KATEDRA ZA
INDUSTRIJSKO
INŽENJERSTVO

Information Security Management System – The Need of the IT Industry

Faculty of Mechanical Engineering
Belgrade, October 26th 2021

Prepared by
Branislav Pribanovic

Branislav Pribanovic

- 2005-2011 Graduated in the Department of Industrial Engineering
- 2011-2018 Serbian Health Insurance Fond
  - Implementation of Integrated Management System
    - *ISO 9001 QMS*
    - *ISO 27001 ISMS*
  - Procurement Sector – Head of Plan and Analysis Department
- 2018-2021 Global Engineering Technologies
  - Document Management Specialist
  - Security Officer
  - Data Protection Officer

Agenda

- ISO 27000 Series
- ISMS
- Implementation of ISO Standards
- ISMS Documentation
- Organization of Information Security (IS)
- HR
- Physical Security
- TOM
- Cyber security
- Security in Development
- Security incident reporting
- Risk assessment
- Business continuity plan
- General Data Protection Regulation

ISO 27000 Series

- 27001:2013 Information Security Management System (ISMS)

- 27701 Privacy Information Management System (PIMS)
- 27017 Information Security for Cloud Services
- 27018 Personally Identifiable Information (PII) in public clouds

SOC

.... stands for ....

Security Operation Center

ISMS

5. Information security documentation

6. Organization of information security

7. Human recources

8. Asset management

9. Acceptable use of assets

10. Cryptography

11. Physical and environmental security

12. Operations security

13. Network controls

14. System acquisition, development and maintenance

15. Supplier relationships

16. Information security incident management

17. Information security aspects of business continuity management

18. Compliance

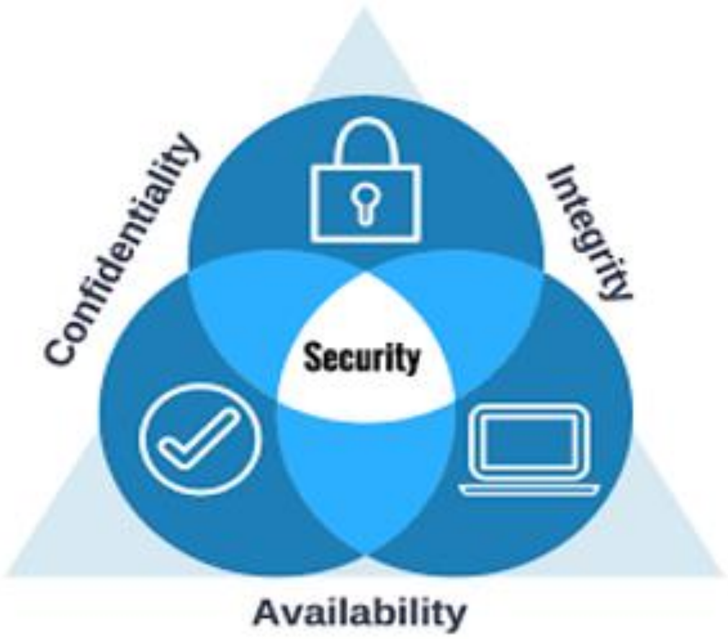
Goals of ISMS

1. Protection of information

2. Minimize Risk

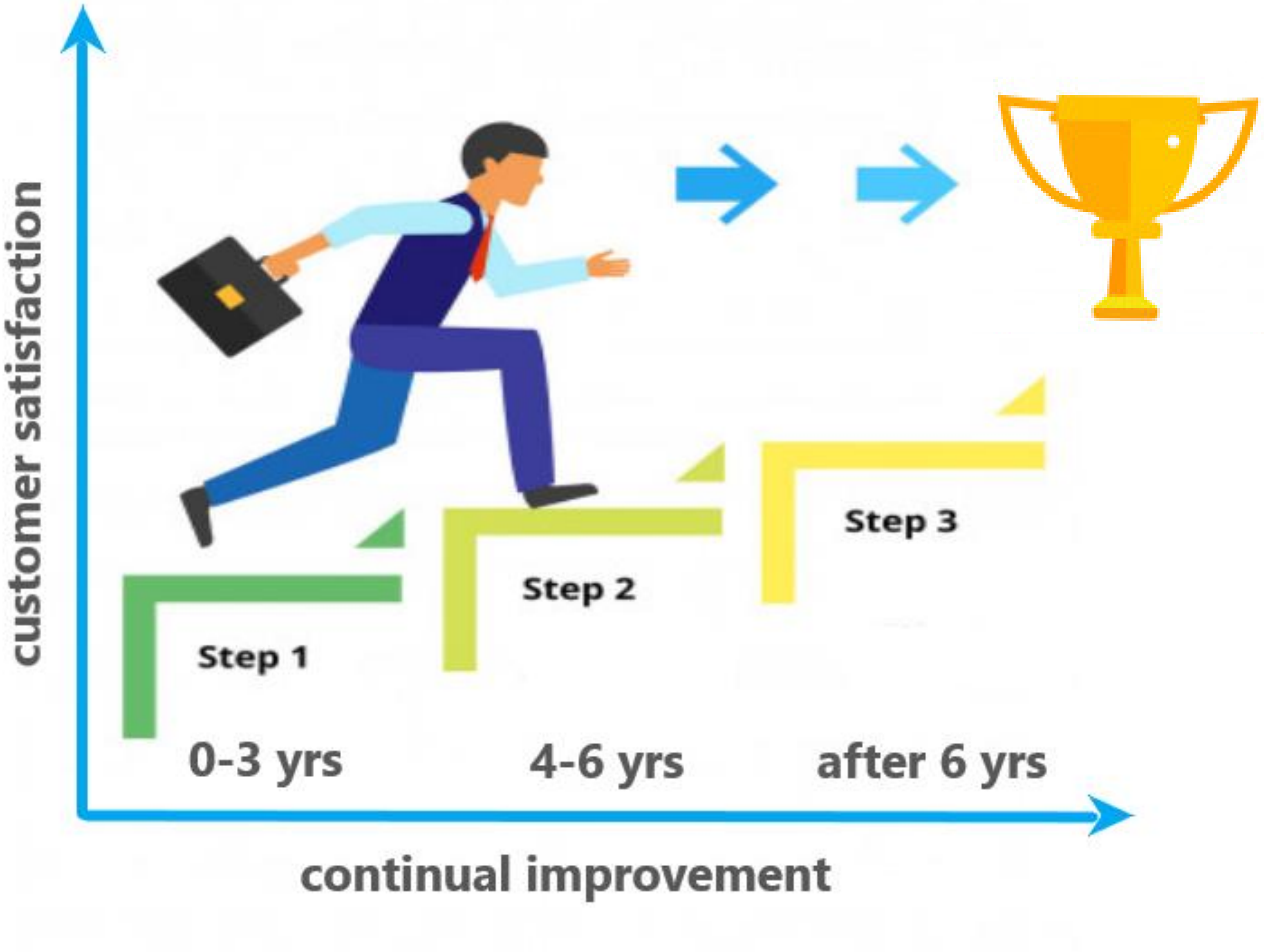
3. Business Continuity

INFORMATION CIA PRINICPLE



- **Confidentiality** - protecting information from being accessed by unauthorized parties.
- **Integrity** - ensuring the authenticity of information—that information is not altered, and that the source of the information is genuine.
- **Availability** - information is accessible by authorized users.

