CYLCOMED

RISK MANAGEMENT APPLIED TO CYBERSECURITY AND PRIVACY WITH ISO27001, ISO27701 AND ISO 27005

Dr. João Paulo Rodrigues

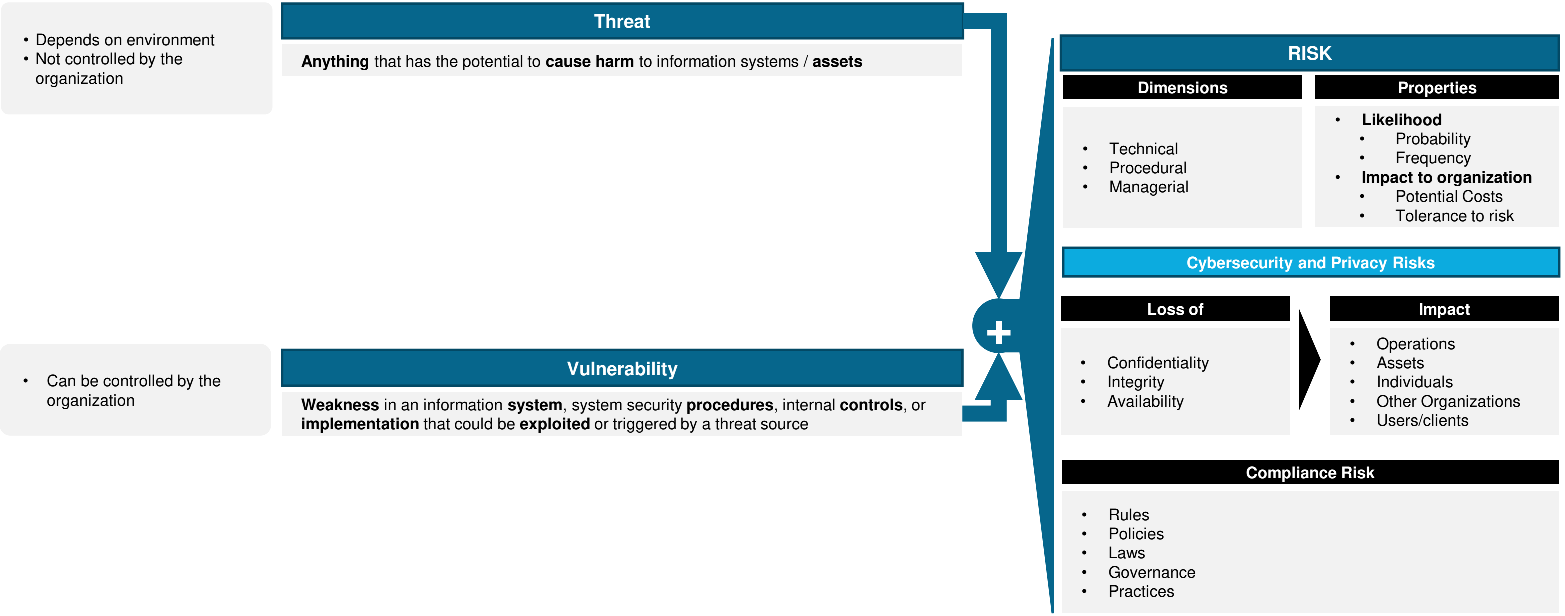
4th of December 2024

TABLE OF CONTENT

- What is Risk and how it is managed
- ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements
- ISO/IEC 27701:2019 – Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines
- ISO 27005:2022 – Information Security, Cybersecurity and Privacy Protection – Guidance on managing Information security risks

WHAT IS RISK AND HOW IT IS MANAGED

WHAT IS RISK



- Depends on environment
- Not controlled by the organization

Threat

Anything that has the potential to **cause harm** to information systems / **assets**

- Can be controlled by the organization

Vulnerability

Weakness in an information **system**, system security **procedures**, internal **controls**, or **implementation** that could be exploited or triggered by a threat source

+

RISK

Dimensions

- Technical
- Procedural
- Managerial

Properties

- **Likelihood**
  - Probability
  - Frequency
- **Impact to organization**
  - Potential Costs
  - Tolerance to risk

Cybersecurity and Privacy Risks

Loss of

- Confidentiality
- Integrity
- Availability

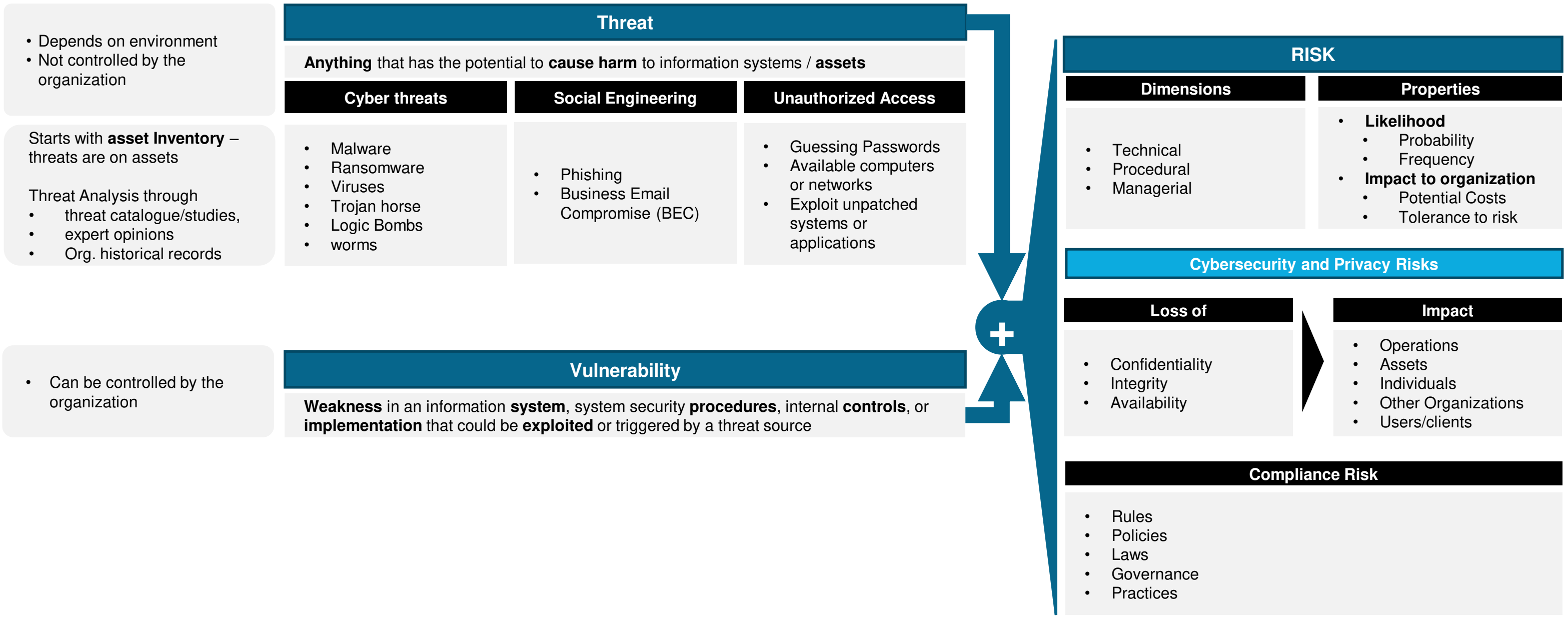
Impact

- Operations
- Assets
- Individuals
- Other Organizations
- Users/clients

Compliance Risk

- Rules
- Policies
- Laws
- Governance
- Practices

WHAT IS RISK – THREAT ANALYSIS



- Depends on environment
- Not controlled by the organization

Starts with **asset Inventory** – threats are on assets

Threat Analysis through
- threat catalogue/studies,
- expert opinions
- Org. historical records

Threat

Anything that has the potential to **cause harm** to information systems / **assets**

Cyber threats	Social Engineering	Unauthorized Access
Malware Ransomware Viruses Trojan horse Logic Bombs worms	Phishing Business Email Compromise (BEC)	Guessing Passwords Available computers or networks Exploit unpatched systems or applications

- Can be controlled by the organization

Vulnerability

Weakness in an information **system**, system security **procedures**, internal **controls**, or **implementation** that could be **exploited** or triggered by a threat source

RISK

Dimensions	Properties
Technical Procedural Managerial	**Likelihood** Probability Frequency **Impact to organization** Potential Costs Tolerance to risk

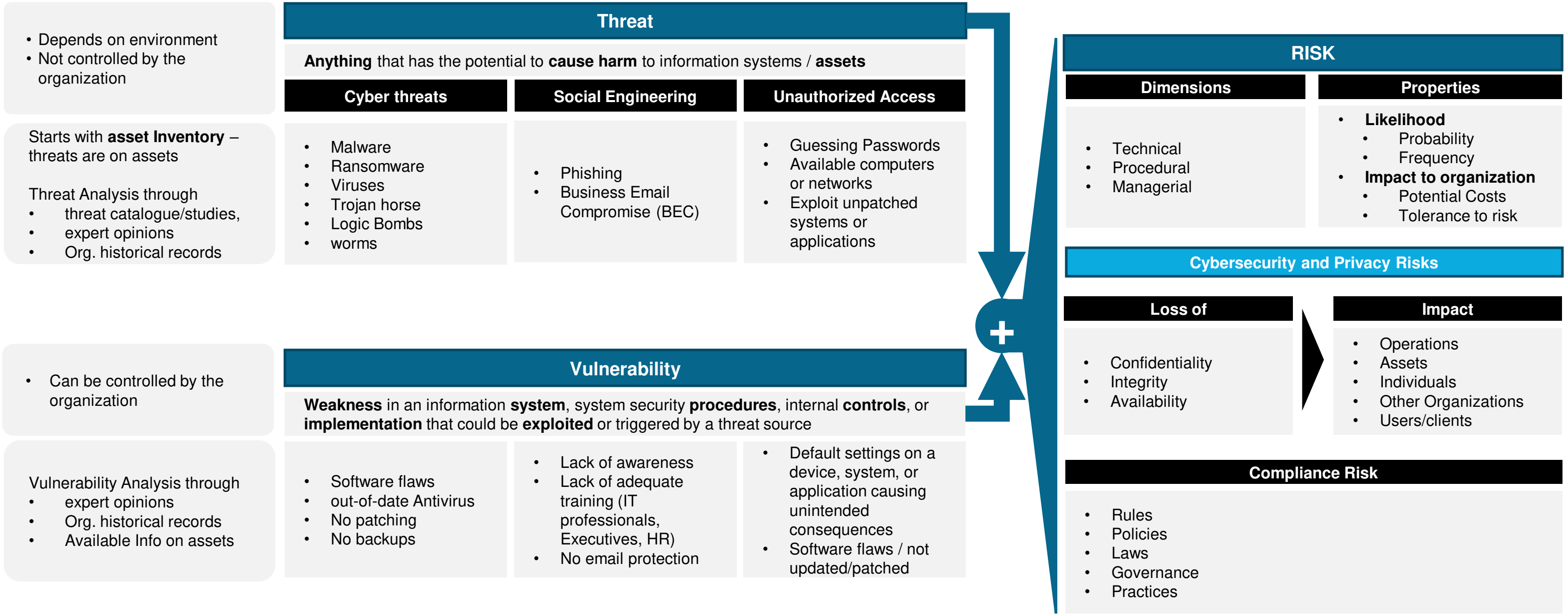
Cybersecurity and Privacy Risks

Loss of	Impact
Confidentiality Integrity Availability	Operations Assets Individuals Other Organizations Users/clients

