss of confidentiality
Impact rating
- Likelihood of threat exploitation
- Magnitude of impact
- Adequacy of planned or current controls
Step 7. Risk determination
Risks and associated risk levels
Step 8.
Control recommendations
Recommended controls
Step 9.
Results documentation
Risk assessment report

QUOTE

“He who makes no mistakes makes nothing”

☺ Terima Kasih ☺