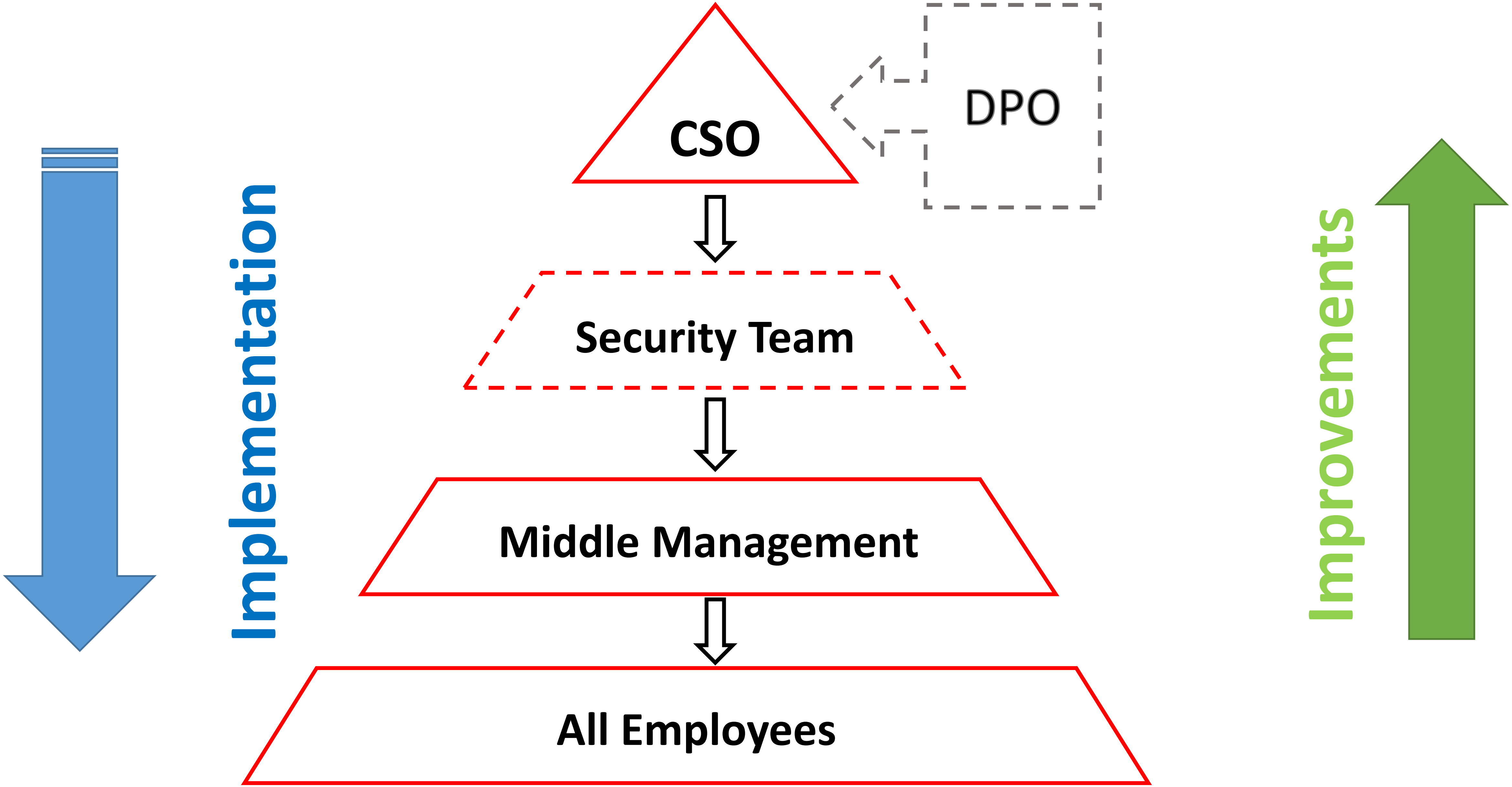
Impementation of ISO Standard - Management System



! Full impemented Management System

!! Regular business process

Organization of information security



CSO

DPO

Security Team

Middle Management

All Employees

Implementation

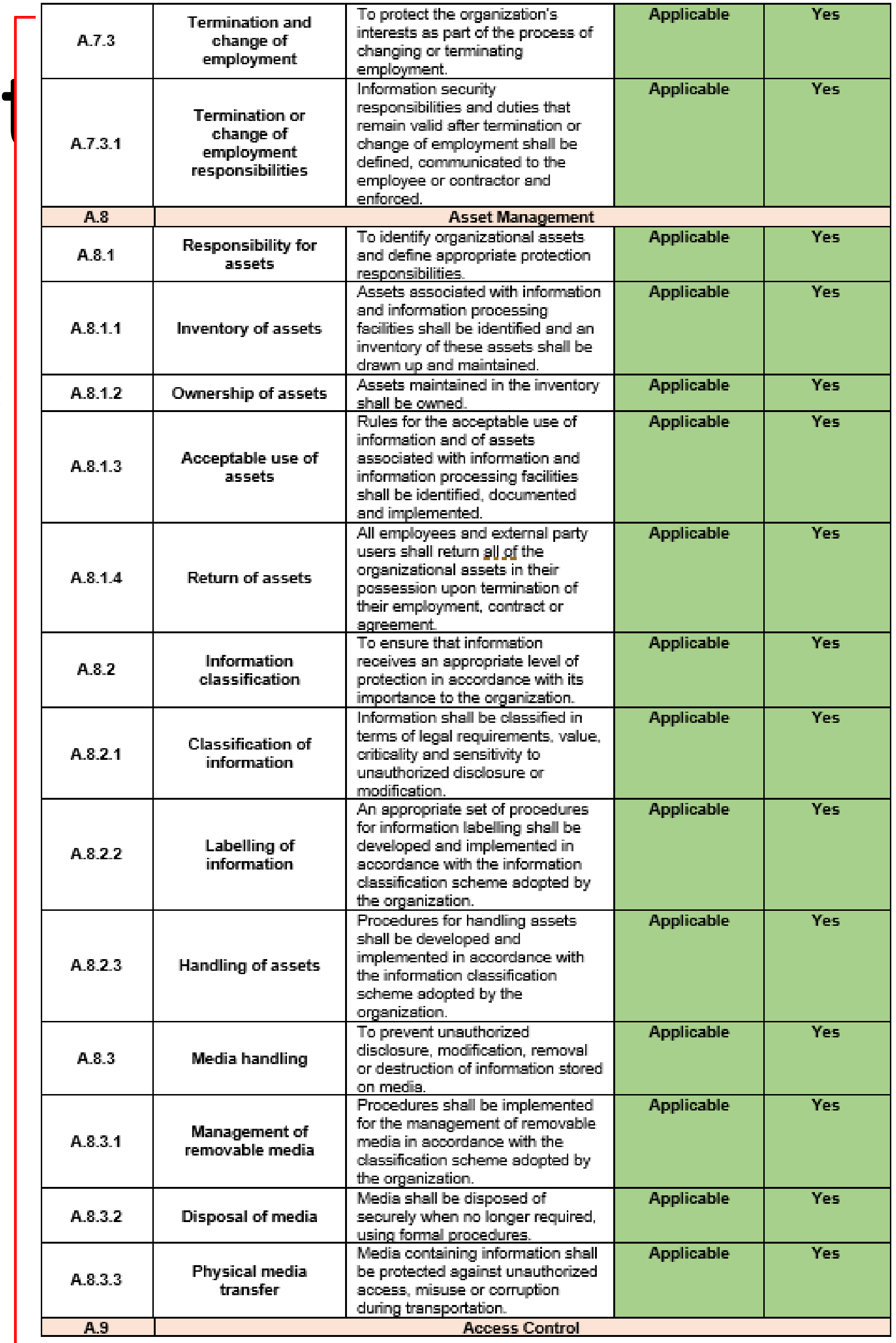
Improvements

Security Officer duties

1. Documentation → Review and Creation
2. Internal Audit → PDCA
3. External Audit → Prepare and Represent
4. Management Review → Reporting
5. Incident Management → Analyse and Measures
6. Risk Asessment → Continual Conducting
7. Security Awareness Training → Plan and Prepare
8. Business continuity → Plan and Test

Information security documentat

- Information Security Policy – Official Document
- Security Policies and Procedures
- Security Handbook / Booklet
- Statement of Aplicability
- Intranet / Security Portal



A.7.3	Termination and change of employment	To protect the organization's interests as part of the process of changing or terminating employment.	Applicable	Yes
A.7.3.1	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	Applicable	Yes
A.8	Asset Management			
A.8.1	Responsibility for assets	To identify organizational assets and define appropriate protection responsibilities.	Applicable	Yes
A.8.1.1	Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	Applicable	Yes
A.8.1.2	Ownership of assets	Assets maintained in the inventory shall be owned.	Applicable	Yes
A.8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	Applicable	Yes
A.8.1.4	Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	Applicable	Yes
A.8.2	Information classification	To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.	Applicable	Yes
A.8.2.1	Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.	Applicable	Yes
A.8.2.2	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Applicable	Yes
A.8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Applicable	Yes
A.8.3	Media handling	To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.	Applicable	Yes
A.8.3.1	Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	Applicable	Yes
A.8.3.2	Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.	Applicable	Yes
A.8.3.3	Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	Applicable	Yes
A.9	Access Control			