Compliance Risk

- Rules
- Policies
- Laws
- Governance
- Practices

WHAT IS RISK – VULNERABILITY ANALYSIS



- Depends on environment
- Not controlled by the organization

Starts with **asset Inventory** – threats are on assets

Threat Analysis through
- threat catalogue/studies,
- expert opinions
- Org. historical records

Threat

Anything that has the potential to **cause harm** to information systems / **assets**

Cyber threats
- Malware
- Ransomware
- Viruses
- Trojan horse
- Logic Bombs
- worms

Social Engineering
- Phishing
- Business Email Compromise (BEC)

Unauthorized Access
- Guessing Passwords
- Available computers or networks
- Exploit unpatched systems or applications

+

- Can be controlled by the organization

Vulnerability Analysis through
- expert opinions
- Org. historical records
- Available Info on assets

Vulnerability

Weakness in an information **system**, system security **procedures**, internal **controls**, or **implementation** that could be **exploited** or triggered by a threat source

- Software flaws
- out-of-date Antivirus
- No patching
- No backups

- Lack of awareness
- Lack of adequate training (IT professionals, Executives, HR)
- No email protection

- Default settings on a device, system, or application causing unintended consequences
- Software flaws / not updated/patched

RISK

Dimensions
- Technical
- Procedural
- Managerial

Properties
- **Likelihood**
  - Probability
  - Frequency
- **Impact to organization**
  - Potential Costs
  - Tolerance to risk

Cybersecurity and Privacy Risks

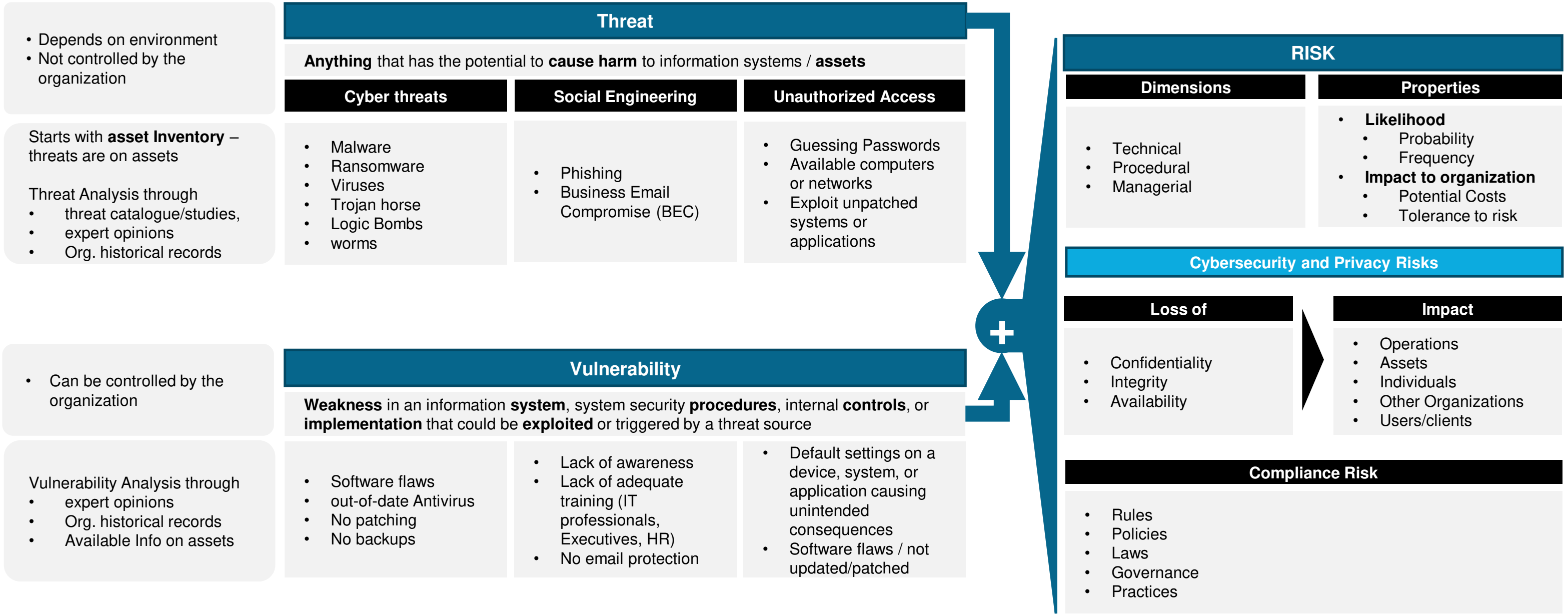
Loss of
- Confidentiality
- Integrity
- Availability

Impact
- Operations
- Assets
- Individuals
- Other Organizations
- Users/clients

Compliance Risk

- Rules
- Policies
- Laws
- Governance
- Practices

WHAT IS RISK – RISK EVALUATION



- Depends on environment
- Not controlled by the organization

Starts with **asset Inventory** – threats are on assets

Threat Analysis through
- threat catalogue/studies,
- expert opinions
- Org. historical records

Threat

Anything that has the potential to **cause harm** to information systems / **assets**

Cyber threats
- Malware
- Ransomware
- Viruses
- Trojan horse
- Logic Bombs
- worms

Social Engineering
- Phishing
- Business Email Compromise (BEC)

Unauthorized Access
- Guessing Passwords
- Available computers or networks
- Exploit unpatched systems or applications

- Can be controlled by the organization

Vulnerability Analysis through
- expert opinions
- Org. historical records
- Available Info on assets

Vulnerability

Weakness in an information **system**, system security **procedures**, internal **controls**, or **implementation** that could be **exploited** or triggered by a threat source

- Software flaws
- out-of-date Antivirus
- No patching
- No backups

- Lack of awareness
- Lack of adequate training (IT professionals, Executives, HR)
- No email protection

- Default settings on a device, system, or application causing unintended consequences
- Software flaws / not updated/patched

+

RISK

Dimensions
- Technical
- Procedural
- Managerial

Properties
- **Likelihood**
  - Probability
  - Frequency
- **Impact to organization**
  - Potential Costs
  - Tolerance to risk

Cybersecurity and Privacy Risks

Loss of
- Confidentiality
- Integrity
- Availability

Impact
- Operations
- Assets
- Individuals
- Other Organizations
- Users/clients

Compliance Risk

- Rules
- Policies
- Laws
- Governance
- Practices

RISK CRITERIA/TOLERANCE

Determined by business leaders

Likelihood	Descriptor
1	Rare
2	Unlikely
3	Possible
4	Likely
5	Almost Certain

	Consequence Score				
Factors	1	2	3	4	5
Safety					
Service/Facility					
Compliance					
Complaint					
Performance Rating					
Image					
Key Objectives delivery					
Claims					
Environment					
Budget					
Contracts					

	Consequence Score				
Likelihood	1	2	3	4	5
5	🟨	🟧	🟥	🟥	🟥
4	🟨	🟧	🟧	🟥	🟥
3	🟩	🟨	🟧	🟧	🟥
2	🟩	🟨	🟨	🟧	🟧
1	🟩	🟩	🟩	🟨	🟨

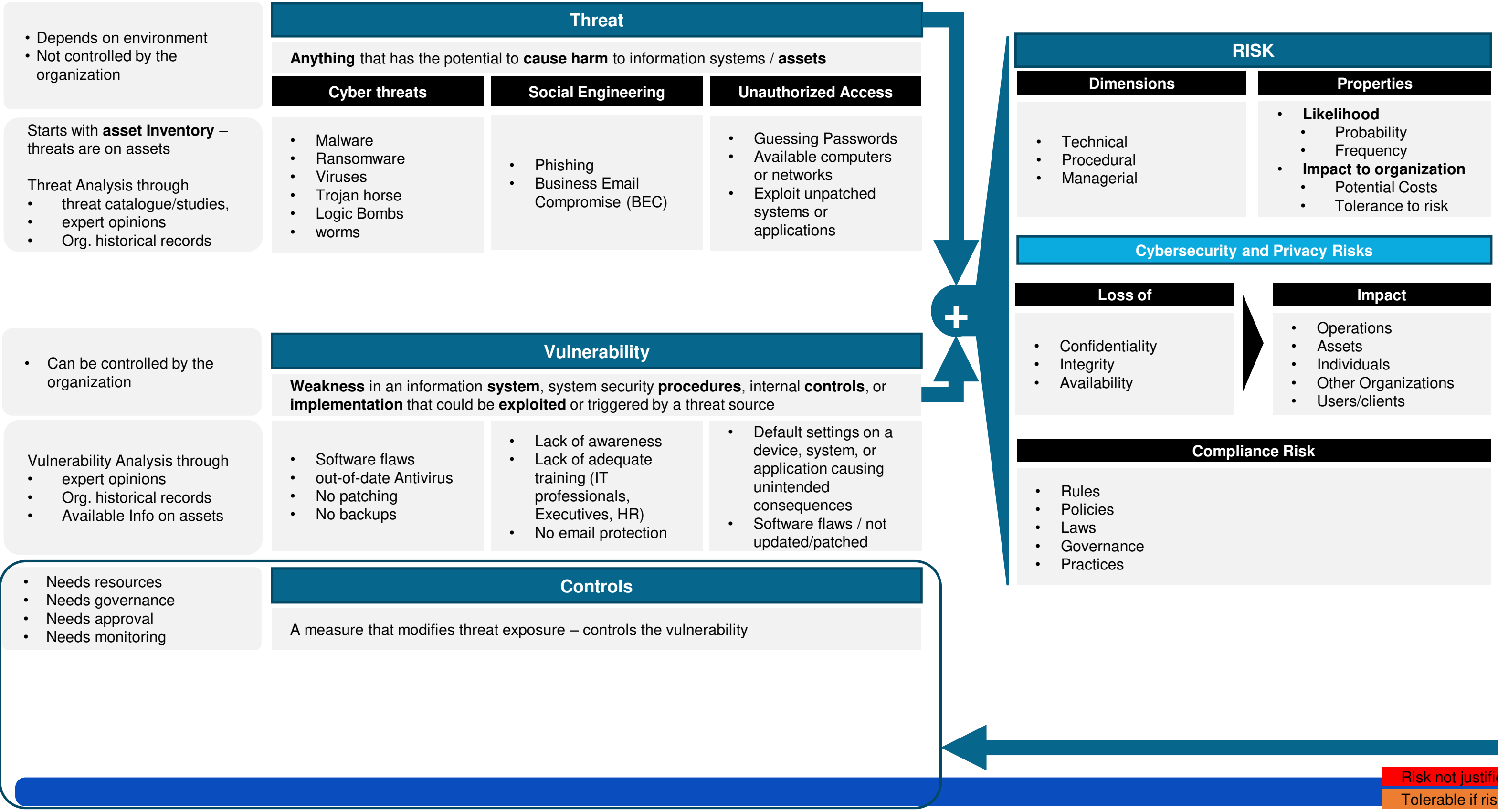
🟥 Risk not justified in any circumstances

🟧 Tolerable if risk reduction is impracticable

🟨 Tolerable. Cost to reduce does not compensate risk

🟩 Assure risk remains at this level

WHAT IS RISK – CONTROLLING THE RISK



- Depends on environment
- Not controlled by the organization

Starts with **asset Inventory** – threats are on assets

Threat Analysis through
- threat catalogue/studies,
- expert opinions
- Org. historical records

