anDREa Risks

R001: Data breaches

Without clear policies in place, employees may not know how to handle sensitive information properly, which could increase the risk of data breaches.

R002: Compliance issues

The organization are required to adhere to various laws and regulations that govern the handling of sensitive information. Without proper policies in place, it is impossible for the organization to demonstrate compliance with these regulations.

R003: Reputation damage

A data breach or compliance issue can damage the organization's reputation, which could lead to a loss of trust from customers, clients, and other stakeholders.

R004: Financial losses

Data breaches and compliance issues can also result in financial losses, such as fines, legal fees, and lost business.

R005: Outdated policies

Information security policies should be reviewed and updated regularly to ensure that they reflect the current threats, vulnerabilities, and regulatory landscape. If the policies are not reviewed periodically, they may become outdated and may not effectively address the organization's current risks.

R006: Non-compliance

Failing to review and update policies can also lead to non-compliance with laws and regulations that govern the handling of sensitive information. This can result in fines, legal consequences, and damage to the organization's reputation.

R007: Increased risk of data breaches

Outdated policies may not adequately address current threats and vulnerabilities, which could increase the risk of data breaches.

R008: Decreased employee awareness

Periodically reviewing and updating policies helps to ensure that employees are aware of the current information security requirements and are trained to follow them. If policies are not reviewed regularly, employees may not be aware of the latest requirements, which could lead to mistakes and increase the risk of data breaches.

R009: Decreased employee engagement

Employees who are unsure of their responsibilities or do not have the necessary resources to fulfill their responsibilities may become disengaged and less productive.

R010: Processes incorrect or not executed

Incorrectly defined and allocated responsibilities can lead to confusion and inefficiencies, as employees may not know who is responsible for certain tasks or may duplicate work.

R011: Non authorized people or processes gain access via devices used for work.

Devices used for work can be used by non-authorized people or processes to gain access.

R012: Devices for work used in uncontrolled/unknown work environments

Uncontrolled/unknown work environments can provide opportunity for unauthorized people or processes to gain access.

R013: Employees with a history that conflicts with information security profile needed

People with a conflicting history might not fit the profile to comply to the policies and procedures.

R014: Employees not sufficiently aware of their duties

When people do not know what they can and cannot do, unintentionally or in good faith the information security objectives can be compromised.

R015: Employees not willing to comply

People not willing to comply, are a risk to the organization's information security objectives.

R016: Employees leaving the organization have access to the organization's assets or information.

People no longer part of the organization should not have access to the organization's assets and information.

R017: Incorrect handling of security incidents

Security incidents can have a significant impact on several stakeholders. Incorrect handling of a security incident aggrevates the problem and in potential more than the incident itself.

R018: Supplier works in a not sufficient compliant way

During the creation/delivery the supplier exposes the organization to unnecessary risks.

R019: Supplier delivers results that are not sufficiently compliant or does not deliver in accordance to the contract

Incorrect working products pose a risk and can result in extra costs and time to go to production.

R020: Insufficient priority, attention, or means to ensure the required level of the ISMS

When ISMS, including all required resources and personall, is not sufficiently embeded in the organization without sufficient redudancy, detoriation can go unnoticed, or the organization might be faced suddently with insufficient operating ISMS.

R021: Unauthorized access

If access controls are not properly implemented or enforced, unauthorized individuals may be able to access sensitive information assets, potentially leading to data breaches or other security incidents.

R022: Insider threat

Insiders with access to sensitive information assets, such as employees or contractors, may pose a risk if they misuse their privileges or disclose information without authorization

R023: Lack of accountability

If access controls are not properly documented or audited, it may be difficult to determine who has accessed specific information assets and when, potentially leading to a lack of accountability in the event of a security incident.

R024: Technical vulnerabilities

Access controls may be bypassed if they are not implemented or maintained properly, potentially leading to security vulnerabilities.

R025: Key management

If keys used for cryptography are not properly managed, it may be possible for unauthorized individuals to access encrypted information. This could include risks such as key loss, theft, or improper key distribution.

R026: Implementation vulnerabilities

Cryptographic algorithms may have vulnerabilities that could be exploited by attackers, potentially leading to the compromise of encrypted information.

R027: Algorithmic vulnerabilities

If cryptographic controls are not properly implemented, it may be possible for attackers to bypass them and access encrypted information.

R028: Legal and regulatory compliance

Some cryptographic controls may be subject to legal or regulatory requirements, and non-compliance with these requirements could result in legal or financial risks for the organization.