MS)

es.
its

e

ation

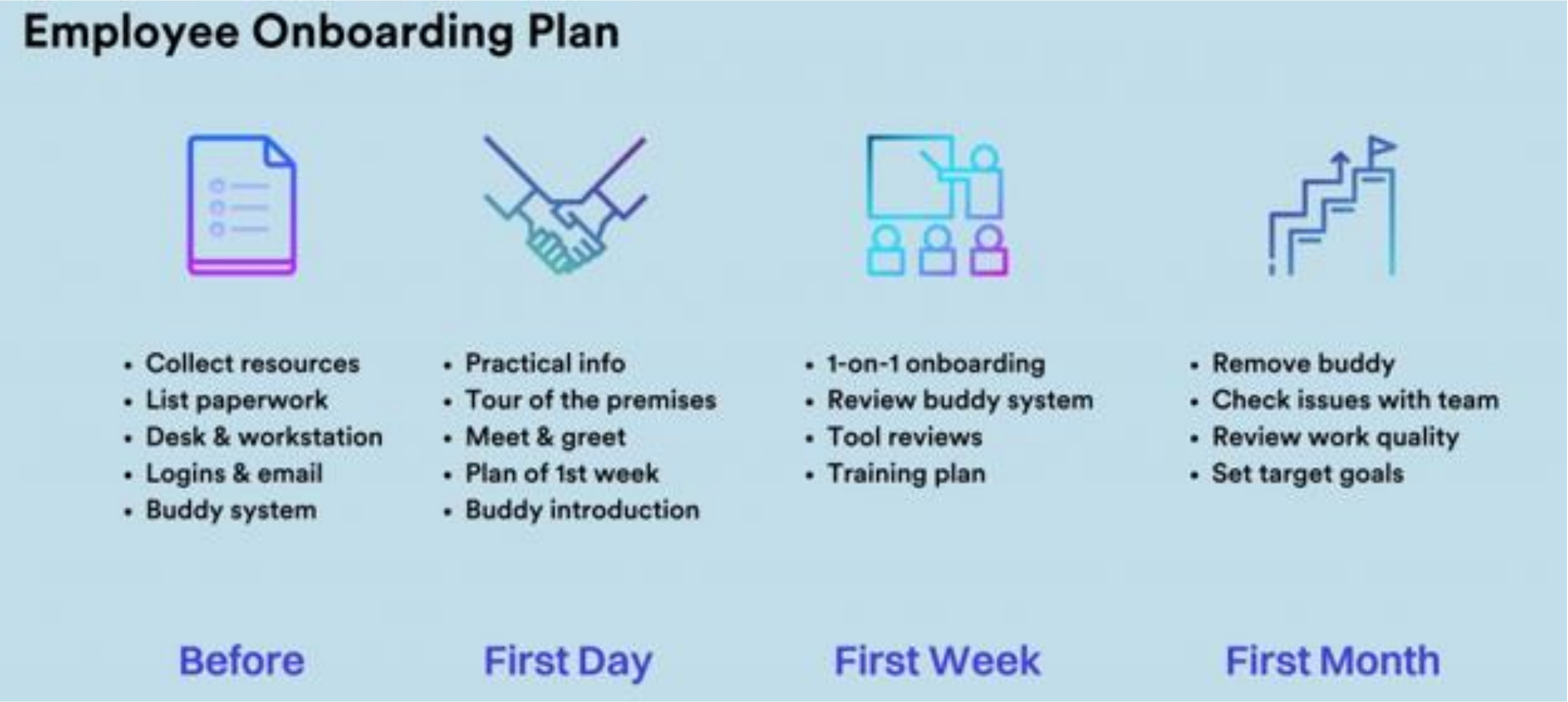
the

is

Human Recources

- Onboarding Process

- Departing Process



Employee Onboarding Plan

Before

- Collect resources
- List paperwork
- Desk & workstation
- Logins & email
- Buddy system

First Day

- Practical info
- Tour of the premises
- Meet & greet
- Plan of 1st week
- Buddy introduction