Threat

Anything that has the potential to **cause harm** to information systems / **assets**

Cyber threats
- Malware
- Ransomware
- Viruses
- Trojan horse
- Logic Bombs
- worms

Social Engineering
- Phishing
- Business Email Compromise (BEC)

Unauthorized Access
- Guessing Passwords
- Available computers or networks
- Exploit unpatched systems or applications

- Can be controlled by the organization

Vulnerability Analysis through
- expert opinions
- Org. historical records
- Available Info on assets

Vulnerability

Weakness in an information **system**, system security **procedures**, internal **controls**, or **implementation** that could be **exploited** or triggered by a threat source

- Software flaws
- out-of-date Antivirus
- No patching
- No backups

- Lack of awareness
- Lack of adequate training (IT professionals, Executives, HR)
- No email protection

- Default settings on a device, system, or application causing unintended consequences
- Software flaws / not updated/patched

- Needs resources
- Needs governance
- Needs approval
- Needs monitoring

Controls

A measure that modifies threat exposure – controls the vulnerability

RISK

Dimensions
- Technical
- Procedural
- Managerial

Properties
- **Likelihood**
  - Probability
  - Frequency
- **Impact to organization**
  - Potential Costs
  - Tolerance to risk

Cybersecurity and Privacy Risks

Loss of
- Confidentiality
- Integrity
- Availability

Impact
- Operations
- Assets
- Individuals
- Other Organizations
- Users/clients

Compliance Risk
- Rules
- Policies
- Laws
- Governance
- Practices

RISK CRITERIA/TOLERANCE

Determined by business leaders

Likelihood	Descriptor
1	Rare
2	Unlikely
3	Possible
4	Likely
5	Almost Certain

	Consequence Score				
Factors	1	2	3	4	5
Safety					
Service/Facility					
Compliance					
Complaint					
Performance Rating					
Image					
Key Objectives delivery					
Claims					
Environment					
Budget					
Contracts					

	Consequence Score				
Likelihood	1	2	3	4	5
5	🟨	🟧	🟥	🟥	🟥
4	🟨	🟧	🟧	🟥	🟥
3	🟩	🟨	🟧	🟧	🟥
2	🟩	🟨	🟨	🟧	🟧
1	🟩	🟩	🟩	🟨	🟨

- 🟥 Risk not justified in any circumstances
- 🟧 Tolerable if risk reduction is impracticable
- 🟨 Tolerable. Cost to reduce does not compensate risk
- 🟩 Assure risk remains at this level

WHAT IS RISK – CONTROLLING THE RISK

CYLCOMED

- Depends on environment
- Not controlled by the organization

Starts with **asset Inventory** – threats are on assets

Threat Analysis through
- threat catalogue/studies,
- expert opinions
- Org. historical records

Threat

Anything that has the potential to **cause harm** to information systems / **assets**

Cyber threats	Social Engineering	Unauthorized Access
Malware Ransomware Viruses Trojan horse Logic Bombs worms	Phishing Business Email Compromise (BEC)	Guessing Passwords Available computers or networks Exploit unpatched systems or applications

+

- Can be controlled by the organization

Vulnerability Analysis through
- expert opinions
- Org. historical records
- Available Info on assets

Vulnerability

Weakness in an information **system**, system security **procedures**, internal **controls**, or **implementation** that could be **exploited** or triggered by a threat source

Software flaws out-of-date Antivirus No patching No backups	Lack of awareness Lack of adequate training (IT professionals, Executives, HR) No email protection	Default settings on a device, system, or application causing unintended consequences Software flaws / not updated/patched

- Needs resources
- Needs governance
- Needs approval
- Needs monitoring

Controls selected by experts, following standards and technologies best practices ex.: ISO 27001, ISO 27701

Controls

A measure that modifies threat exposure – controls the vulnerability

Frequent software updates Frequent Antivirus Update Auto Patching mechanisms Backup servers	Awareness training Proper training programs Spam protection / attachment removal, etc...	Change default settings to a secure one Frequent software patches/updates

RISK

Dimensions	Properties
Technical Procedural Managerial	**Likelihood** Probability Frequency **Impact to organization** Potential Costs Tolerance to risk

Cybersecurity and Privacy Risks

Loss of	Impact
Confidentiality Integrity Availability	Operations Assets Individuals Other Organizations Users/clients

Compliance Risk

- Rules
- Policies
- Laws
- Governance
- Practices

RISK CRITERIA/TOLERANCE

Determined by business leaders

Likelihood	Descriptor
1	Rare
2	Unlikely
3	Possible
4	Likely
5	Almost Certain

	Consequence Score				
Factors	1	2	3	4	5
Safety					
Service/Facility					
Compliance					
Complaint					
Performance Rating					
Image					
Key Objectives delivery					
Claims					
Environment					
Budget					
Contracts					

	Consequence Score				
Likelihood	1	2	3	4	5
5	🟨	🟧	🟥	🟥	🟥
4	🟨	🟧	🟧	🟥	🟥
3	🟩	🟨	🟧	🟧	🟥
2	🟩	🟨	🟨	🟧	🟧
1	🟩	🟩	🟩	🟨	🟨

🟥 Risk not justified in any circumstances

🟧 Tolerable if risk reduction is impracticable

🟨 Tolerable. Cost to reduce does not compensate risk

🟩 Assure risk remains at this level

WHAT IS RISK – CONSIDER RANSOMWARE ATTACK

CYLCOMED

- Depends on environment
- Not controlled by the organization

Starts with **asset Inventory** – threats are on assets

Threat Analysis through
- threat catalogue/studies,
- expert opinions
- Org. historical records

Threat

Anything that has the potential to **cause harm** to information systems / **assets**

Cyber threats	Social Engineering	Unauthorized Access
Malware Ransomware Viruses Trojan horse Logic Bombs worms	Phishing Business Email Compromise (BEC)	Guessing Passwords Available computers or networks Exploit unpatched systems or applications

+

- Can be controlled by the organization

Vulnerability Analysis through
- expert opinions
- Org. historical records
- Available Info on assets

Vulnerability

Weakness in an information **system**, system security **procedures**, internal **controls**, or **implementation** that could be **exploited** or triggered by a threat source

Software flaws out-of-date Antivirus No patching No backups	Lack of awareness Lack of adequate training (IT professionals, Executives, HR) No email protection	Default settings on a device, system, or application causing unintended consequences Software flaws / not updated/patched

- Needs resources
- Needs governance
- Needs approval
- Needs monitoring

Controls selected by experts, following standards and technologies best practices ex.: ISO 27001, ISO 27701

Controls

A measure that modifies threat exposure – controls the vulnerability

Frequent software updates Frequent Antivirus Update Auto Patching mechanisms Backup servers	Awareness training Proper training programs Spam protection / attachment removal, etc...	Change default settings to a secure one Frequent software patches/updates

RISK

Dimensions	Properties
Technical Procedural Managerial	**Likelihood** Probability Frequency **Impact to organization** Potential Costs Tolerance to risk

Cybersecurity and Privacy Risks

Loss of	Impact
Confidentiality Integrity Availability	Operations Assets Individuals Other Organizations Users/clients

Compliance Risk

- Rules
- Policies
- Laws
- Governance
- Practices

RISK CRITERIA/TOLERANCE

Determined by business leaders

Likelihood	Descriptor
1	Rare
2	Unlikely
3	Possible
4	Likely
5	Almost Certain

	Consequence Score				
Factors	1	2	3	4	5
Safety					
Service/Facility					
Compliance					
Complaint					
Performance Rating					
Image					
Key Objectives delivery					
Claims					
Environment					
Budget					
Contracts					

	Consequence Score				
Likelihood	1	2	3	4	5
5	🟨	🟧	🟥	🟥	🟥
4	🟨	🟧	🟧	🟥	🟥
3	🟩	🟨	🟧	🟧	🟥
2	🟩	🟨	🟨	🟧	🟧
1	🟩	🟩	🟩	🟨	🟨

🟥 Risk not justified in any circumstances

🟧 Tolerable if risk reduction is impracticable

🟨 Tolerable. Cost to reduce does not compensate risk

🟩 Assure risk remains at this level

WHAT IS RISK – CONSIDER RANSOMWARE ATTACK

- Depends on environment
- Not controlled by the organization

Starts with **asset Inventory** – threats are on assets

Threat Analysis through
- threat catalogue/studies,
- expert opinions
- Org. historical records

Threat

Anything that has the potential to **cause harm** to information systems / **assets**

Cyber threats
- Malware
- Ransomware
- Viruses
- Trojan horse
- Logic Bombs
- worms

Social Engineering
- Phishing
- Business Email Compromise (BEC)

Unauthorized Access
- Guessing Passwords
- Available computers or networks
- Exploit unpatched systems or applications

+

- Can be controlled by the organization

Vulnerability Analysis through
- expert opinions
- Org. historical records
- Available Info on assets

Vulnerability

Weakness in an information **system**, system security **procedures**, internal **controls**, or **implementation** that could be **exploited** or triggered by a threat source

- Software flaws
- out-of-date Antivirus
- No patching
- **No backups**

- Lack of awareness
- Lack of adequate training (IT professionals, Executives, HR)
- No email protection

- Default settings on a device, system, or application causing unintended consequences
- Software flaws / not updated/patched

- Needs resources
- Needs governance
- Needs approval
- Needs monitoring

Controls selected by experts, following standards and technologies best practices ex.: ISO 27001, ISO 27701

Controls

A measure that modifies threat exposure – controls the vulnerability

- Frequent software updates
- Frequent Antivirus Update
- Auto Patching mechanisms
- Backup servers

- Awareness training
- Proper training programs
- Spam protection / attachment removal, etc...

- Change default settings to a secure one
- Frequent software patches/updates

RISK

Dimensions
- Technical
- Procedural
- Managerial

Properties
- **Likelihood**
  - Probability
  - Frequency
- **Impact to organization**
  - Potential Costs
  - Tolerance to risk

Cybersecurity and Privacy Risks

Loss of
- Confidentiality
- Integrity
- Availability

Impact
- Operations
- Assets
- Individuals
- Other Organizations
- Users/clients

Compliance Risk
- Rules
- Policies
- Laws
- Governance
- Practices

RISK CRITERIA/TOLERANCE

Determined by business leaders

Likelihood	Descriptor
1	Rare
2	Unlikely
3	Possible
4	Likely
5	Almost Certain

	Consequence Score				
Factors	1	2	3	4	5
Safety		🟩	🟨	🟧	🟥
Service/Facility		🟩	🟨	🟧	🟥
Compliance		🟩	🟨	🟧	🟥
Complaint		🟩	🟨	🟧	🟥
Performance Rating		🟩	🟨	🟧	🟥
Image		🟩	🟨	🟧	🟥
Key Objectives delivery		🟩	🟨	🟧	🟥
Claims		🟩	🟨	🟧	🟥
Environment		🟩	🟨	🟧	🟥
Budget		🟩	🟨	🟧	🟥
Contracts		🟩	🟨	🟧	🟥

	Consequence Score				
Likelihood	1	2	3	4	5
5	🟨	🟧	🟥	🟥	🟥
4	🟨	🟧	🟧	🟥	🟥
3	🟩	🟨	🟧	🟧	🟥
2	🟩	🟨	🟨	🟧	🟧
1	🟩	🟩	🟩	🟨	🟨

🟥	Risk not justified in any circumstances
🟧	Tolerable if risk reduction is impracticable
🟨	Tolerable. Cost to reduce does not compensate risk
🟩	Assure risk remains at this level