R029: Lack of security testing

If systems are not adequately tested for security vulnerabilities, it may be possible for attackers to exploit those vulnerabilities, potentially leading to security breaches.

R030: Vulnerabilities in new systems

New systems may have vulnerabilities that are not yet known or that have not yet been addressed, potentially leading to security breaches.

R031: Unauthorized changes

If changes are not properly controlled, it may be possible for unauthorized individuals to make changes to information systems or other assets, potentially leading to security breaches or operational disruptions.

R032: Lack of visibility

If assets are not properly tracked and monitored, it may be difficult to determine their location, status, or value, potentially leading to operational disruptions or financial losses.

R033: Lack of accountability for assets

When people do not know what they can and cannot do, unintentionally or in good faith the information security objectives can be compromised.

R034: Inconsistent classification

If information is classified inconsistently, it may be difficult to determine the appropriate controls and handling procedures, potentially leading to security breaches or other incidents

R035: Operational disruption

If equipment is not properly maintained, it may disrupt normal operations, potentially leading to financial losses or reputational damage

R036: Loss of information

Loss of information can lead to various other risks, including financial losses. reputation damage and others. A distinction exists between primary data sources and supportive data sources (backups, snapshots).

R037: Delayed incident response

A delayed incident response can lead to various other risks, including loss of information, legal compliancy issues and reputation damage.

R038: Unsecure network

If there are insufficient procedures and security measures for networks, there is a risk of unauthorized access to information via the network.
Namely:
- maintaining services and management requirements for networks.
- separation of networks.
- network routing.
- identification of network equipment.
- protection of diagnosis and configuration ports.

R039: Unsafe transport of information and unsafe access to information in application services via network

If there are no policies, procedures, and measures to protect information that is being transported, exchanged, and accessed through application services, there is a risk of unauthorized access to information. Namely:
- rules procedures and measures.
- protection of information with regard to online transactions and e-commerce.
- agreements with external parties on information exchange.
- protection of information in messages.
- concluding confidentiality and confidentiality agreements.
- security of information on public networks.

R040: Insecure development of (unsafe) software

If no policies and procedures have been implemented for software development, there is a risk that software will not work according to requirements. This concerns the following:
- change management procedures.
- change management for operating platforms (OS).
- possibly: limitation of changes to software.
- development of secure systems (security by design).
- secure development and use of mobile code.
- security development and test environment, including the protection of test data.
- test procedures based on established acceptance criteria.
- test procedures, including
system security testing.
- OTAP environments.

R041: Insufficient continuity Security Officer

If the Security Officer is no longer able to perform his duties (planned or unplanned), there is a risk that the schedule of the ISMS will no longer be followed and the organization runs the risk of no longer being compliant with the information security standard and legislation.

R042: Insufficient measures against malicious software

If no proper security measures have been taken and rules of conduct have been implemented against malicious software, then there is a risk of damage to information and business operations.

R043: Adding incorrect user during Workspace creation

Adding an incorrect Accountable or Privileged Member during Workspace creation could lead to unauthorized access to data, data breaches and security incidents

R044: Lack of automation leading to human errors

Without automation, resources can be deleted which should not be deleted.

R045: Authorized users are unable to execute the necessary action

If authorized users are unable to perform the required action, there is a risk of significant data loss, which could have critical implications for users. It is imperative to mitigate this risk by ensuring that users have the necessary capabilities to manage and safeguard their data effectively.

R046: Downtime Entra ID

Downtime of the Entra ID can lead to authentication failures and inaccessibility of cloud services including myDRE

R047: Data center destruction

Destruction of the Microsoft West Europe Data Center in Amsterdam is catastrophic for myDRE. In anDREa Information Security Strategy this is outside Boundary of Reasonable Preparedness.

R048: Redundancy

If there is not enough redundancy, important processes might get disrupted.

R049: Platform or VM unavailability

Faulty updates can lead to platform or VM unavailability

R050: Application changes

Changes, especially undocumented/uninformed changes, in an application can confuse people and result in entry mistakes.

R051: Incorrect or incomplete reporting

Decisions can be made on incorrect or incomplete information and/or demonstration of compliance is not sufficiently correct

R052: Secret Management

Secrets and Service Principal credentials are used by client applications to authenticate against Azure resources. These credentials have a fixed validity period and must be rotated before expiry to prevent authentication failures.