First Week

- 1-on-1 onboarding
- Review buddy system
- Tool reviews
- Training plan

First Month

- Remove buddy
- Check issues with team
- Review work quality
- Set target goals

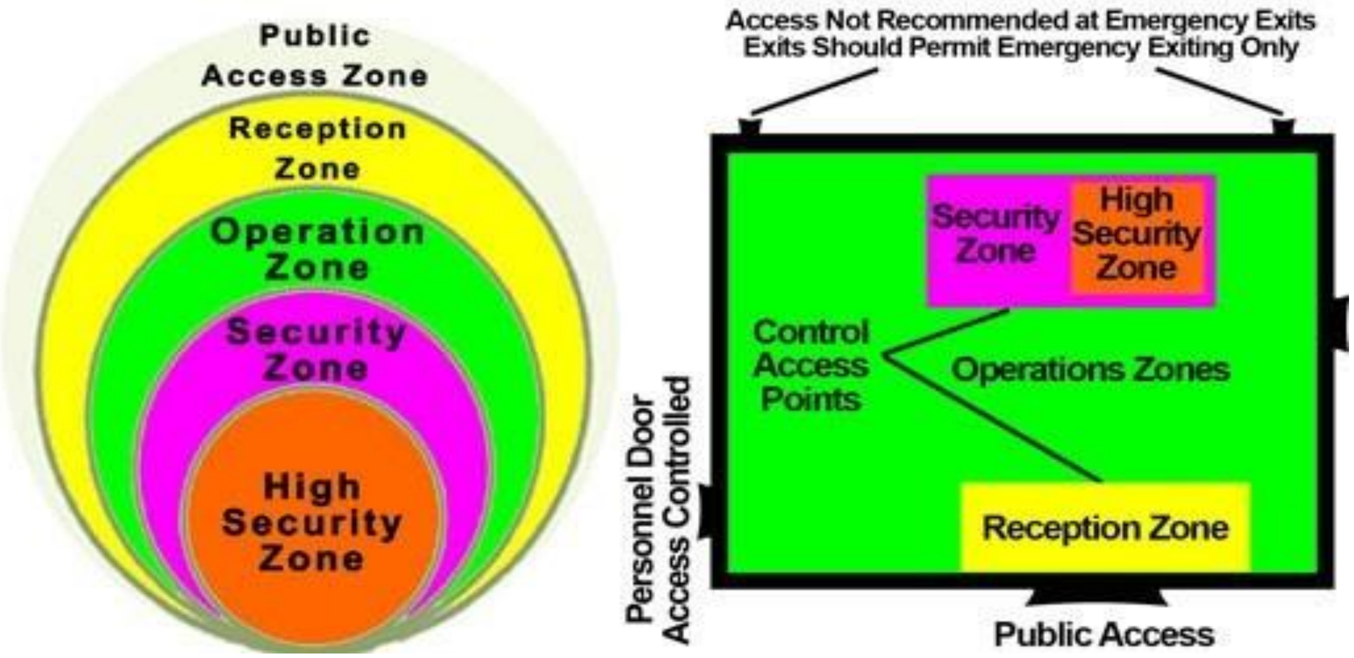
- Security Awerness Training

- Knowledge Testing

Physical and environmental security

- ➢ Limited Access Rights

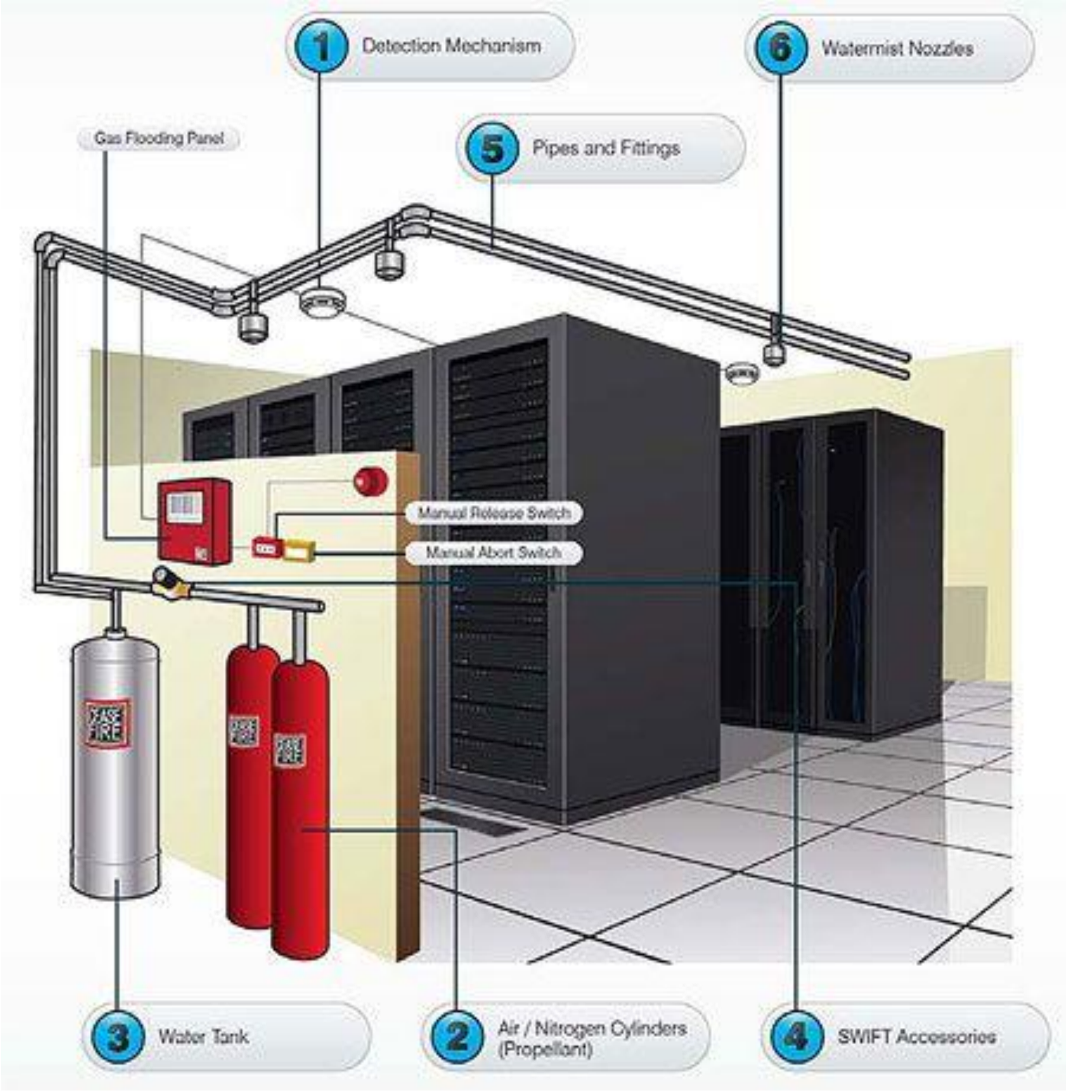
- ➢ Security Zones



Physical and environmental security

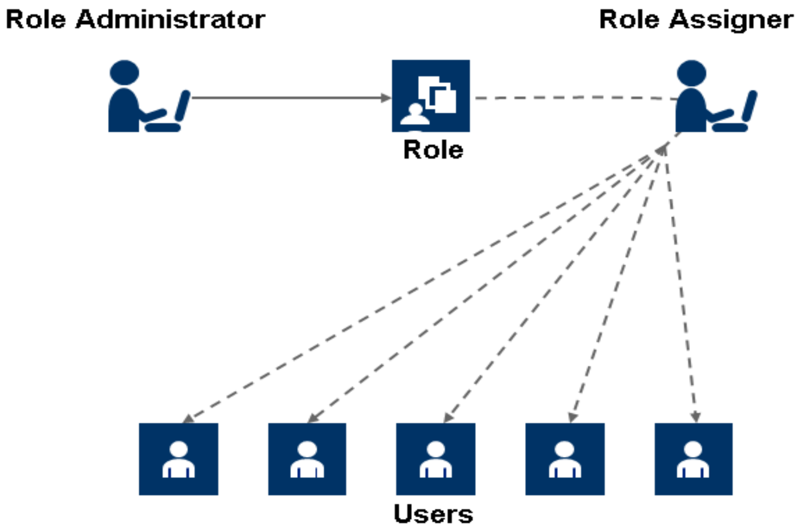
- Alarm systems

- Server Room Protection



Technical and Organisational Measures

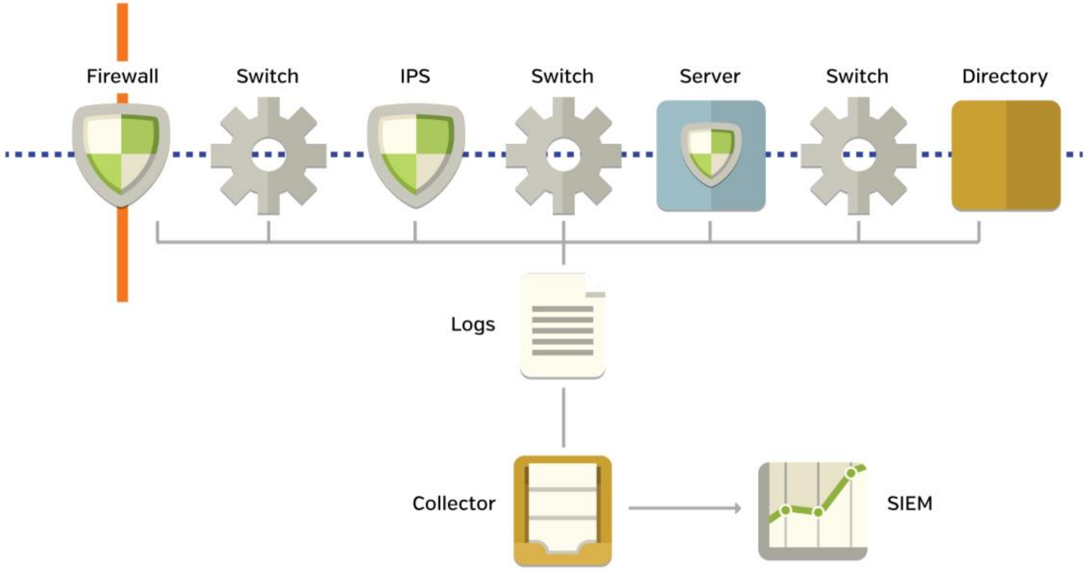
- Segregation of Duties
  - Regular user
  - Adminr user
  - Super-Admin user



- Password and Encryption
  - Strong Password
  - Unique Password
  - Password Safety
  - Expiration Period
  - AES 256 Bit Encryption

Technical and Organisational Measures

- Network Infrastructure
  - Next Generation Firewall
  - Network Segregation
  - Servers and Databases
  - Link and Backup
  - **V**irtual **P**rivate **N**etwork (VPN)



Data centre monitoring visualized by @marknca

- Monitoring and reporting
  - Logs Monitoring
  - Network Monitoring
  - Server Monitoring

Cyber Security

EVERY DAY

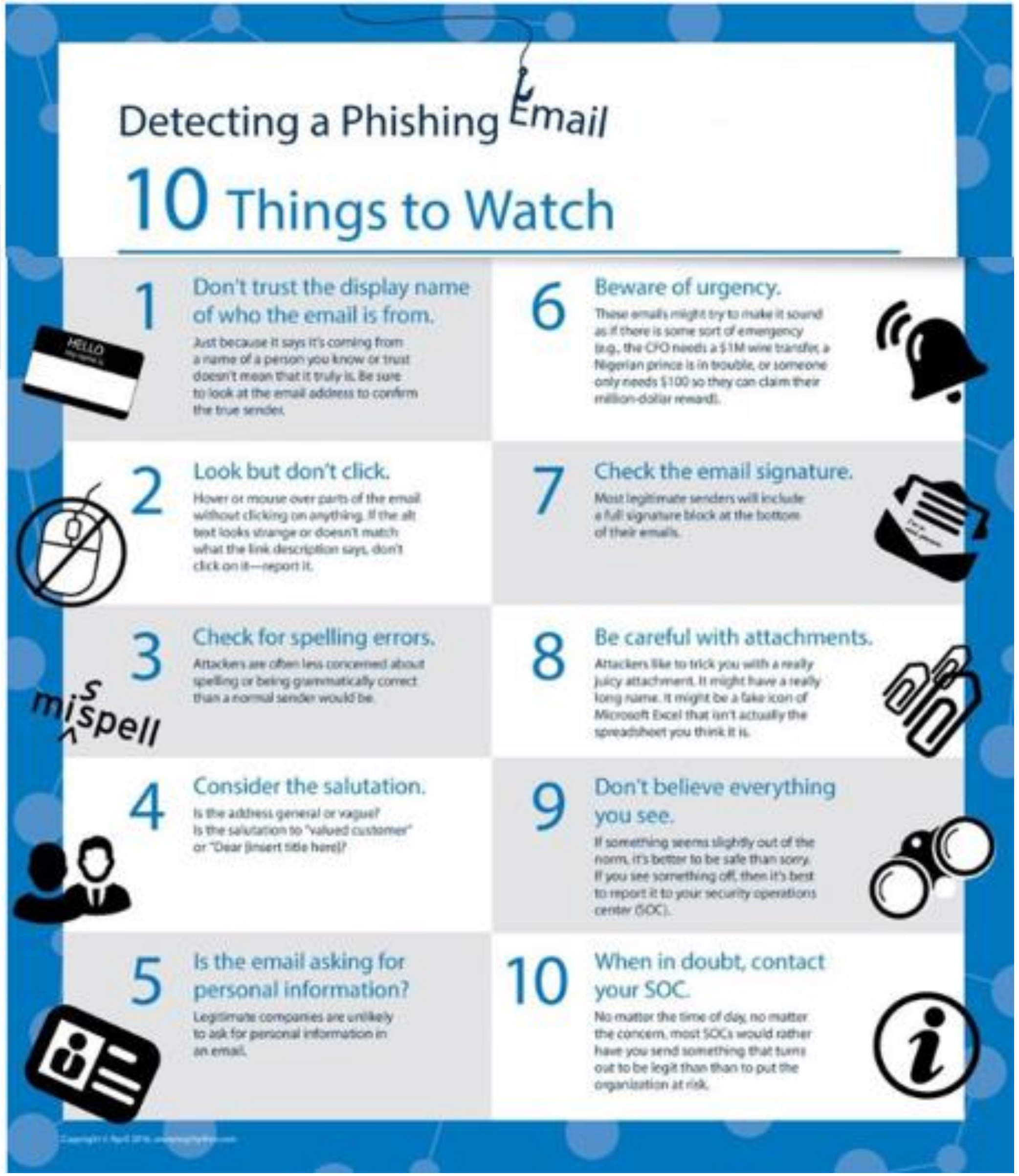
156 MILLION
Phishing emails are sent

16 MILLION
make it through Spam filters

8 MILLION
are opened

800,000 links
are clicked

80,000 people fall for a scam
and share their personal info


HELLO
mispell
s

Detecting a Phishing Email

10 Things to Watch

1 **Don't trust the display name of who the email is from.** Just because it says it's coming from a name of a person you know or trust doesn't mean that it truly is. Be sure to look at the email address to confirm the true sender.