WHAT IS RISK – CONSIDER RANSOMWARE ATTACK

- Depends on environment
- Not controlled by the organization

Starts with **asset Inventory** – threats are on assets

Threat Analysis through
- threat catalogue/studies,
- expert opinions
- Org. historical records

Threat

Anything that has the potential to **cause harm** to information systems / **assets**

Cyber threats	Social Engineering	Unauthorized Access
Malware Ransomware Viruses Trojan horse Logic Bombs worms	Phishing Business Email Compromise (BEC)	Guessing Passwords Available computers or networks Exploit unpatched systems or applications

+

- Can be controlled by the organization

Vulnerability Analysis through
- expert opinions
- Org. historical records
- Available Info on assets

Vulnerability

Weakness in an information **system**, system security **procedures**, internal **controls**, or **implementation** that could be **exploited** or triggered by a threat source

Software flaws out-of-date Antivirus No patching No backups	Lack of awareness Lack of adequate training (IT professionals, Executives, HR) No email protection	Default settings on a device, system, or application causing unintended consequences Software flaws / not updated/patched

- Needs resources
- Needs governance
- Needs approval
- Needs monitoring

Controls selected by experts, following standards and technologies best practices ex.: ISO 27001, ISO 27701

Controls

A measure that modifies threat exposure – controls the vulnerability

Frequent software updates Frequent Antivirus Update Auto Patching mechanisms Backup servers	Awareness training Proper training programs Spam protection / attachment removal, etc...	Change default settings to a secure one Frequent software patches/updates

RISK

Dimensions	Properties
Technical Procedural Managerial	**Likelihood** Probability Frequency **Impact to organization** Potential Costs Tolerance to risk

Cybersecurity and Privacy Risks

Loss of	Impact
Confidentiality Integrity Availability	Operations Assets Individuals Other Organizations Users/clients

Compliance Risk

- Rules
- Policies
- Laws
- Governance
- Practices

RISK CRITERIA/TOLERANCE

Determined by business leaders

Likelihood	Descriptor
1	Rare
2	Unlikely
3	Possible
4	Likely
5	Almost Certain

	Consequence Score				
Factors	1	2	3	4	5
Safety					
Service/Facility					
Compliance					
Complaint					
Performance Rating					
Image					
Key Objectives delivery					
Claims					
Environment					
Budget					
Contracts					

	Consequence Score				
Likelihood	1	2	3	4	5
5	🟨	🟧	🟥	🟥	🟥
4	🟨	🟧	🟧	🟥	🟥
3	🟩	🟨	🟧	🟧	🟥
2	🟩	🟨	🟨	🟧	🟧
1	🟩	🟩	🟩	🟨	🟨

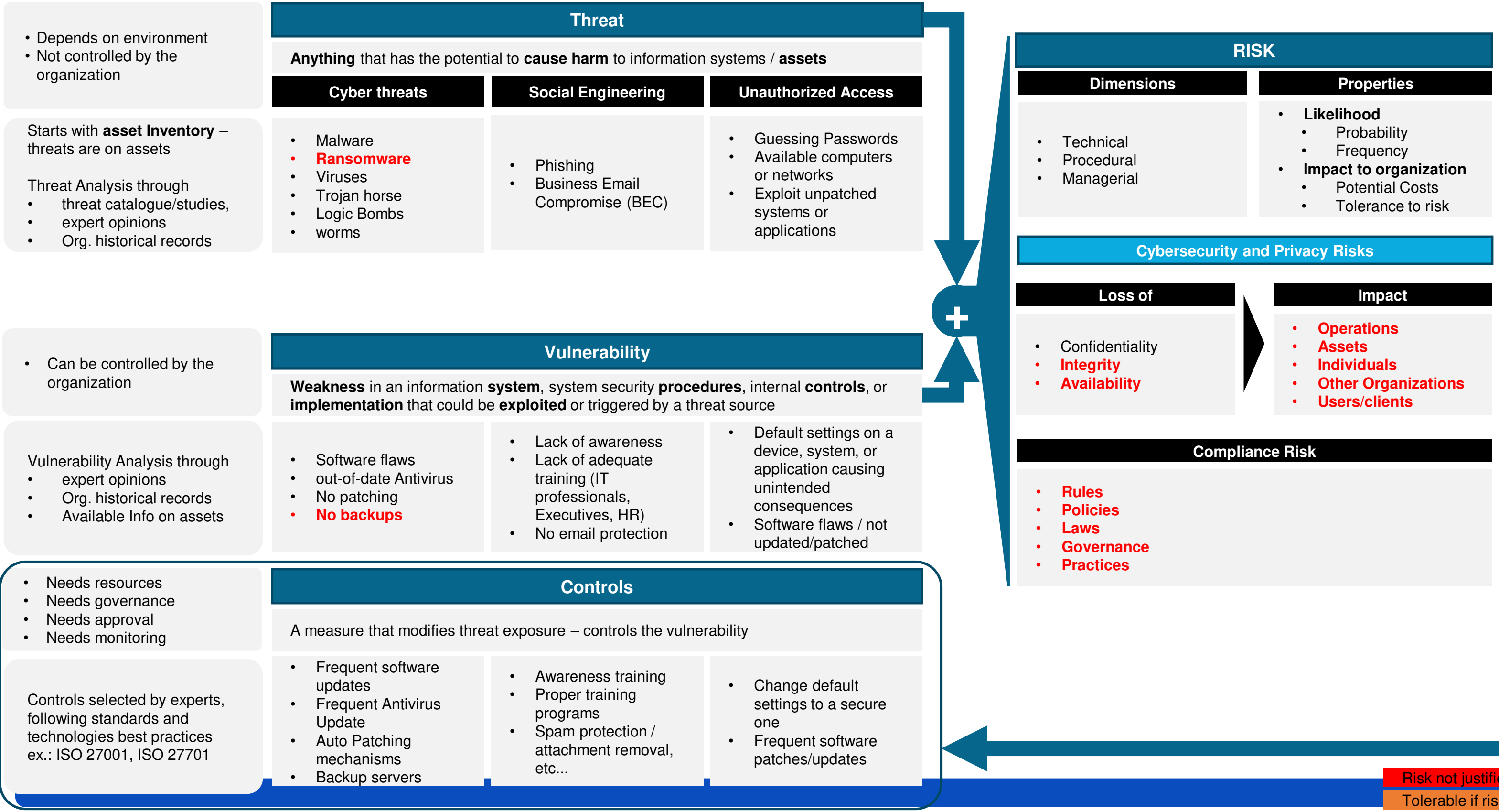
🟥 Risk not justified in any circumstances

🟧 Tolerable if risk reduction is impracticable

🟨 Tolerable. Cost to reduce does not compensate risk

🟩 Assure risk remains at this level

WHAT IS RISK – CONSIDER RANSOMWARE ATTACK



- Depends on environment
- Not controlled by the organization

Starts with **asset Inventory** – threats are on assets

Threat Analysis through
- threat catalogue/studies,
- expert opinions
- Org. historical records

Threat

Anything that has the potential to **cause harm** to information systems / **assets**

Cyber threats
- Malware
- **Ransomware**
- Viruses
- Trojan horse
- Logic Bombs
- worms

Social Engineering
- Phishing
- Business Email Compromise (BEC)

Unauthorized Access
- Guessing Passwords
- Available computers or networks
- Exploit unpatched systems or applications

+

- Can be controlled by the organization

Vulnerability Analysis through
- expert opinions
- Org. historical records
- Available Info on assets

Vulnerability

Weakness in an information **system**, system security **procedures**, internal **controls**, or **implementation** that could be **exploited** or triggered by a threat source

- Software flaws
- out-of-date Antivirus
- No patching
- **No backups**

- Lack of awareness
- Lack of adequate training (IT professionals, Executives, HR)
- No email protection

- Default settings on a device, system, or application causing unintended consequences
- Software flaws / not updated/patched

- Needs resources
- Needs governance
- Needs approval
- Needs monitoring

Controls selected by experts, following standards and technologies best practices ex.: ISO 27001, ISO 27701

Controls

A measure that modifies threat exposure – controls the vulnerability

- Frequent software updates
- Frequent Antivirus Update
- Auto Patching mechanisms
- Backup servers

- Awareness training
- Proper training programs
- Spam protection / attachment removal, etc...

- Change default settings to a secure one
- Frequent software patches/updates

RISK

Dimensions
- Technical
- Procedural
- Managerial

Properties
- **Likelihood**
  - Probability
  - Frequency
- **Impact to organization**
  - Potential Costs
  - Tolerance to risk

Cybersecurity and Privacy Risks

Loss of
- Confidentiality
- **Integrity**
- **Availability**

Impact
- **Operations**
- **Assets**
- **Individuals**
- **Other Organizations**
- **Users/clients**

Compliance Risk
- **Rules**
- **Policies**
- **Laws**
- **Governance**
- **Practices**

RISK CRITERIA/TOLERANCE

Determined by business leaders

Likelihood	Descriptor
1	Rare
2	Unlikely
3	Possible
4	Likely
5	Almost Certain

	Consequence Score				
Factors	1	2	3	4	5
Safety					
Service/Facility					
Compliance					
Complaint					
Performance Rating					
Image					
Key Objectives delivery					
Claims					
Environment					
Budget					
Contracts					

	Consequence Score				
Likelihood	1	2	3	4	5
5	🟨	🟧	🟥	🟥	🟥
4	🟨	🟧	🟧	🟥	🟥
3	🟩	🟨	🟧	🟧	🟥
2	🟩	🟨	🟨	🟧	🟧
1	🟩	🟩	🟩	🟨	🟨

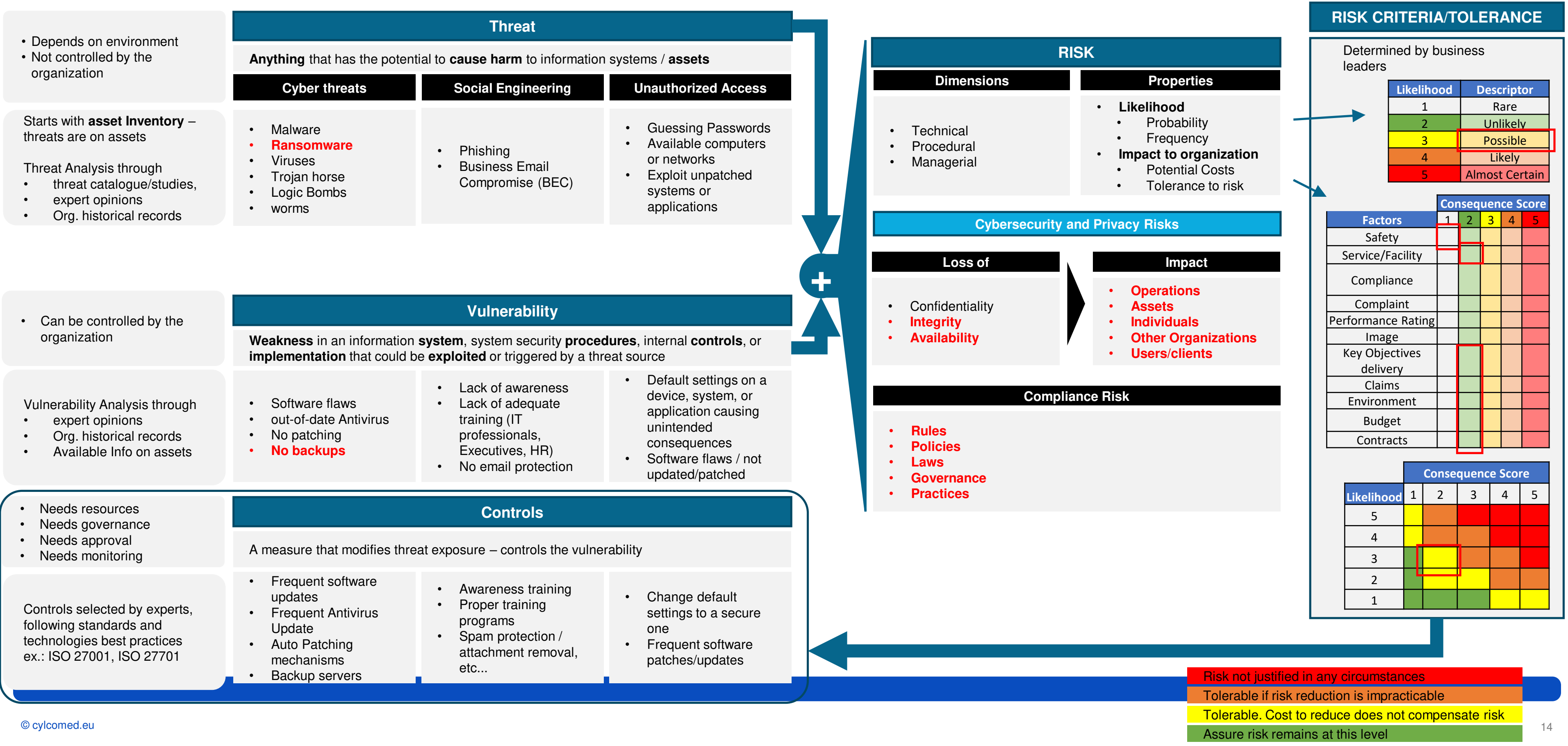
🟥 Risk not justified in any circumstances

🟧 Tolerable if risk reduction is impracticable

🟨 Tolerable. Cost to reduce does not compensate risk

🟩 Assure risk remains at this level

WHAT IS RISK – CONSIDER RANSOMWARE ATTACK ON HOTEL



- Depends on environment
- Not controlled by the organization

Starts with **asset Inventory** – threats are on assets

Threat Analysis through
- threat catalogue/studies,
- expert opinions
- Org. historical records

Threat

Anything that has the potential to **cause harm** to information systems / **assets**

Cyber threats	Social Engineering	Unauthorized Access
• Malware • **Ransomware** • Viruses • Trojan horse • Logic Bombs • worms	• Phishing • Business Email Compromise (BEC)	• Guessing Passwords • Available computers or networks • Exploit unpatched systems or applications

+

- Can be controlled by the organization

Vulnerability Analysis through
- expert opinions
- Org. historical records
- Available Info on assets

Vulnerability

Weakness in an information **system**, system security **procedures**, internal **controls**, or **implementation** that could be **exploited** or triggered by a threat source

• Software flaws • out-of-date Antivirus • No patching • **No backups**	• Lack of awareness • Lack of adequate training (IT professionals, Executives, HR) • No email protection	• Default settings on a device, system, or application causing unintended consequences • Software flaws / not updated/patched

- Needs resources
- Needs governance
- Needs approval
- Needs monitoring

Controls selected by experts, following standards and technologies best practices ex.: ISO 27001, ISO 27701

Controls

A measure that modifies threat exposure – controls the vulnerability

• Frequent software updates • Frequent Antivirus Update • Auto Patching mechanisms • Backup servers	• Awareness training • Proper training programs • Spam protection / attachment removal, etc...	• Change default settings to a secure one • Frequent software patches/updates

RISK

Dimensions	Properties
• Technical • Procedural • Managerial	• **Likelihood** • Probability • Frequency • **Impact to organization** • Potential Costs • Tolerance to risk

Cybersecurity and Privacy Risks

Loss of	Impact
• Confidentiality • **Integrity** • **Availability**	• **Operations** • **Assets** • **Individuals** • **Other Organizations** • **Users/clients**

Compliance Risk

- **Rules**
- **Policies**
- **Laws**
- **Governance**
- **Practices**

RISK CRITERIA/TOLERANCE

Determined by business leaders

Likelihood	Descriptor
1	Rare
2	Unlikely
3	Possible
4	Likely
5	Almost Certain

	Consequence Score				
Factors	1	2	3	4	5
Safety					
Service/Facility					
Compliance					
Complaint					
Performance Rating					
Image					
Key Objectives delivery					
Claims					
Environment					
Budget					
Contracts					

	Consequence Score				
Likelihood	1	2	3	4	5
5	🟨	🟧	🟥	🟥	🟥
4	🟨	🟧	🟧	🟥	🟥
3	🟩	🟨	🟧	🟧	🟥
2	🟩	🟨	🟨	🟧	🟧
1	🟩	🟩	🟩	🟨	🟨

🟥 Risk not justified in any circumstances

🟧 Tolerable if risk reduction is impracticable

🟨 Tolerable. Cost to reduce does not compensate risk

🟩 Assure risk remains at this level

WHAT IS RISK – CONSIDER RANSOMWARE ATTACK ON HOSPITAL WITH RISK CONTROL

CYLCOMED

- Depends on environment
- Not controlled by the organization

Starts with **asset Inventory** – threats are on assets

Threat Analysis through
- threat catalogue/studies,
- expert opinions
- Org. historical records

Threat

Anything that has the potential to **cause harm** to information systems / **assets**

Cyber threats	Social Engineering	Unauthorized Access
Malware **Ransomware** Viruses Trojan horse Logic Bombs worms	Phishing Business Email Compromise (BEC)	Guessing Passwords Available computers or networks Exploit unpatched systems or applications

+

- Can be controlled by the organization

Vulnerability Analysis through
- expert opinions
- Org. historical records
- Available Info on assets

Vulnerability

Weakness in an information **system**, system security **procedures**, internal **controls**, or **implementation** that could be **exploited** or triggered by a threat source

Software flaws out-of-date Antivirus No patching **No backups**	Lack of awareness Lack of adequate training (IT professionals, Executives, HR) No email protection	Default settings on a device, system, or application causing unintended consequences Software flaws / not updated/patched

- Needs resources
- Needs governance
- Needs approval
- Needs monitoring

Controls selected by experts, following standards and technologies best practices ex.: ISO 27001, ISO 27701

Controls

A measure that modifies threat exposure – controls the vulnerability

Frequent software updates Frequent Antivirus Update Auto Patching mechanisms Backup servers	Awareness training Proper training programs Spam protection / attachment removal, etc...	Change default settings to a secure one Frequent software patches/updates

RISK

Dimensions	Properties
Technical Procedural Managerial	**Likelihood** Probability Frequency **Impact to organization** Potential Costs Tolerance to risk

Cybersecurity and Privacy Risks

Loss of	Impact
Confidentiality **Integrity** **Availability**	**Operations** **Assets** **Individuals** **Other Organizations** **Users/clients**

Compliance Risk

- **Rules**
- **Policies**
- **Laws**
- **Governance**
- **Practices**

RISK CRITERIA/TOLERANCE

Determined by business leaders

Likelihood	Descriptor
1	Rare
2	Unlikely
3	Possible
4	Likely
5	Almost Certain

	Consequence Score				
Factors	1	2	3	4	5
Patient Safety					
Service/Facility					
Compliance					
Complaint					
Performance Rating					
Image					
Key Objectives delivery					
Claims					
Environment					
Budget					
Contracts					

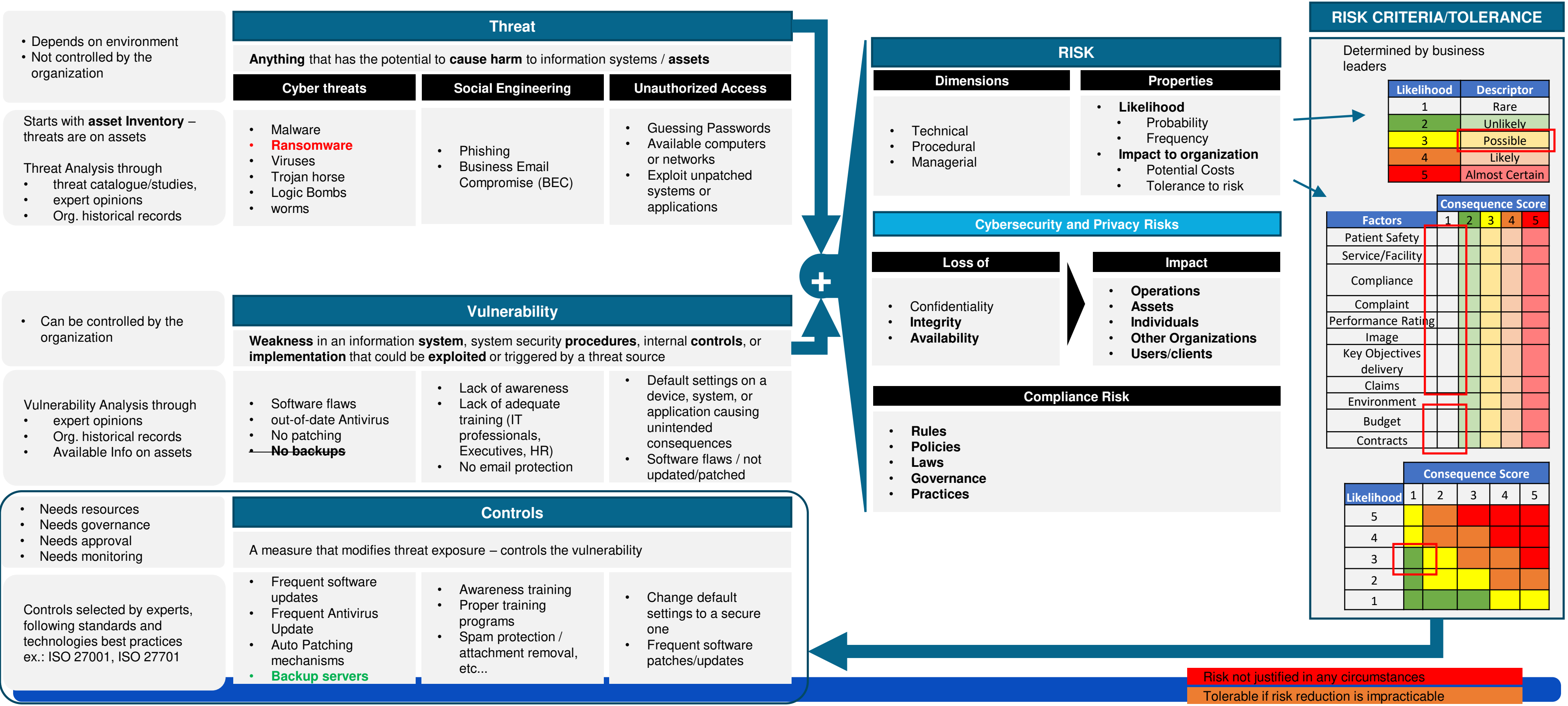
	Consequence Score				
Likelihood	1	2	3	4	5
5	🟨	🟧	🟥	🟥	🟥
4	🟨	🟧	🟧	🟥	🟥
3	🟩	🟨	🟧	🟧	🟥
2	🟩	🟨	🟨	🟧	🟧
1	🟩	🟩	🟩	🟨	🟨