2 **Look but don't click.** Hover or mouse over parts of the email without clicking on anything. If the alt text looks strange or doesn't match what the link description says, don't click on it—report it.

3 **Check for spelling errors.** Attackers are often less concerned about spelling or being grammatically correct than a normal sender would be.

4 **Consider the salutation.** Is the address general or vague? Is the salutation to "valued customer" or "Dear (insert title here)?

5 **Is the email asking for personal information?** Legitimate companies are unlikely to ask for personal information in an email.

6 **Beware of urgency.** These emails might try to make it sound as if there is some sort of emergency (e.g., the CFO needs a $1M wire transfer, a Nigerian prince is in trouble, or someone only needs $100 so they can claim their million-dollar reward).

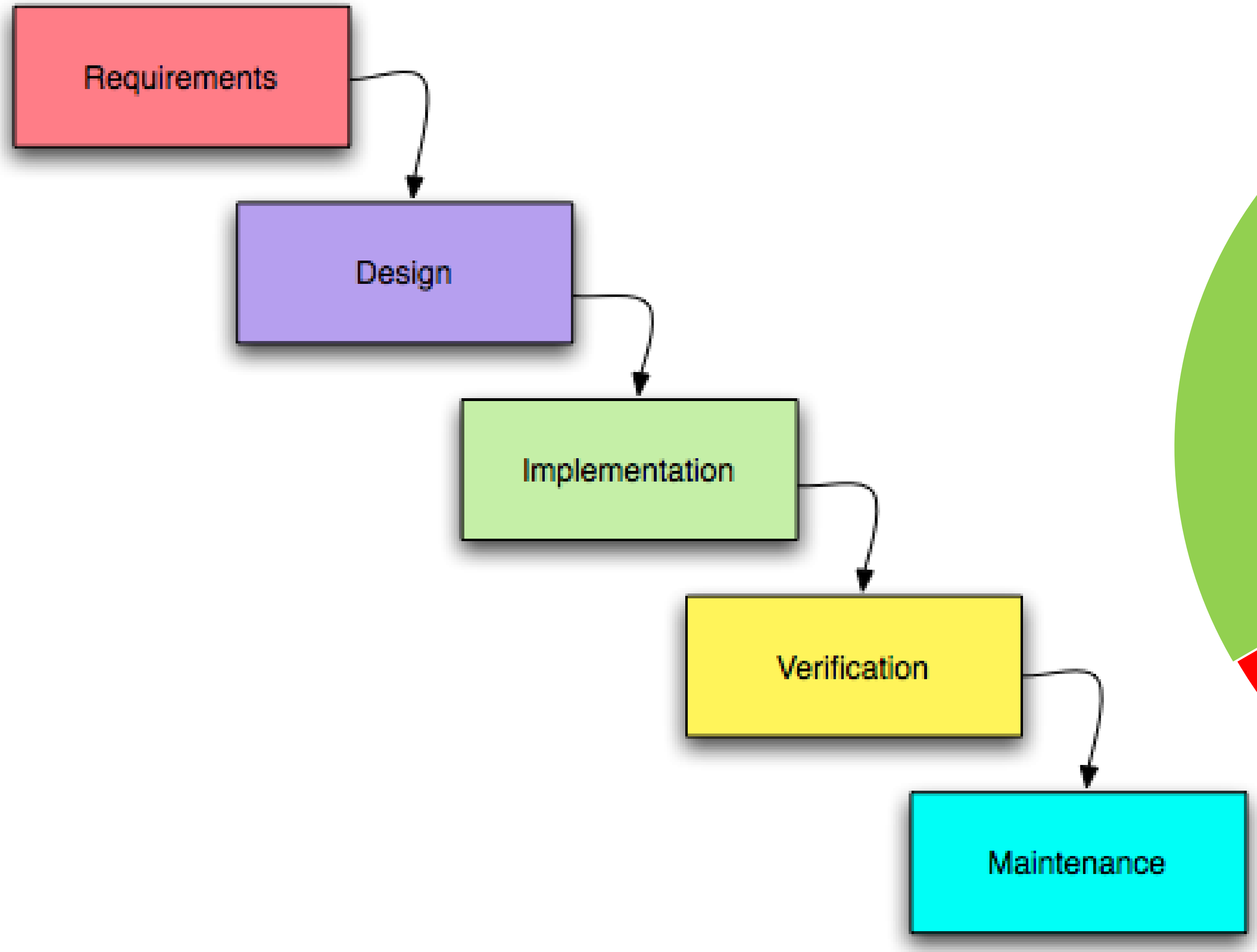
7 **Check the email signature.** Most legitimate senders will include a full signature block at the bottom of their emails.

8 **Be careful with attachments.** Attackers like to trick you with a really juicy attachment. It might have a really long name. It might be a fake icon of Microsoft Excel that isn't actually the spreadsheet you think it is.

9 **Don't believe everything you see.** If something seems slightly out of the norm, it's better to be safe than sorry. If you see something off, then it's best to report it to your security operations center (SOC).

10 **When in doubt, contact your SOC.** No matter the time of day, no matter the concern, most SOCs would rather have you send something that turns out to be legit than than to put the organization at risk.

Security in Development

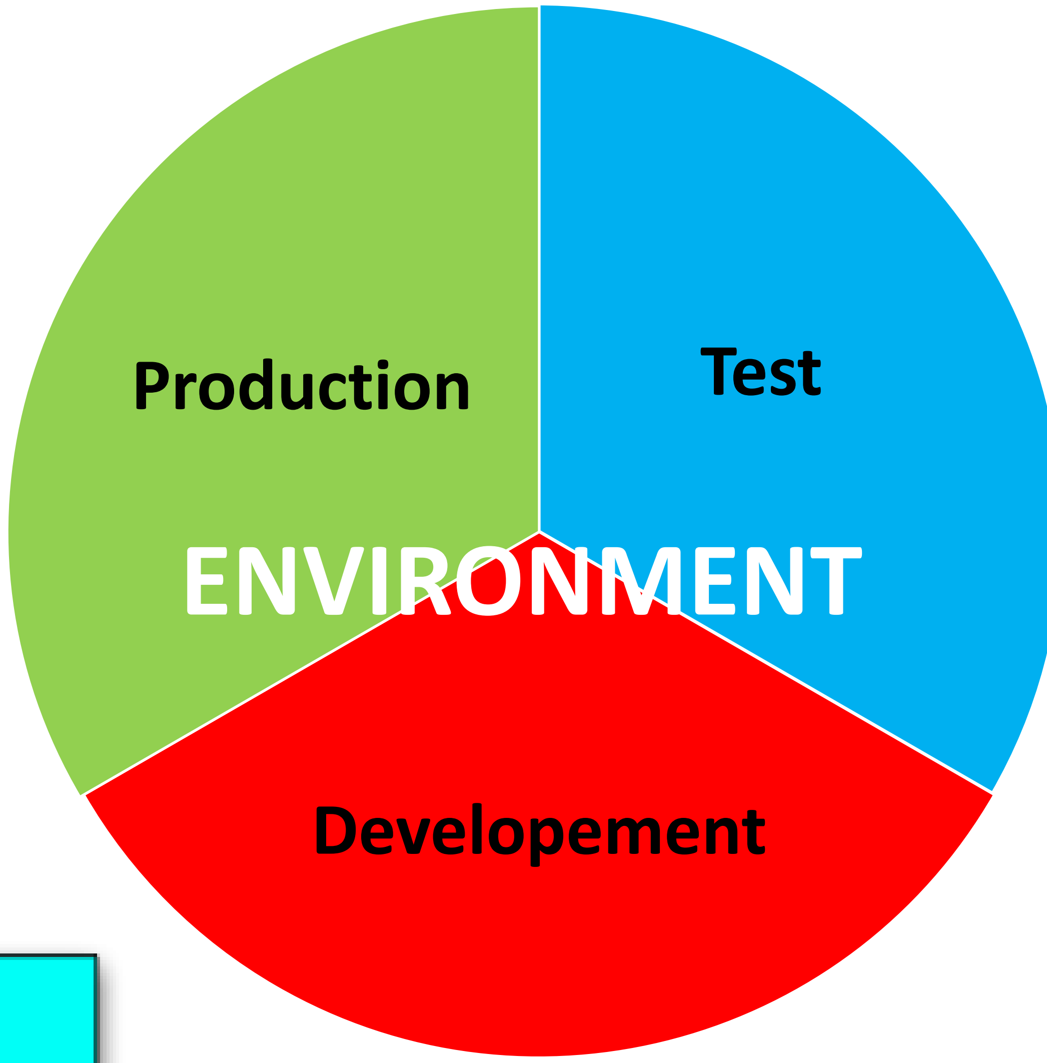

Requirements

Design

Implementation

Verification

Maintenance


Production

Test

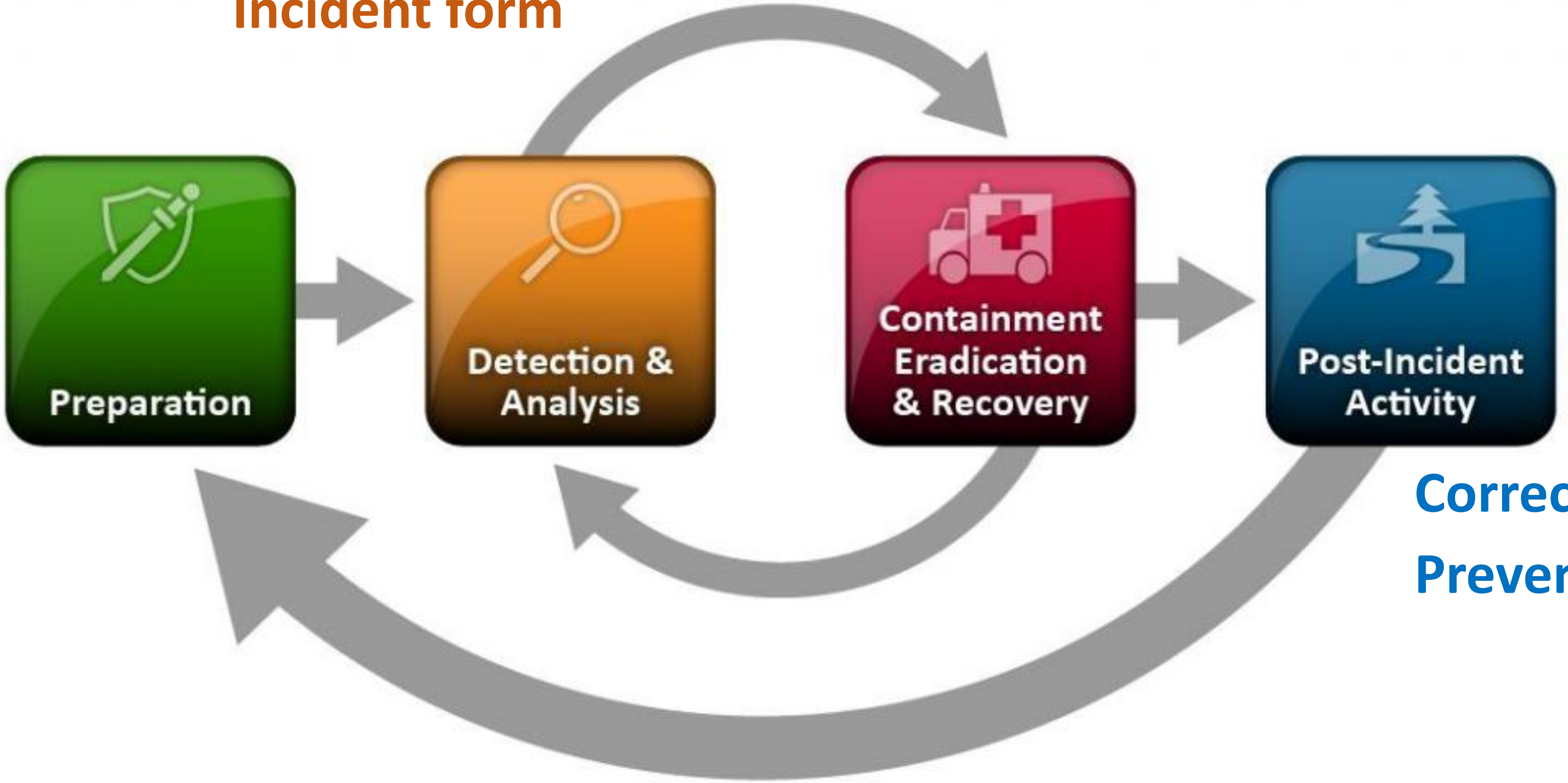
ENVIRONMENT

Developement

Security Incident Reporting

Incident form

Awareness

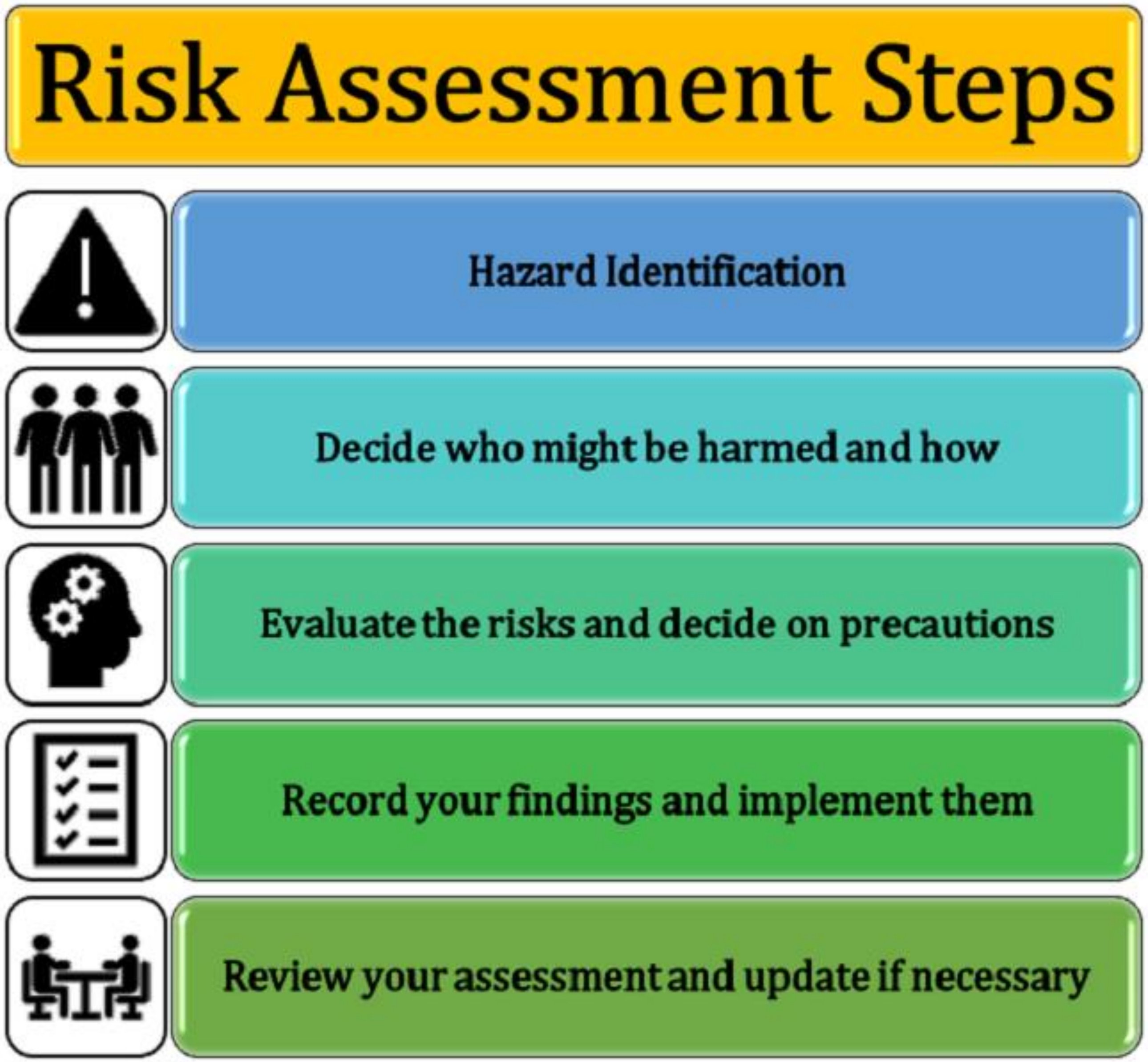


Corrective Measures

Preventive Measures

Security Incident Report

Risk Assessment



Risk Assessment Steps

- Hazard Identification
- Decide who might be harmed and how
- Evaluate the risks and decide on precautions
- Record your findings and implement them
- Review your assessment and update if necessary

Probability

A - Almost Certain (once a month)

B - Likely (quarterly)

C - Possible (several times a year)

D - Unlikely (once a year)

E - Rare (once in a few years)

Impact

1 – Insignificant

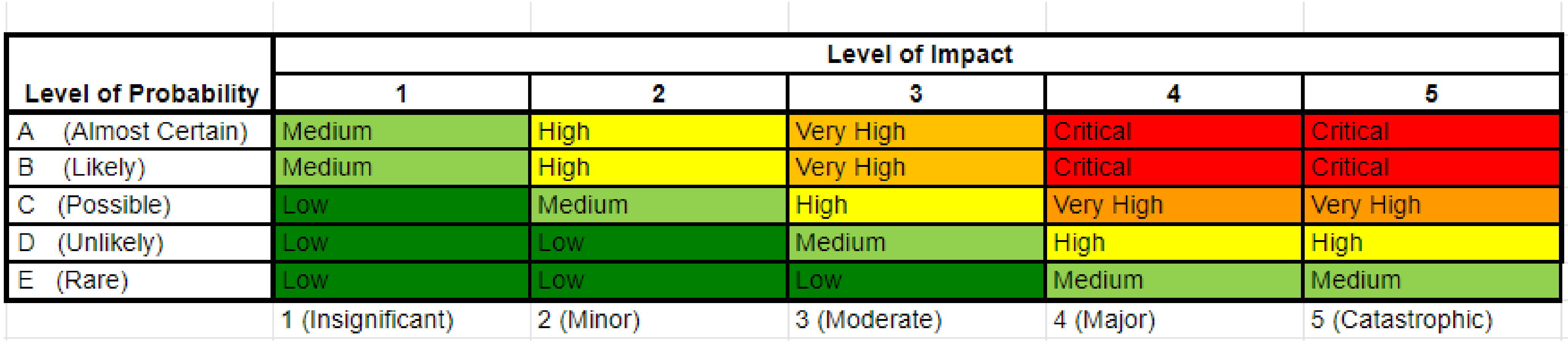
2 – Minor

3 – Moderate

4 – Major

5 – Catastrophic

Risk Assessment



Level of Probability	Level of Impact				
	1	2	3	4	5
A (Almost Certain)	Medium	High	Very High	Critical	Critical
B (Likely)	Medium	High	Very High	Critical	Critical
C (Possible)	Low	Medium	High	Very High	Very High
D (Unlikely)	Low	Low	Medium	High	High
E (Rare)	Low	Low	Low	Medium	Medium
	1 (Insignificant)	2 (Minor)	3 (Moderate)	4 (Major)	5 (Catastrophic)

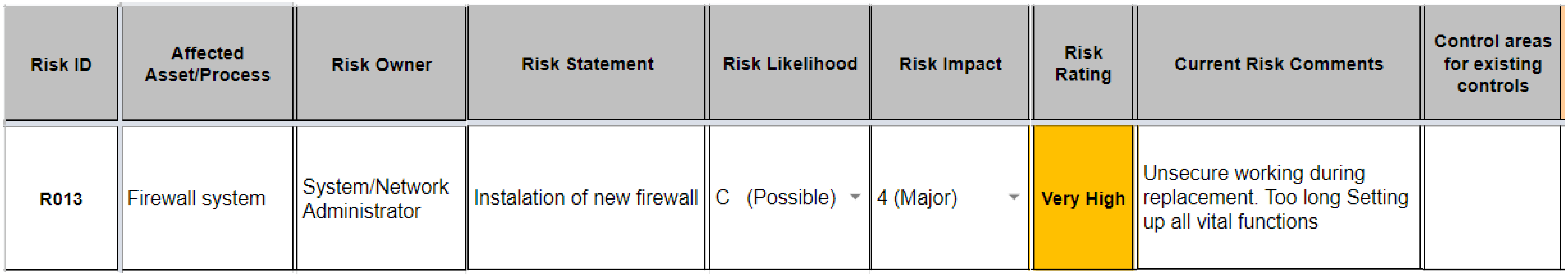
- Low
- Medium

Acceptable risk value

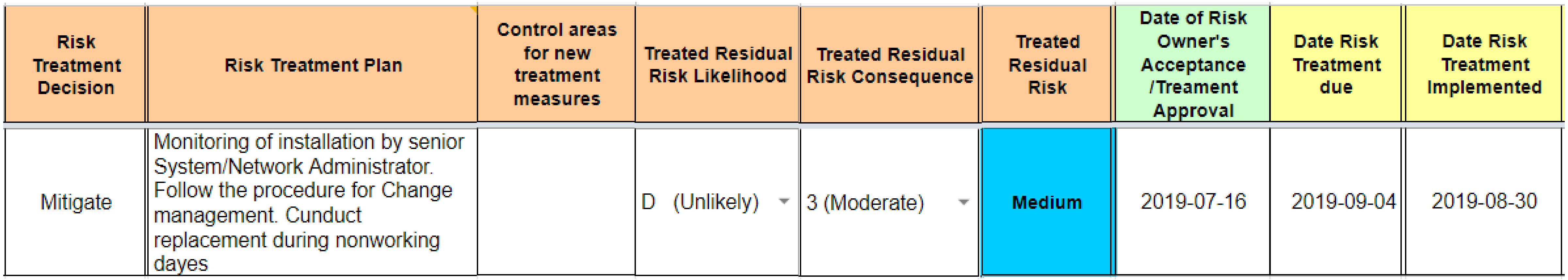
- High
- Very High
- Critical

Need to be managed

Risk Assessment



Risk ID	Affected Asset/Process	Risk Owner	Risk Statement	Risk Likelihood	Risk Impact	Risk Rating	Current Risk Comments	Control areas for existing controls
R013	Firewall system	System/Network Administrator	Instalation of new firewall	C (Possible)	4 (Major)	**Very High**	Unsecure working during replacement. Too long Setting up all vital functions	



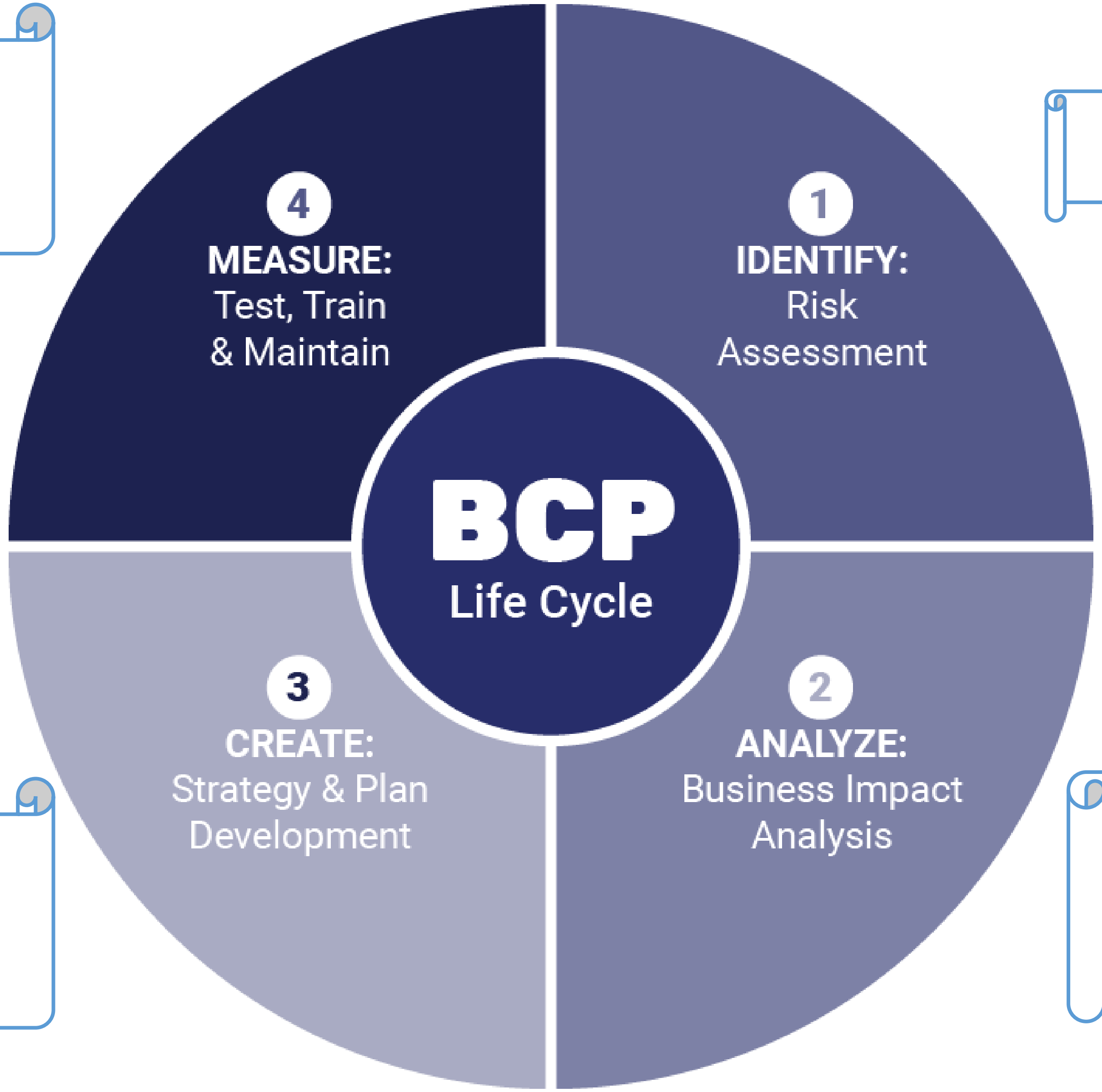
Risk Treatment Decision	Risk Treatment Plan	Control areas for new treatment measures	Treated Residual Risk Likelihood	Treated Residual Risk Consequence	Treated Residual Risk	Date of Risk Owner's Acceptance /Treament Approval	Date Risk Treatment due	Date Risk Treatment Implemented
Mitigate	Monitoring of installation by senior System/Network Administrator. Follow the procedure for Change management. Cunduct replacement during nonworking dayes		D (Unlikely)	3 (Moderate)	**Medium**	2019-07-16	2019-09-04	2019-08-30

Business Continuity Plan

Disaster Recovery Plan

Checklist
Responsibilities
Recovery Team

Identify all scenarios



Assembly Point
Back-Up Location
Recovery Plans

Priorities
Resources
Alignment with SLA

GDPR - General Data Protection Regulation

Approved on April 27, 2016

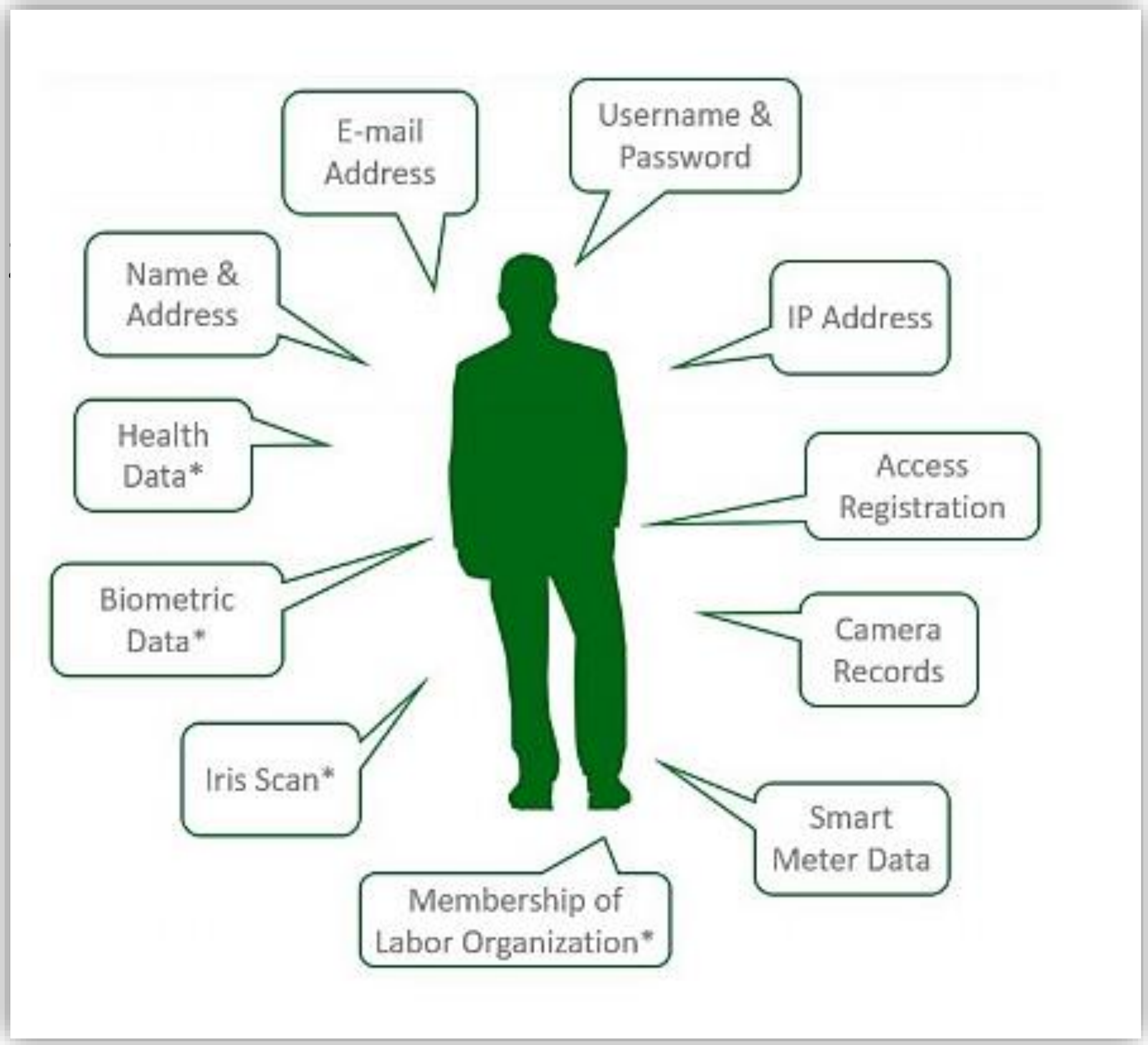
⇨

by May 25,

- All data pertaining to individuals

  not only uniquely identifying information

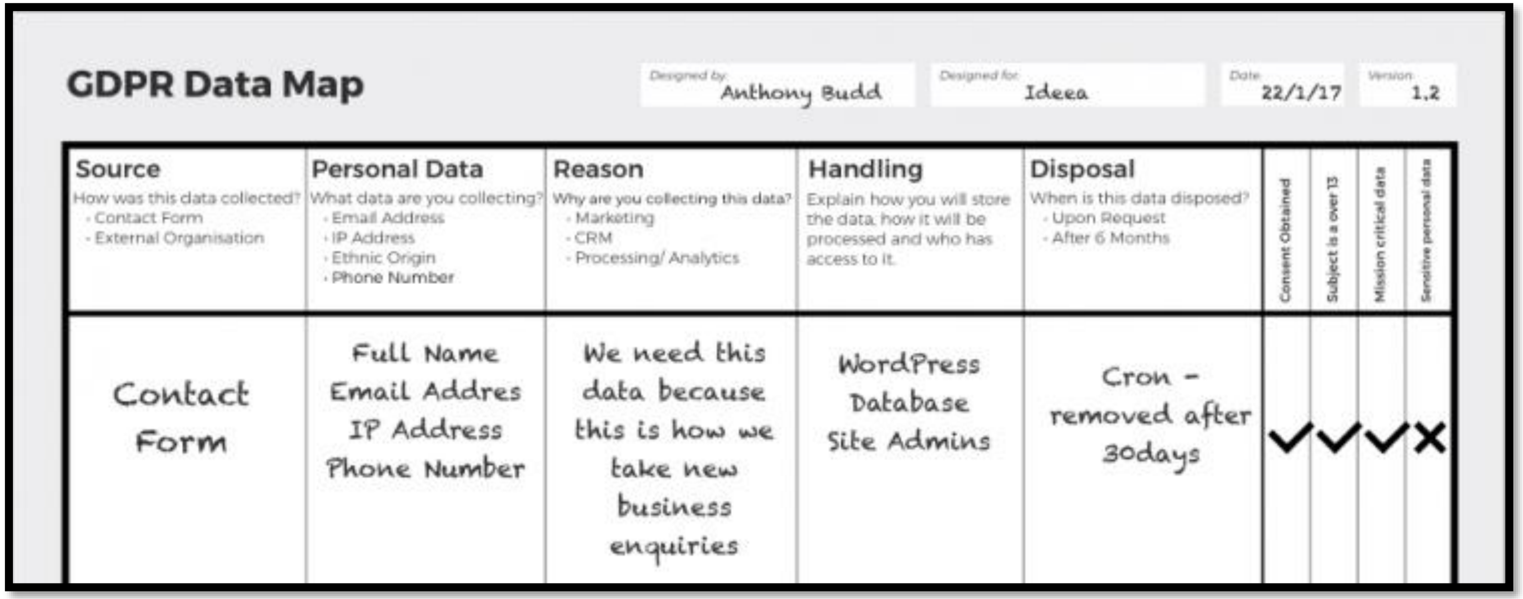
  information routinely requested by websites



GDPR - General Data Protection Regulation

- At least two identifying information

- GDPR Principles
  - *Lawfulness*
  - *Fairness*
  - *Transparency*
  - *Purpose limitation*
  - *Accuracy*
  - *Retention*



GDPR Data Map

Designed by: Anthony Budd
Designed for: Ideea
Date: 22/1/17
Version: 1,2

Source How was this data collected? - Contact Form - External Organisation	Personal Data What data are you collecting? - Email Address - IP Address - Ethnic Origin - Phone Number	Reason Why are you collecting this data? - Marketing - CRM - Processing/ Analytics	Handling Explain how you will store the data, how it will be processed and who has access to it.	Disposal When is this data disposed? - Upon Request - After 6 Months	Consent Obtained	Subject is a over 13	Mission critical data	Sensitive personal data
Contact Form	Full Name Email Addres IP Address Phone Number	We need this data because this is how we take new business enquiries	WordPress Database Site Admins	Cron - removed after 30days	✓	✓	✓	✗

- Data Protection Officer

- Noncompliance with GDPR ⇨ Up to €20 million **or** 4% annual global income