- 🟥 Risk not justified in any circumstances
- 🟧 Tolerable if risk reduction is impractical
- 🟨 Tolerable. Cost to reduce does not compensate risk
- 🟩 Assure risk remains at this level

© cylcomed.eu

WHAT IS RISK – CONSIDER RANSOMWARE ATTACK ON HOSPITAL WITH RISK CONTROL

CYLCOMED



- Depends on environment
- Not controlled by the organization

Starts with **asset Inventory** – threats are on assets

Threat Analysis through
- threat catalogue/studies,
- expert opinions
- Org. historical records

Threat

Anything that has the potential to **cause harm** to information systems / **assets**

Cyber threats	Social Engineering	Unauthorized Access
• Malware • Ransomware • Viruses • Trojan horse • Logic Bombs • worms	• Phishing • Business Email Compromise (BEC)	• Guessing Passwords • Available computers or networks • Exploit unpatched systems or applications

- Can be controlled by the organization

Vulnerability Analysis through
- expert opinions
- Org. historical records
- Available Info on assets

Vulnerability

Weakness in an information **system**, system security **procedures**, internal **controls**, or **implementation** that could be **exploited** or triggered by a threat source

• Software flaws • out-of-date Antivirus • No patching • ~~**No backups**~~	• Lack of awareness • Lack of adequate training (IT professionals, Executives, HR) • No email protection	• Default settings on a device, system, or application causing unintended consequences • Software flaws / not updated/patched

- Needs resources
- Needs governance
- Needs approval
- Needs monitoring

Controls selected by experts, following standards and technologies best practices ex.: ISO 27001, ISO 27701

Controls

A measure that modifies threat exposure – controls the vulnerability

• Frequent software updates • Frequent Antivirus Update • Auto Patching mechanisms • **Backup servers**	• Awareness training • Proper training programs • Spam protection / attachment removal, etc...	• Change default settings to a secure one • Frequent software patches/updates

RISK

Dimensions	Properties
• Technical • Procedural • Managerial	• **Likelihood** • Probability • Frequency • **Impact to organization** • Potential Costs • Tolerance to risk

Cybersecurity and Privacy Risks

Loss of	Impact
• Confidentiality • **Integrity** • **Availability**	• **Operations** • **Assets** • **Individuals** • **Other Organizations** • **Users/clients**

Compliance Risk

- **Rules**
- **Policies**
- **Laws**
- **Governance**
- **Practices**

RISK CRITERIA/TOLERANCE

Determined by business leaders

Likelihood	Descriptor
1	Rare
2	Unlikely
3	Possible
4	Likely
5	Almost Certain

	Consequence Score				
Factors	1	2	3	4	5
Patient Safety					
Service/Facility					
Compliance					
Complaint					
Performance Rating					
Image					
Key Objectives delivery					
Claims					
Environment					
Budget					
Contracts					

	Consequence Score				
Likelihood	1	2	3	4	5
5	🟨	🟧	🟥	🟥	🟥
4	🟨	🟧	🟧	🟥	🟥
3	🟩	🟨	🟧	🟧	🟥
2	🟩	🟨	🟨	🟧	🟧
1	🟩	🟩	🟩	🟨	🟨

🟥 Risk not justified in any circumstances

🟧 Tolerable if risk reduction is impractical

🟨 Tolerable. Cost to reduce does not compensate risk

🟩 Assure risk remains at this level

NHS RISK REGISTER REPORT - CONSEQUENCES SCORE AND FACTORS

CYLCOMED

	Consequence Score				
	Negligible	Minor	Moderate	Major	Catastrophic
Factors	1	2	3	4	5
Patient Safety	Minimal injury requiring no/minimal intervention or treatment.	Minor implications for patient safety if unresolved	Treatment or service has significantly reduced effectiveness Major patient safety implications if findings are not acted on	Major injury leading to long-term incapacity/disability	An issue which impacts on a large number of patients, increased probability of death or irreversible health effects.
Service/Facility	Peripheral element of treatment or service suboptimal	Overall treatment or service suboptimal Loss/interruption of more than 8 hours	Treatment or service has significantly reduced effectiveness		An issue which impacts on a large number of patients, increased probability of death or irreversible health effects. Permanent loss of service or facility
Compliance		single failure to meet internal standards Breech of statutory legislation	Repeated failure to meet statutory or contractual standards Challenging external recommendations/improvement notice	Non-compliance with national standards with significant risk to patients if unresolved Enforcement action Multiple breeches in statutory duty Improvement notices	Gross failure to meet national standards Multiple breeeches in statutory or regulatory duty Prosecution
Complaint	Informal complaint/inquiry			Multiple complaints/independent review	
Performance Rating		Reduced performance rating if unresolved		Low performance rating	
Image		Elements of public expectation not being met	Local media coverage - long-term reduction in public confidence	National media coverage with less than 3 days service well below reasonable public expectation	National media coverage with greater than 3 days service well below reasonable public expectation
Key Objectives delivery				Uncertain delivery of key objective/service due to lack of staff	
Claims		Claim less than £10.000		Claim(s) between £100.000 and £1 million	Claim(s) > £1 million
Environment		Minor impact on environment			Catastrophic impact on environment
Budget		loss of 01-0.25 per cent of budget	Loss of 0.25 - 0.5 per cent of budget	Non-compliance with national 10-25 per cent over project budget Uncertain delivery of key objective/Loss of 0.5 - 1.0 per cent of budget	Incident leading to greater than 25 per cent over project budget
Contracts					Loss of contract / payment by results

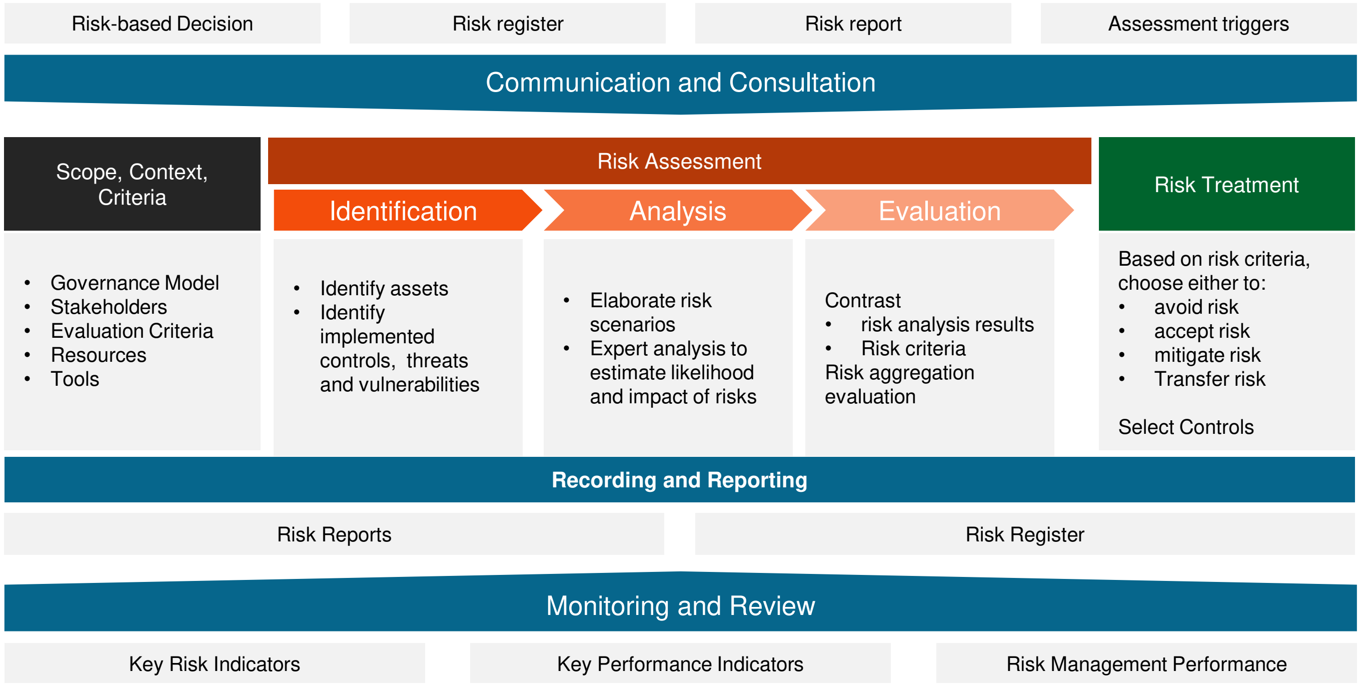
based on https://www.uhd.nhs.uk/uploads/about/docs/bod/2022/6.3_risk_register_report.pdf)

NHS RISK REGISTER REPORT - LIKELIHOOD SCORE

Likelihood Score	Descriptor	Frequency - How often might it/does it happen
1	Rare	- This will probably never happen/occur - Not expected to occur for years
2	Unlikely	- Do not expect it to happen/ocur but it is possible it may do so - expected to occur at least annually
3	Possible	- Might happen or recur occasionally - Expected to occur monthly
4	Likely	- Will probably happen/recur but it is not a persisting issue - Expected to occur weekly
5	Almost Certain	- Will undoubtedly happen/occur, possibly frequently - Expected to occur daily

based on https://www.uhd.nhs.uk/uploads/about/docs/bod/2022/6.3_risk_register_report.pdf)

SIMPLIFIED PROCESS FLOW DIAGRAM OF ISO 31000 – RISK MANAGEMENT GUIDELINES



Risk-based Decision

Risk register

Risk report

Assessment triggers

Communication and Consultation

Scope, Context, Criteria

- Governance Model
- Stakeholders
- Evaluation Criteria
- Resources
- Tools

Risk Assessment

Identification

- Identify assets
- Identify implemented controls, threats and vulnerabilities

Analysis

- Elaborate risk scenarios
- Expert analysis to estimate likelihood and impact of risks

Evaluation

Contrast
- risk analysis results
- Risk criteria

Risk aggregation evaluation

Risk Treatment

Based on risk criteria, choose either to:
- avoid risk
- accept risk
- mitigate risk
- Transfer risk

Select Controls

Recording and Reporting

Risk Reports

Risk Register

Monitoring and Review

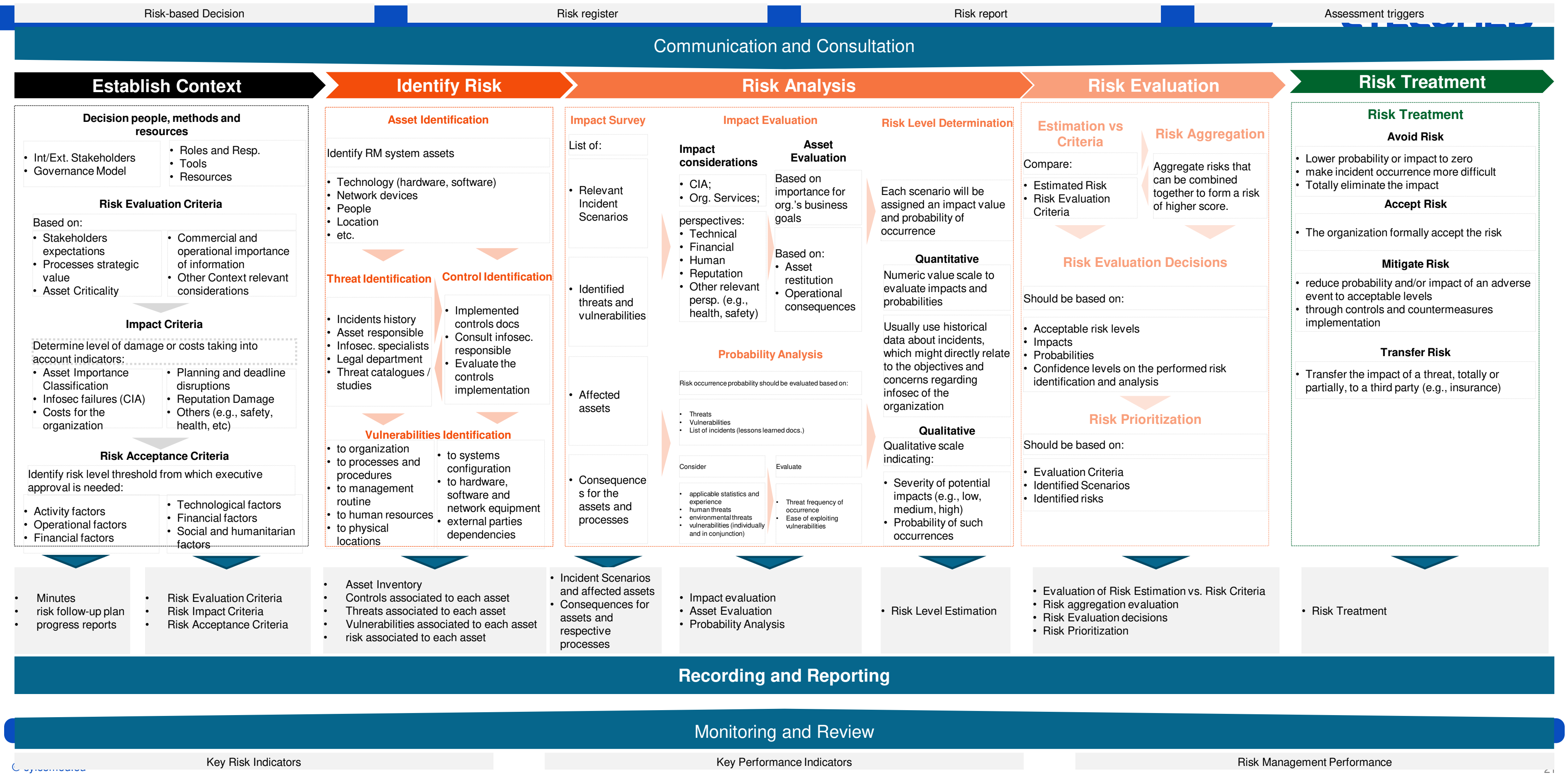
Key Risk Indicators

Key Performance Indicators

Risk Management Performance

ISO 27005:2022 – INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION – GUIDANCE ON MANAGING INFORMATION SECURITY RISKS

ISO 27005 – PROCESS FLOW DIAGRAM



Risk-based Decision | Risk register | Risk report | Assessment triggers

Communication and Consultation

Establish Context

Decision people, methods and resources

- Int/Ext. Stakeholders
- Governance Model

- Roles and Resp.
- Tools
- Resources

Risk Evaluation Criteria

Based on:

- Stakeholders expectations
- Processes strategic value
- Asset Criticality

- Commercial and operational importance of information
- Other Context relevant considerations

Impact Criteria

Determine level of damage or costs taking into account indicators:

- Asset Importance Classification
- Infosec failures (CIA)
- Costs for the organization

- Planning and deadline disruptions
- Reputation Damage
- Others (e.g., safety, health, etc)

Risk Acceptance Criteria

Identify risk level threshold from which executive approval is needed:

- Activity factors
- Operational factors
- Financial factors

- Technological factors
- Financial factors
- Social and humanitarian factors

Identify Risk

Asset Identification

Identify RM system assets

- Technology (hardware, software)
- Network devices
- People
- Location
- etc.

Threat Identification

- Incidents history
- Asset responsible
- Infosec. specialists
- Legal department
- Threat catalogues / studies

Control Identification

- Implemented controls docs
- Consult infosec. responsible
- Evaluate the controls implementation

Vulnerabilities Identification

- to organization
- to processes and procedures
- to management routine
- to human resources
- to physical locations

- to systems configuration
- to hardware, software and network equipment
- external parties dependencies

Risk Analysis

Impact Survey

List of:

- Relevant Incident Scenarios
- Identified threats and vulnerabilities
- Affected assets
- Consequences for the assets and processes

Impact Evaluation

Impact considerations

- CIA;
- Org. Services;

perspectives:

- Technical
- Financial
- Human
- Reputation
- Other relevant persp. (e.g., health, safety)

Asset Evaluation

Based on importance for org.'s business goals

Based on:

- Asset restitution
- Operational consequences

Probability Analysis

Risk occurrence probability should be evaluated based on:

- Threats
- Vulnerabilities
- List of incidents (lessons learned docs.)

Consider

- applicable statistics and experience
- human threats
- environmental threats
- vulnerabilities (individually and in conjunction)

Evaluate

- Threat frequency of occurrence
- Ease of exploiting vulnerabilities

Risk Level Determination

Each scenario will be assigned an impact value and probability of occurrence

Quantitative

Numeric value scale to evaluate impacts and probabilities

Usually use historical data about incidents, which might directly relate to the objectives and concerns regarding infosec of the organization

Qualitative

Qualitative scale indicating:

- Severity of potential impacts (e.g., low, medium, high)
- Probability of such occurrences

Risk Evaluation

Estimation vs Criteria

Compare:

- Estimated Risk
- Risk Evaluation Criteria

Risk Aggregation

Aggregate risks that can be combined together to form a risk of higher score.

Risk Evaluation Decisions

Should be based on:

- Acceptable risk levels
- Impacts
- Probabilities
- Confidence levels on the performed risk identification and analysis

Risk Prioritization

Should be based on:

- Evaluation Criteria
- Identified Scenarios
- Identified risks

Risk Treatment

Risk Treatment

Avoid Risk

- Lower probability or impact to zero
- make incident occurrence more difficult
- Totally eliminate the impact

Accept Risk

- The organization formally accept the risk

Mitigate Risk

- reduce probability and/or impact of an adverse event to acceptable levels
- through controls and countermeasures implementation

Transfer Risk

- Transfer the impact of a threat, totally or partially, to a third party (e.g., insurance)

- Minutes
- risk follow-up plan
- progress reports

- Risk Evaluation Criteria
- Risk Impact Criteria
- Risk Acceptance Criteria

- Asset Inventory
- Controls associated to each asset
- Threats associated to each asset
- Vulnerabilities associated to each asset
- risk associated to each asset

- Incident Scenarios and affected assets
- Consequences for assets and respective processes

- Impact evaluation
- Asset Evaluation
- Probability Analysis

- Risk Level Estimation

- Evaluation of Risk Estimation vs. Risk Criteria
- Risk aggregation evaluation
- Risk Evaluation decisions
- Risk Prioritization

- Risk Treatment

Recording and Reporting

Monitoring and Review

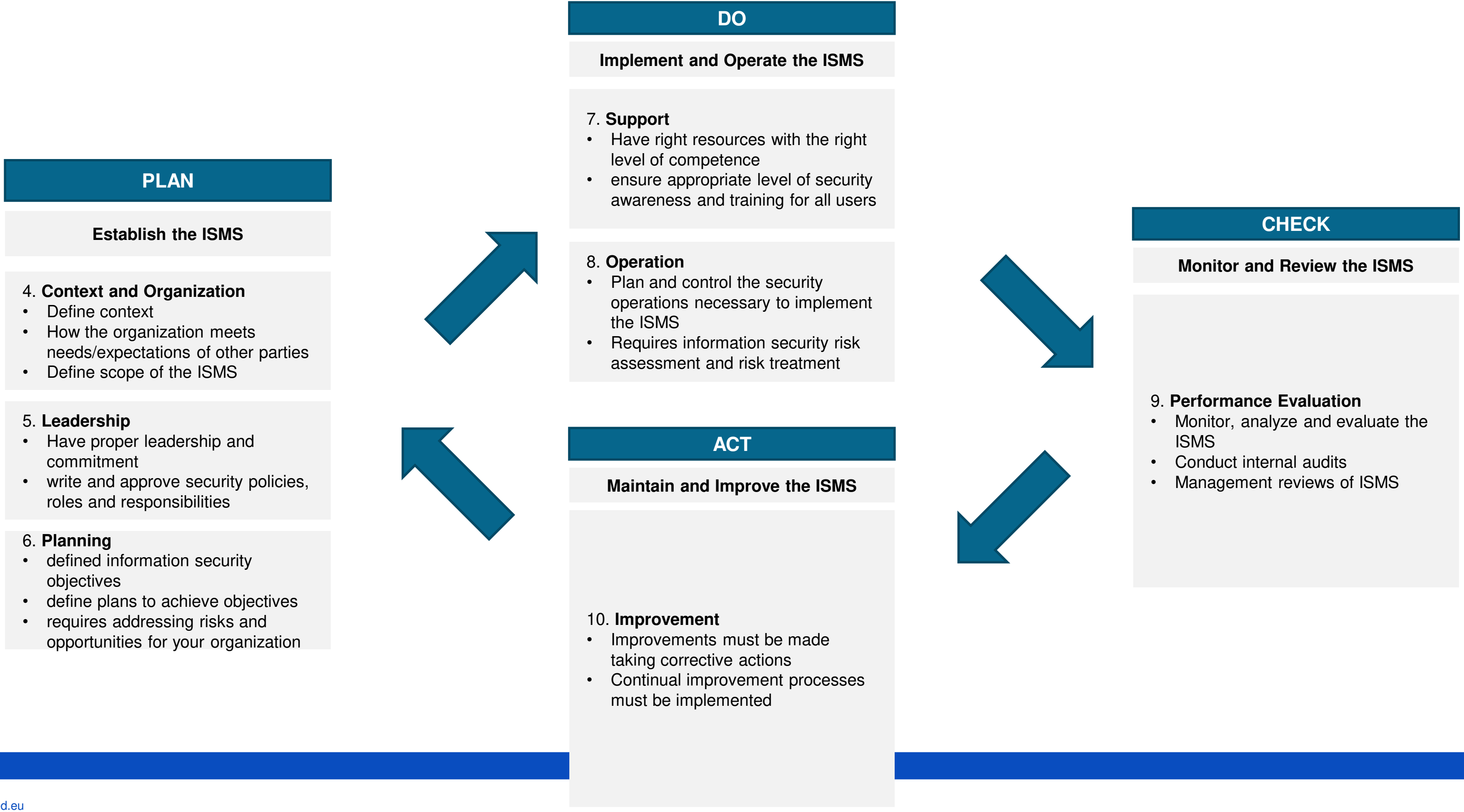
Key Risk Indicators | Key Performance Indicators | Risk Management Performance

ISO/IEC 27001:2022 INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION – INFORMATION SECURITY MANAGEMENT SYSTEMS - REQUIREMENTS

ISO 27001:2022 - SCOPE

- ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS) within an organization.

ISO 27001:2022 - FRAMEWORK PROCESS FLOW



PLAN

Establish the ISMS

4. **Context and Organization**
- Define context
- How the organization meets needs/expectations of other parties
- Define scope of the ISMS

5. **Leadership**
- Have proper leadership and commitment
- write and approve security policies, roles and responsibilities

6. **Planning**
- defined information security objectives
- define plans to achieve objectives
- requires addressing risks and opportunities for your organization

DO

Implement and Operate the ISMS

7. **Support**
- Have right resources with the right level of competence
- ensure appropriate level of security awareness and training for all users

8. **Operation**
- Plan and control the security operations necessary to implement the ISMS
- Requires information security risk assessment and risk treatment

CHECK

Monitor and Review the ISMS

9. **Performance Evaluation**
- Monitor, analyze and evaluate the ISMS
- Conduct internal audits
- Management reviews of ISMS

ACT

Maintain and Improve the ISMS

10. **Improvement**
- Improvements must be made taking corrective actions
- Continual improvement processes must be implemented

ISO 27001 ANNEX A CONTROLS (HTTPS://WWW.ISMS.ONLINE/ISO-27001/ANNEX-A/)

Organizational

1. Policies for Information Security
2. Information Security Roles and responsibilities
3. Segregation of Duties
4. Management Responsibilities
5. Contact with Authorities
6. Contact with Special Interest Groups
7. Threat Intelligence
8. Information Security in Project Management
9. Inventory of Information and Other Associated Assets
10. Acceptable Use of Information and Other Associated Assets
11. Return of Assets
12. Classification of Information
13. Labelling of Information
14. Information transfer
15. Access Control
16. identity Management
17. Authentication Information
18. Access rights
19. Information Security in Supplier Relationships
20. Addressing Information Security Within Supplier Agreements
21. Managing Information Security in the ICT Supply Chain
22. Monitoring, Review and Change Management of Supplier Services
23. Information Security for Use of Cloud Services
24. Information Security Incident Management planning and Preparation
25. Assessment and Decision on Information Security Events
26. Response to Information Security Incidents
27. Learning from Information Security Incidents
28. Collection of Evidence
29. Information Security During Disruption
30. ICT Readiness for Business Continuity
31. Legal, Statutory, Regulatory and Contractual Requirements
32. Intellectual Property Rights
33. Protection of Records
34. Privacy and Protection of PII
35. Independent review of Information Security
36. Compliance with Policies, Rules and Standards for Information Security
37. Documented Operating Procedures

People

1. Screening
2. Terms and Conditions of Employment
3. Information Security Awareness, Education and training
4. Disciplinary Process
5. Responsibilities After termination or Change of Employment
6. Confidentiality or Non-Disclosure Agreements
7. Remote Working
8. Information Security Event Reporting

Physical

1. Physical Security Perimeters
2. Physical Entry
3. Security Offices, Rooms and Facilities
4. Physical Security Monitoring
5. Protecting Against Physical and Environmental Threats
6. Working In Secure Areas
7. Clear Desk and Clear Screen
8. Equipment Siting and Protection
9. Security of Assets Off-Premise
10. Storage Media
11. Supporting Utilities
12. Cabling Security
13. Equipment Maintenance
14. Secure Disposal or Re-Use of Equipment

Technical

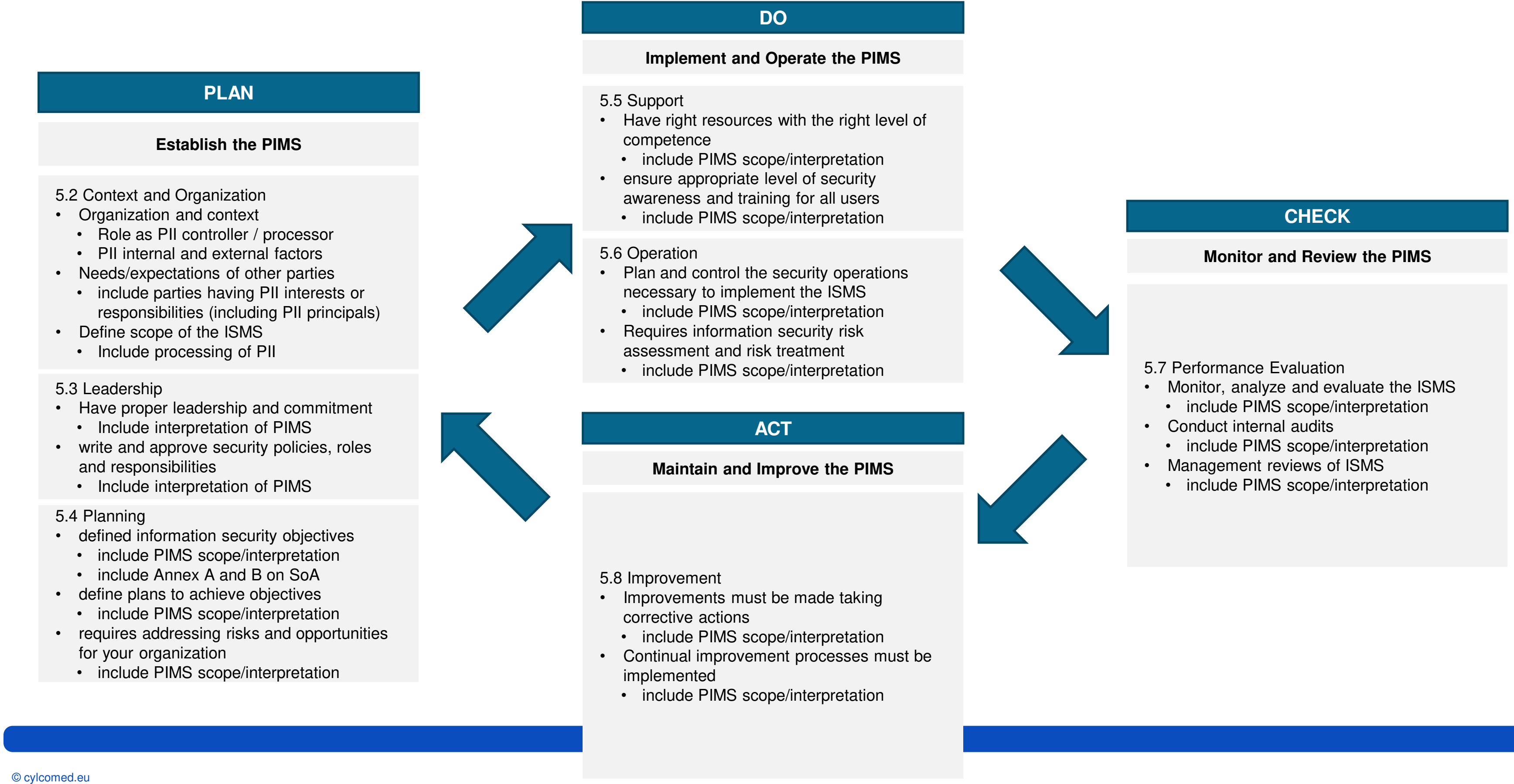
1. User Endpoint Devices
2. Privileged Access Rights
3. Information Access Restriction
4. Access to Source Code
5. Secure Authentication
6. Capacity Management
7. Protection Against Malware
8. Management of technical Vulnerabilities
9. Configuration Management
10. Information Deletion
11. Data Masking
12. Data Leakage Prevention
13. Information Backup
14. Redundancy of Information Processing Facilities
15. Logging
16. Monitoring Activities
17. Clock Synchronization
18. Use of Privileged Utility Programs
19. Installation of Software on Operational Systems
20. Networks Security
21. Security of Network Devices
22. Segregation of Networks
23. Web Filtering
24. Use of Cryptography
25. Secure Development Life Cycle
26. Application Security Requirements
27. Secure System Architecture and Engineering Principles
28. Secure Coding
29. Secure Testing in Development and Acceptance
30. Outsourced Development
31. Separation of Development, Test and Production Environments
32. Change Management
33. Test Information
34. Protection of Information Systems During Audit Testing

ISO/IEC 27701 – SECURITY TECHNIQUES – EXTENSION TO ISO/IEC 27001 AND ISO/IEC 27002 FOR PRIVACY INFORMATION MANAGEMENT – REQUIREMENTS AND GUIDELINES

ISO 27701 - SCOPE

- ISO 27701 extends the ISO 27001 standard for privacy information management. It specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS).
- It provides PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing.

FRAMEWORK ANALYSIS – ISO 27701:2022



PLAN

Establish the PIMS

5.2 Context and Organization
- Organization and context
  - Role as PII controller / processor
  - PII internal and external factors
- Needs/expectations of other parties
  - include parties having PII interests or responsibilities (including PII principals)
- Define scope of the ISMS
  - Include processing of PII

5.3 Leadership
- Have proper leadership and commitment
  - Include interpretation of PIMS
- write and approve security policies, roles and responsibilities
  - Include interpretation of PIMS

5.4 Planning
- defined information security objectives
  - include PIMS scope/interpretation
  - include Annex A and B on SoA
- define plans to achieve objectives
  - include PIMS scope/interpretation
- requires addressing risks and opportunities for your organization
  - include PIMS scope/interpretation

DO

Implement and Operate the PIMS

5.5 Support
- Have right resources with the right level of competence
  - include PIMS scope/interpretation
- ensure appropriate level of security awareness and training for all users
  - include PIMS scope/interpretation

5.6 Operation
- Plan and control the security operations necessary to implement the ISMS
  - include PIMS scope/interpretation
- Requires information security risk assessment and risk treatment
  - include PIMS scope/interpretation

CHECK

Monitor and Review the PIMS

5.7 Performance Evaluation
- Monitor, analyze and evaluate the ISMS
  - include PIMS scope/interpretation
- Conduct internal audits
  - include PIMS scope/interpretation
- Management reviews of ISMS
  - include PIMS scope/interpretation

ACT

Maintain and Improve the PIMS

5.8 Improvement
- Improvements must be made taking corrective actions
  - include PIMS scope/interpretation
- Continual improvement processes must be implemented
  - include PIMS scope/interpretation

ISO 27701 ANNEX A CONTROLS – PII CONTROLLERS AND PROCESSORS

CYLCOMED

	PII Controller	PII Processor
Conditions for collection and processing	1. Identify and document purpose 2. Identify lawful basis 3. Determine when and how consent is to be obtained 4. Obtain and record consent 5. Privacy impact assessment 6. Contractors with PII processors 7. Joint PII controller 8. Records related to processing PII	1. Customer agreement 2. Organization’s purposes 3. Marketing and advertising use 4. Infringing instruction 5. Customer obligations 6. Records related to processing PII
Obligations to PII principals	1. Determine and fulfilling obligations to PII principals 2. Determine information for PII principals 3. Providing information to PII principals 4. Providing mechanism to modify or withdraw consent 5. Providing mechanism to object to PII processing 6. Access, correction and/or erasure 7. PII controllers’ obligations to inform third parties 8. Providing copy of PII processed 9. Handling requests 10. Automated decision making	1. Obligations to PII principals
Privacy by design and privacy by default	1. Limit collection 2. Limit processing 3. Accuracy and quality 4. PII minimization objectives 5. PII de-identification and deletion at the end of processing 6. Temporary files 7. retention 8. Disposal 9. PII transmission controls	1. Temporary files 2. Return, transfer or disposal of PII 3. PII transmission controls
PII sharing, transfer and disclosure	1. Identify basis for PII transfer between jurisdictions 2. Countries and international organizations to which PII can be transferred 3. Records of transfer of PII 4. Records of PII disclosure to third parties	1. Basis for PII transfer between jurisdictions 2. Countries and international organizations to which PII can be transferred 3. Records of PII disclosure to third parties 4. Notification of PII disclosure requests 5. Legally binding PII disclosures 6. Disclosure of sub-contractors used to process PII 7. Engagement of a subcontractor to process PII 8. Change of subcontractor to process PII

Q & A

CYLCOMED

THANK YOU FOR YOUR ATTENTION

cylcomed.eu

Funded by
the European Union

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI