University of
Bedfordshire

Unit title and code: Information Governance and Compliance CIS102-6

Assignment title: Assignment – Information Governance Policy for the Deep-Engineering & Co company

Group Number: 03

Group Leader: Mohammad Omar Faysel Student ID: 2338591
Group Member: Hasan Farooq Student ID: 2103875
Group Member: Ademola Babatunde Sulaimon. Student ID: 2413934
Group Member: Valentin Ceptureanu Student ID:2012010
Group Member: Fatoba Oluwapelumi Student ID: 2333318

Peer review form of the weight in Group Work

Group Number: 03

Student Name	SID	Contribution %	
Mohammad Omar Faysel	2338591	100%	
Hasan Farooq	2103875	100%	
Ademola Babatunde	2413934	100%	
Valentin Ceptureanu	2012010	100%	
Fatoba Oluwapelumi	2333318	100%	

Table of Contents

List of Figure

1.Introduction.

Knowledge forms the basic vital resource whose protection needs to be laid down in the digitalised modern world. Based in Oxford, DeepEngineering & Co. is the highest rated when it comes to security compliance data. According to Internet Society (2023), the guiding principle of this policy is to protect the confidentiality, integrity, and availability (CIA) of user data from online threats, provide for compliance with legal and regulatory issues mainly Regulation on Data Protection (GDPR), and give a strong foundation for information management.

1.1 Importance of Information Governance.

Information governance is super important for Deep Engineering and Co. Because it helps build trust with all sorts of important people, like customers and stake holders. Effective information governance enhances that the organization remains proactive in addressing potential threats. It is about cultivating a culture of security and accountability, the company can maintain its reputation and protect its assets. (UK Data Service, 2021)

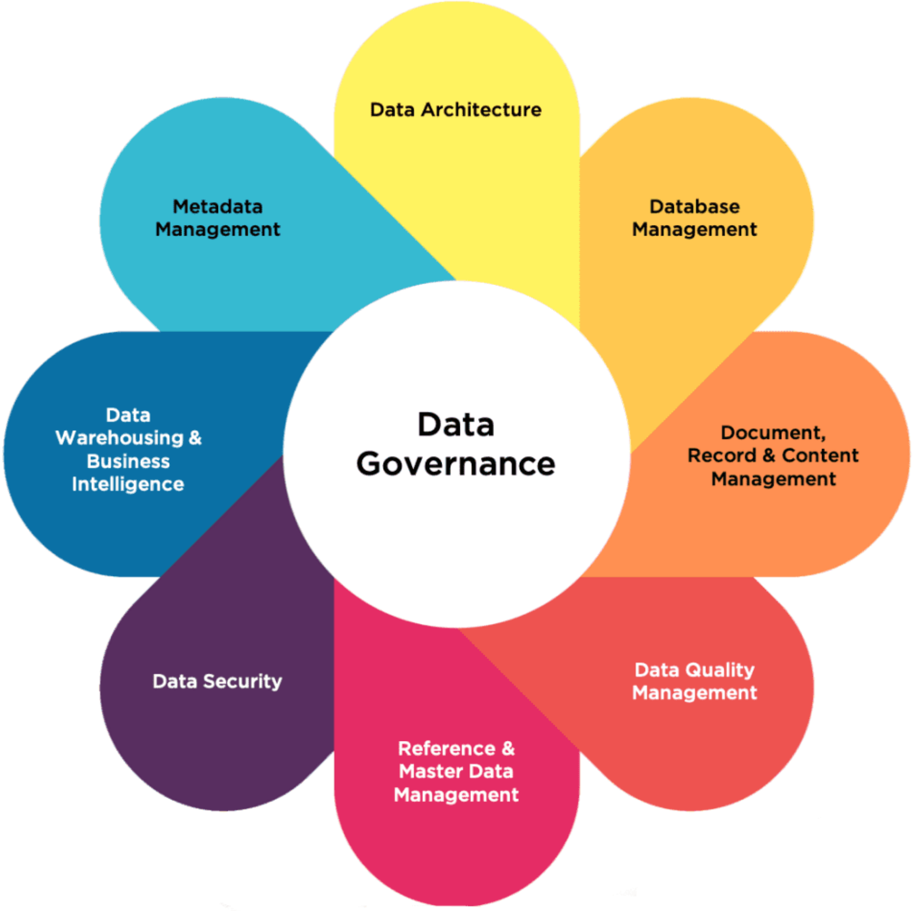
Data Architecture
Database Management
Document, Record & Content Management
Data Quality Management
Reference & Master Data Management
Data Security
Data Warehousing & Business Intelligence
Metadata Management
Data Governance

Figure 1: Data Governance Source (Mitratech, 2023)

1.2 Scope.

This policy applies to any persons that interface with Deep-Engineering & Co. information assets: that is, employees, third parties, contractors, or any others who might possibly access such information. It reflects the information management of data classification, storage, access, and procedures that constitute its handling. Whereby ensuring understanding of responsibilities in well-established guidelines, such as that third-party contractors accessing AWS servers must implement multi-factor authentication (MFA) like in-house engineers do(Improvado 2024).

2. Information Governance Framework

An information governance (IG) framework gives organisations a structured approach to manage their information assets in a way that will ensure security, compliance, efficiency and integrity, if followed effectively. An IG framework contains many policies, processes and procedures that can help Deep-Engineering & co effectively handle data while staying in-line with their business and legal requirements, (Smallwood, 2014). Which is why it is so crucial for an organization like Deep-Engineering & co to follow an IG framework.

2.1. ISO/IEC 27001

ISO 27001 Information Government (IG) Framework, published by the international organization and published by the International Electrotechnical Commission provides the risk -based agent to increase the information security management system (Edwards, 2024) in the organization. A main principle for this approach is adaptation to the CIA framework: All information is the privacy, integrity and availability of all information, which promotes secure data management. Deep construction and co use these benefits only to limit data access to authorized persons, keep this data as accurate as possible, and ensure accessibility if necessary (Anon., 2024). ISO will support certification according to 27001 and ensure that GDPR is completed. GDPR aims to protect the privacy of user data and impose heavy fines for fractures (GDPR.EU, 2020). UK Data Protection Act also requires audio data management, obligations, which will follow deep engineering subjects such as the British -based company (Gov.UK, 2018). Therefore, the principles that have been adopted to increase the integrity of data security, compliance and commercial integrity of deep engineering subjects are considered.

2.1.1. Key Focus Area

Leadership and Commitment

ISO 27001 supports Deep-Engineering & Co's top management in giving strong guidance as well as support to an effective Information Security Management System (ISMS). Leadership shall align security objectives with business goals so that there is a maximum level of security.

Risk Management

The framework strengthens risk management by forcing Deep-Engineering & Co to categorize its data depending on the degree of sensitivity and danger it holds, same as concerning what security measures it needs to put in place (Lee, 2020). Such proactive work can dramatically decrease our exposure and vulnerability, hence increasing protection toward data.

Security Controls

In ISO 27001's Annex A controls, policy and procedure exist to fortify security, with access granting or denying permission to perform actions on files. This action prevents insider threats and complements the principles of the Zero Trust Security Policy (Wright, 2024).

Compliance with Legal and Regulatory Requirements

ISO 27001 audits in regular intervals sufficiently assure compliance with GDPR, HIPAA, PCI-DSS, among other regulations. Compliance deters legal penalty actions and protects customer data, hence important for Deep-Engineering & Co's reputation and operational integrity.

Continuous Improvement through the PDCA Model
The **Plan-Do-Check-Act (PDCA) model** ensures continuous improvement:

- Assuming: Develop security control, guidelines and compliance goals.
- Check: Monitor performance through revision and assessment.
- ACT: Improvements brought in per audit (ISO Council, 2024).

By using this approach, deep-engineering & co can increase security, take measures against data violations and increase the compliance with regulations. While ISO 27001 is an excellent structure, other information management models also provide benefits, which will be detected in the next part**.**

2.2. Alternative Frameworks

ISO-27001 is not the only information governance framework, there many others that are made that prioritise different aspects of an organisation and their priorities. The table below compares the most prominent information governance framework

	Purpose	**Scope**	**Focus Area**	**Best For**
ISO-27001	Implementing an Information Security Management	Structured Framework with strict compliance and requirements	Prioritising ISMS and security controls	Organisations who want strict and structured security compliance

NIST Cybersecurity Framework	Helping with an organisation's cybersecurity risk management	Flexible, adaptable framework	IT strategy, risk, and performance	Organisations who want to improve risk and security posture
COBIT	Gives a more holistic outline on how to govern/manage IT in general	Overlooks enterprise IT with aligning an organisation's practice with its business goals	IT strategy, risk, and performance	Organizations needing a comprehensive IT governance framework

As shown in the table above these are the most prominent information governance framework that Deep-Engineering can use. For example, instead of the ISO 27001, Deep-Engineering & Co can use the NIST cybersecurity framework (CF) as their information-governance framework. They can benefit from NIST CF's concentration on risk management which can improve the companies cybersecurity posture furthermore, unlike the ISO 27001 which has strict requirements/compliance, the NIST CF is more flexible which can help Deep-Engineering in implementing the framework as they can align the framework to work with the companies culture and they are allowed to drop some aspects of the framework and follow others, (Roy, 2020). Moreover, instead of the NIST CF, Deep-Engineering & Co can use the 'Control Objectives for Information and Related Technologies' (COBIT), which is an Information governance that focuses on the entire IT sector of the organisation. The framework also ensures that the organisation's IT practices align with their business goals, risk strategy and IT security. Deep-Engineering & Co can benefit from the COBIT framework as they would receive guidance broader than just data handling practices, (De Haes, 2020).

However, with, the recommendation for Deep-Engineering is to go ahead with the ISO-27001 framework, because we believe this framework is best suited for them. This is because Deep-Engineering & Co have confirmed the need for a robust and strong policy to adhere to requirements and regulations like the Data Protection 2018 Act, furthermore it is a priority for Deep-Engineering & Co to ensures that their user's data has integrity, that it maintains its confidentiality and availability. All of these principles that Deep-Engineering want to achieve is provided by ISO-27001 by its strict and structured policies, with the framework also aligning with the CIA triad, ISO 27001 out of the other IG frameworks aligns with the goals of Deep-Engineering for the reasons mentioned throughout this section.

3. Roles and Responsibilities.

3.1 Who is Responsible.

- The CISO executes the strategic enclosure of the information security policy. He/she measures the alignment of policy directives with the strategic objectives of the organization and augurs if all necessary resources have been accorded priority for satisfactory implementation (IBM, 2022).
- The DPO ensures the agency is compliant with all conditions of the GDPR, controls data processing activities for the agency, and serves as the contact person for all data subjects and authorities on data protection (SANS Institute, 2022).
- Employees. All employees are responsible for adhering to the information security policy and handling data in accordance with established guidelines. They must be aware of their responsibilities and report any security incident or concerns (Cybersecurity Ventures, 2022).
- IT Staff. The IT staff implements and maintains the technical controls required to protect the organization information assets, ensuring that all systems and networks are secure

3.2 Accountability.

To establish and maintain accountability, Deep-Engineering & Co. has determined its clear lines of responsibility and authority. Every role is defined in its responsibilities and has accountability for the actions taken. Regular training and awareness programs have been initiated by the organization that involves educating people on their responsibilities as well as the importance of information governance. Other means of monitoring compliance with the internal policy and the effectiveness include the use of key performance indicators (KPIs) and periodic audits. For example, 95% of employees are required to undergo annual GDPR training, and annual penetration tests are conducted for system security purposes (Information Governance Initiative, 2022).

3.3. Detailed Explanation of Roles and Responsibilities.

3.3.1 Chief Information Security Officer (CISO).

It's a pivotal point of information security strategy within the organization, with high levels of responsibility for the general development, preparation, and implementation of security policies and procedures following industry best practices and regulatory requirements. Among those responsibilities, the CISO must ensure that the organization is provided with the necessary resources and support to protect itself at all times plausibly. Such resources and support require, on a proactive basis, regular reviews and updates of security policies, risk assessments, and incident responsiveness (IBM, 2022).

3.3.2 Data Protection Officer (DPO).

The DPO is the most important person when it comes to guaranteeing compliance with the GDPR. The DPO shall monitor the organizations, ensuring that all data processes are compliant with GDPR regulations. The DPO acts as a contact point for the data subject, where the data subject can seek guidance and support regarding any aspect of data protection. The DPO shall also liaise with regulatory authorities to ensure that the organization fulfills all obligations under the GDPR.

3.3.3 Employees.

Every employee carries an important function in the protection of the organization. Employees are responsible for followingwhenb function security policies and procedures to safeguard data in such a way that confidentiality, integrity, and availability are preserved. Regular training and awareness programs intend to ensure that employees are equally well-informed about their responsibilities to information security.

3.3.4 IT Staff.

The IT staff is responsible for implementing and maintaining the technical controls that protect the organization information assets. This includes ensuring that all systems and networks are secure, implementing access controls, and conducting regular security audits. The IT staff must also prepare to respond to security incidents, ensuring that any breaches are contained and mitigated as quickly as possible (TechTarget, 2022).

3.4 GDPR Specifics.

Deep-Engineering & Co. Is committed to adhering to the core principles of GDPR, including data minimization, accuracy and accountability. The organization will implement measures to ensure that only the necessary data is collected and processed, and that all data is kept accurate and up to date. Additionally, the organization will maintain a comprehensive record of data processing activities and conduct regular audits to ensure compliance with GDPR requirements. (GDPR, 2018).

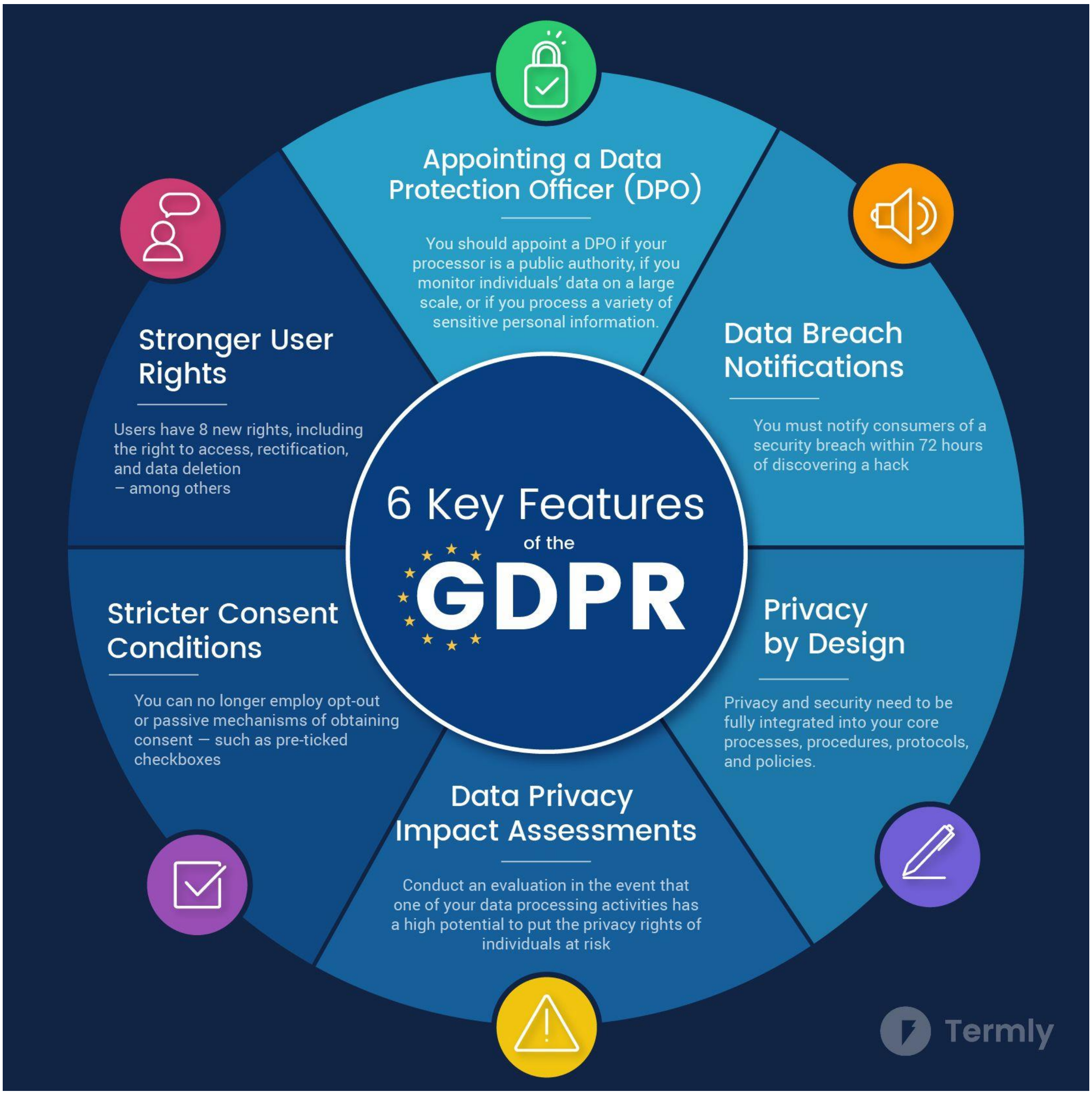
Appointing a Data Protection Officer (DPO)
You should appoint a DPO if your processor is a public authority, if you monitor individuals' data on a large scale, or if you process a variety of sensitive personal information.
Data Breach Notifications
You must notify consumers of a security breach within 72 hours of discovering a hack
Privacy by Design
Privacy and security need to be fully integrated into your core processes, procedures, protocols, and policies.
Data Privacy Impact Assessments
Conduct an evaluation in the event that one of your data processing activities has a high potential to put the privacy rights of individuals at risk
Stricter Consent Conditions
You can no longer employ opt-out or passive mechanisms of obtaining consent — such as pre-ticked checkboxes
Stronger User Rights
Users have 8 new rights, including the right to access, rectification, and data deletion – among others
6 Key Features
of the
GDPR
Termly

Figure 2: GDPR. Source. (Pinterest, n.d.)

3.5 Risk Management Strategies.

In order to obtain a better cybersecurity focus, Deep-Engineering & Co. will develop a general risk management strategy. Identification of potential risks, periodic assessments, and coming up with plan can adequately and competently address all these risks. The organization will also conduct annual penetrations test against its system and networks, looking for vulnerabilities to be disclosed and adequately dealt with (ISO/IEC, 2024).

3.6 Conclusion.

Effective information management is important for Deep Engineering & Company to maintain its good name and protect the property. The organization will be ahead of the curve when it comes to addressing the potential threats by assuming clear roles and responsibilities and ensuring that all individuals maintain a safe environment. Regular training, consciousness programs and auditing are all important to ensure compliance with various legal and government requirements, especially GDPR. By doing this, a strong culture of deep engineering science and co.plant security protects and accountability and effective information.

4. Data Classification & Handling Policy

The data classification and handling policy within ISO-27001 is implemented by Deep-Engineering to assess risks that certain data may face, which will assist in the classification and protection of such data. With this policy, resources will be allocated more effectively in protecting valuable data-assets.

4.1. Classification Tiers

This policy recommends that the first step of implementing such a policy is to classify data into tiers, this will help Deep-Engineering evaluate their most 'prized assets', these classification tiers are:

- **Public Data:** Easily accessible by anyone (i.e. Website)
- **Internal Data:** Data meant for the company only
- **Confidential Data:** Business-Critical (i.e. financial records, contracts)
- **Restricted Data:** Very confidential, strict access control (i.e. Customer PII, Medical Records)

The implementation of this step will help Deep-Engineering Clearly see what is the most valuable assets that they have within their organisations along with other assets, which is why this classification step is important for the policy to be effective, (HighTable, 2022).

4.2. Data Handling Procedures

Within the data policy of the ISO 27001 framework, ISO recommend procedures that will ensure that all phases of data-handling including: data-at-rest, data-in-transit and the disposal of data is all done with confidentiality and integrity of the data in mind, (Lopes, 2019).

ISO recommends a plethora of procedures within this policy that organisations can implement, which will help them instil confidentiality and integrity within their data. Some of these procedures are:

Encryption - for data at rest and in transit, it will turn confidential data into ciphertext which is hard to read and decipher, which instils confidentiality and helps protect data from unauthorized users

Access Control – Fundamental principle that allows an organization to dictate rights of a user's ability to write, read or execute files and there are different types of access controls

Hash Functions – this is a mathematical function that accepts an input (user data) and outputs a fixed length digest (a mixture of characters and numbers) this is a great way of organisations to instil integrity because the functions output will change if file has been changes.

These are some of the procedures ISO recommends along with many others that are well documented in this data policy, that will help Deep-Engineering & co handle their sensitive data with compliance and security, (Achmadi, 2018).

4.3. Data Retention & Disposal Policy

Another Important Aspect of the Data Policy is the retention and disposal of specific data, i.e. user data, that Deep-Engineering & Co possess. ISO outlines in the 27001 framework that standards like the GDPR act and the Data Protection Act 2018, have a ruling on how long an organisation can keep hold on specific data before they need to dispose of such data. For example, the Data protection act 2018, which is the most relevant to Deep-Engineering & Co, because of their location, outlines that personal data must have a retention period. More specifically, the act outlines that 'personal data shall be kept for no longer than is necessary for the purposes for which the personal data are processed', (HM Revenue & Customs, 2023). This means that it will be in Deep-Engineering's best interest to abide with the data retention & disposal policy to avoid facing harsh penalties, moreover, it will help them avoid any potential data leaks and internal attacks as well, which is a major plus for Deep-Engineering & Co.

5. Compliance and Legal Considerations

5.1. GDPR Requirement Under ISO/IEC 27001

- The implementation of the ISO 27001 framework in Deep-Engineering & CO establishes compliance with GDPR and other industry standards. ISO 27001 provides a structured data security approach and allows compliance with GDPR requirements, including design, risk management, access control, encryption, events, events and data protection by continuous monitoring, which effectively protect individual information.

- Lawful processing: ISO/IEC 27001 assists in the lawful processing since it entails an ISMS where data protection policies are integrated regarding how they allow the legal collection, utilization, and storage of data (ICO, 2018).

- Rights of the data subject: GDPR simplifies and strengthens the rights of the data subject which include the right of access, right of rectification, right of erasure, and right to object. These rights are supported by access control and audit trail which assists in tracking and regulating who has the privilege of accessing personal data and for what reason (Edwards, M., 2017).

- Data Breaches: The GDPR further demands that data breaches be notified within seventy-two hours from the time it was discovered. ISO/IEC 27001 aids in swift identification and reporting of breaches concerning incidents in the ISMS structure (GDPR, 2018).

- Data Protection by Design and by Default: ISO/IEC 27001 also addresses data protection from the time of designing systems and processes for handling data; this is in compliance with the GDPR requirements. This is done through effectiveness and efficiency in risk assessments and use of suitable technical and organizational measures to protect data (DPC, 2018).

5.2. Industry-Specific Regulations

Deep-Engineering & Co must also adhere to the following industry standards:

- The NIS Directive mandates digital sector organizations to implement security measures and report severe cyberattacks, while ISO/IEC 27001 provides risk management controls aligning with NIS requirements for disruption prevention.
- ISO/IEC 27001: Designed for worldwide information security management, it offers a structure for best practices in information security management and enables companies to manage and safeguard their data resources so as they remain safe and secure.

6. Risk Assessment and Management Using NIST Framework

NIST RMF provides a thorough, flexible, methodical approach for including security into information systems all through the lifetime. It is very important for industries handling private information and needing strict compliance to strict legal standards. The dynamic nature of cyber risks calls especially for NIST RMF's emphasis on ongoing monitoring and real-time risk management (NIST, 2018).

6.1. Comparison with ISO 31000 and FAIR

- ISO 31000: offers general, high-level recommendations for risk control relevant in many different fields. It is less fit for ICT-oriented companies handling complex cybersecurity issues since it lacks the particular attention to information security that NIST RMF addresses.

- FAIR: Factor analysis of information risk, or FAIR, examines operational risk and cybersecurity numerically. FAIR concentrates mostly on the quantification and financial consequences of risks, so it is complementary but not a replacement for the procedural strengths of NIST RMF. Unlike NIST RMF, which offers a standardized set of procedures and integrates security measures.

6.2. Potential Risks for Deep-Engineering & Co

Some of the risks that must be considered when creating the ISO/IEC 27001 policy:

- Data Theft: Often, organizations encounter data breaches that arise from unauthorized access to private information and may result in direct monetary or credibility loss. This is especially an issue because personal information of users might be put out there in the public domain.

- Insider threats: The employees or the contractors privy to the company's programs or possessing access rights to the company's networks may leverage their access to sneak data.

- Cyber Threats: include attacks by hacking, phishing, ransomware or DDoS attacks are some of the most dangerous attacks since they pose a risk to the integrity and cause operations to be disturbed.

6.3. Risk Mitigation, Monitoring Strategies and Continuous Improvement

Data Breaches:

- Encryption and Data Masking: Encrypt the data both stored and in transit implementing access restrictions to allow only approved personnel to get access to such information. Help to guard data at rest and in transit therefore stopping unwanted access (Lord N. , 2023).
- Security Assessment: Conduct penetration testing and security audits to see to it that systems are defended from every kind of assault (CybSafe, 2023).

Insider Threats:

- Activity Tracking: Implement solutions that track the user activity and alert in case of suspicious activity recognized in the network.
- Security Awareness: Implementation of training sessions to ensure that all employees are in the best position and informed when it comes to security measures and the need to protect sensitive information (admin, 2024).
- Access Control and User Authentication: Strict access rules and multi-factor authentication help to limit data access depending on user roles and responsibilities (Rapid7, 2020).

Cyberattacks:

- Advanced firewalls and intrusion detection systems (IDS): to ensure that the network is not attacked or infiltrated by an intruder.
- Constant Monitoring and Vulnerability Assessment: Using automated techniques to track network traffic and routinely evaluate the system for vulnerabilities, help to ensure constant monitoring and vulnerability assessment (Etheridge, E., 2024).
- Incident Response Plan: Formulate and periodically update the incident response plan to enable handling of a cyber attack while minimizing its implications. Create a strategy to address security concerns in the company.

7. E-Report on Information Governance for Deep-Engineering & Co

Protecting sensitive assets and ensuring GDPR compliance at Deep-Engineering & Co relies on strong data security and cybersecurity. This section presents the vital security measures and incident response strategies designed to minimize cyber risks.

7.1. Section 1: Data Security & Cybersecurity Measures

7.1.1 Security Controls

To fortify defences against cyber threats, Deep-Engineering & Co will employ a multi-layered security approach. This includes:

- **Encryption**: All sensitive data, whether stored or transmitted, will be protected with strong encryption standards such as AES256 and TLS 1.2/1.3. Internal communication will use end-to-end encryption (E2EE). There will be also a concerned emphasis on Internal Communication.
- **Access Control**: Deep-Engineering & Co will manage access based on Role-Based Access Control (RBAC), where employees will have permissions only related to their jobs. Access to the sensitive systems will, however, be limited by the implementation of the Principle of Least Privilege PoLP.
- **Firewalls and IDS/IPS**: All the next-generation firewalls (NGFWs) will be implemented to monitor and control network traffic, while intrusion detection/intrusion protection systems (IDS/IPS) shall be used for detecting and responding to network activities in real time.
- **Endpoint protection and patching**: Endpoint security software will be in place on all the company devices, with reviews in place to automate software updates and security patches to reduce vulnerabilities.
- **Multi-Factor Authentication**: Multi-Factor Authentication (MFA), an additional login step, will be applied for any company employees who log in remotely or with administrative or privileged access. Examples of this will include biometrics, One Time Passwords (OTPs), and security tokens. Secure
- **Backups**: Regular backups of critical data will be held online and offline. The immutable backup policy will be implemented to protect against ransomware. Testing will also be performed regularly on restoration procedures.

7.1.2 Incident Response Procedures

Deep-Engineering & Co. will maintain a well-defined incident response plan to effectively manage cybersecurity incidents. This plan includes the following key stages:

- **Incident Identification and Reporting:**
  - Employees will report instances through the central system.
  - Monitoring and contextual analysis of potential threats shall be in charge of a Cybersecurity Incident Response Team (CIRT).
- **Containment and Mitigation:**
  - Actions to contain incidents are immediate, containing for instance isolation of affected systems.
  - A data breach, will notify affected individuals and, authorities as required by GDPR Article 33.

- **Investigation and Root Cause Analysis:**
  - Forensic examination shall examine the evidence to identify the cause of incidents.
  - The log files and any audit trail that might be available will be saved and preserved for all future use if there comes a legal and compliance need.
- **Recovery and Restoration:**
  - Systems will be restored from secure backups.
  - Compromised credentials will be revoked, and security measures strengthened.
- **Post-Incident Review and Policy Updates:**
  - Post-incident analyses will identify areas for security improvement.
  - Security policies will be updated based on lessons learned.

By adhering to these security controls and incident response procedures, Deep-Engineering & Co. will strengthen its cybersecurity posture and ensure compliance with GDPR, ISO 27001, and the NIST Cybersecurity Framework.

7. Section 2: Training & Awareness

To cultivate a security-conscious culture and minimize human error, Deep-Engineering & Co. will implement a comprehensive training and awareness program.

7.2.1 Employee Training on Data Handling and Cybersecurity

- **Data Protection and GDPR Compliance:** Employees will be trained on GDPR principles and the secure handling of Personally Identifiable Information (PII).
- **Secure Remote Work Practices:** Guidelines will be provided for secure VPN usage and avoiding public Wi-Fi for work tasks.
- **Strong Passwords and Authentication:** Robust password policies (minimum 12 characters, password managers, periodic changes) and the use of passphrases will be enforced.
- **Cybersecurity Awareness:** Employees will be educated on common cyber threats (phishing, malware, insider threats) and participate in simulated phishing campaigns.

7.2.2 Regular Audits and Compliance Checks

- **Security Audits and Penetration Testing:** Annual penetration testing, vulnerability assessments, and SIEM-based log monitoring will be conducted.
- **Compliance Checks and Internal Reviews:** Periodic GDPR compliance audits and security awareness training assessments will be performed.
- **Third-Party Security Assessments:** Vendors and third-party providers will be regularly audited for compliance with ISO 27001 and NIST standards.
- **Continuous Improvement and Policy Updates:** Lessons from incidents will be incorporated into policy refinements, and training content will be updated annually.

7.2.3 Ethical Responsibilities and Duty of Care

- A zero-trust mindset will be promoted regarding sensitive data.
- Corporate responsibility in protecting customer data will be emphasized.
- Clear disciplinary actions will be implemented for policy violations.

Conclusion

Deep-Engineering & Co. will establish a robust information governance framework aligned with ISO 27001, NIST, and GDPR to effectively mitigate cybersecurity risks. This will be achieved through rigorous security controls, a structured incident response plan, and a cybersecurity-aware workforce."

8. Problem-Solving in Cybersecurity: Application to a Specific Case

Case Study: Data Breach at Deep-Engineering & Co

Scenario: Due to a series of chain events since the incident, a phishing attack led to unauthorized access of sensitive customer data. Customer data, including personally identifiable information (PII), is hence exposed. It is a symptom of a broader problem for the field of cybersecurity: namely, human error; the problem of information governance policies that are simply not strong enough. Thus, using the NIST Cybersecurity Framework and ISO 27001 as guidelines for solving the problems, this must, therefore, be mitigated against in terms of effect and occurrence.

Step 1: Problem Identification

Through the Intrusion Detection System (IDS) real time monitoring of uunusual login attempts and suspicious data transfers. This emphasizes the need for Phishing Awareness, Strong Access Control and Real time incident detection.

Step 2: Root Cause Analysis

A post-incident forensic analysis is to be conducted using the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover). This will highlight the security breach such as lack of email filtering system and unenforced MFA.

This is in line with NIST Cybersecurity Framework (2023) which recommends continuous security monitoring to detect, analyse, and respond to cyber threats in real time.

Step 3: Implement Solutions and Preventative Measures

Deep-Engineering & Co therefore needs to adopt the following p**preventive actions**:

- **Enhancing Phishing Awareness Training**: This was substantiated by ENISA (the European Union Agency for Cybersecurity), who confirmed that per 2023, around 90% of cyber incidents are consequent to phishing, demanding an induction of continuous training on an ongoing basis.

- **Strengthening** get admission to manipulate policies by adoption of RBAC and enforcement of MFA. Following ISO 27001 to make sure that RBAC and MFA introduced can genuinely lessen a degradation of access to the system by as a minimum over 70%, in permitting unauthorized get entry to (ISO/IEC, 2022).
- **Advanced Threat Detection Response System**: These include enforcing IDS/IPS with real-time attack mitigation, continuous log monitoring, and implementing an overall SIEM for giving detection of anomalies.
- **Conducting Regular Audits and Compliance Checks**: Such as quarterly penetration testing, GDPR compliance audits and incident response plan this adheres to the GDPR Article 32 which mandates organizations to implement "appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

Step 4: Evaluation and Continuous Improvement:

- This will enhance the subsequent findings aaccording to Verizon's 2023 Data Breach Investigations Report, which state that agencies that have carried out MFA and supplied worker education lessen breach risks by means of as much as eighty%. This well-knownshows that Human blunders is a first-rate safety hazard, Multi-layered protection (MFA, RBAC, IDS, SIEM) machine mitigates threats efficiently, proactive monitoring and incident reaction reduce damage and recuperation time in addition to Compliance with ISO 27001 and GDPR guarantees records safety and legal adherence

By integrating cybersecurity focus, robust get admission to manage, and actual-time monitoring, Deep-Engineering.

9.Policy Enforcement & Monitoring for Information Governance

Effective records governance is crucial to companies retaining facts protection, regulatory compliance, and prevention of unauthorized use or get admission to. A robust enforcement and tracking framework guarantees compliance with installed pointers in addition to discouraging transgressions. This paper will outline the exercise of monitoring for compliance and implementing sanctions for lack thereof.

9.1.Compliance Monitoring

To follow the statistical regime's rules for personnel and stakeholders, the organization will use a combination of computerized and guide surveillance mechanisms. They adopt automated tracking units, compliance reports, general revision and real time information.

9.1.1. Regular Audits

Periodic audits are important in evaluating compliance with guidelines, determining vulnerabilities, and reducing risks. The commercial enterprise will carry out two kinds of audits:

- Internal Audits: The IT safety or compliance crew of the corporation conducts these audits, which take a look at departmental coverage adherence, access controls, and statistics coping with tactics. Internal audits may be performed each randomly and at everyday periods to assess persevered compliance.
- External Audits: These are carried out by way of unbiased auditors who confirm adherence to industry norms like GDPR, HIPAA, ISO 27001, and different guidelines. The organization's safety and governance rules are objectively reviewed by means of external auditors.
- Department review: In order to create something, their strategy is in line with the business structure, each department will self -drive. Senior control results can be knowledgeable to solve any question.

9.1.2. Automated Monitoring Tools

For complement of manual auditing, the company will appoint automatic monitoring equipment to track, detect and report in the fixed guidelines. These devices will include:

- SIM system for security information and event management (SIM): They collect log data from many sources and analyze and present immediately irregularities, illegal access efforts or policy violations.
- Data Loss Prevention (DLP) Solution: DLP system keeps an eye on e -post, download and data transfer to prevent sensitive information from errors or unintentional leaks. If a user tries to send banned data outside the network, the system will reject the transfer and inform the administrators.
- Monitoring of user activities (UAM): It monitors employees' activity in relation to business systems, reports irregularities for data access or illegal login efforts.
- Identity and Access Management (IAM) Tool: Roll-Based Access Control (RBAC), used by the IAM system, limits the access to the employee to the data needed for their job. IAM equipment helps detect examples where users try to access a system or data without authority.

9.1.3. Real-Time Alerts & Reporting

Security tools will be configured to warn of security breaches, policy violations or real time for suspicious activity on data. Warning will be:

- Warning IT security personnel on unauthorized access efforts or violations of the policy.
- Register security programs automatically for examination.
- Provide dashboards and auditor and match report on the manager

9.2.Consequences of Non-Compliance

In order to maintain the culture of compliance and protect organizational resources, the company will implement a strictly set of restrictions on non-transport. Providing corrective measures to remove limitations will serve to break the limitations.

9.2.1. Warning & Remediation

- There will be a formal warning as a result of the first minor offenses committed
- Workers who violate the policy by ignorance will have to undergo compulsory safety training to establish appropriate computing practices.
- To guarantee future compliance, several instructions will be provided.

9.2.2. Access Restrictions

To repeat criminals or more serious violations, access restrictions will be used, including:

- an obstacle of sensitive data or system access, either temporarily or permanently.
- The person's increased system activity monitoring to find further fractures.
- Special authority is required for specific operations until match is restored.

9.2.3. Disciplinary Actions

If an employee continues to disregard the guidelines for management management, the company can take disciplinary measures, for example:

- The work suspension pending an investigation is completed.
- Switch to a position with low access to data.
- A formal reprimand that is registered in human resource files for the worker.
- Reduced duties related to IT security or data management.

9.2.4. Legal & Financial Penalties

In cases where non-not-propaganda results in legal fractures, data violations or financial losses, further punishment will be used:

- The work suspension pending an investigation is completed.
- Switch to a position with low access to data.
- A formal reprimand that is registered in human resource files for the worker.
- Reduced duties related to IT security or data management.

9.2.5. Incident Response & Damage Control

If any breach of policy leads to databuks, the company will take measures to reduce the effect:

- Security and IT departments will look at this problem and take care.
- Teams that are responsible for legal and compliance will detect requirements for regulatory reporting and, if necessary, vigilant officers.
- Customers or other parties affected by the incident will be informed and it will be taken care of to ensure that it does not happen again.

10.Conclusion

In a strong information management structure, policy enforcement and monitoring are necessary. Reporting of real time, automatic monitoring and regular audit industry guarantees the following standards and safety rules. Strict restrictions on violations encourage responsibilities and reduce security breaches and the possibility of data.

Constant improvement in the guidelines and strict studies are necessary to maintain a skilled management structure. To keep politics up -to -date, effective and obedient, a special information management committee (IGRC) leads to a systematic review process. Reviews take into account operating changes, security programs, technology successes and regulatory changes. The guidelines have been properly changed, with proper approval, verification and spread to all parties involved.

Annual and trigger -based evaluations work together in response to changed business requirements and new threats. Strategies for continuous development, such as AI-operated enforcement equipment, staff training, benchmarking against industry standards and automated compliance monitoring, further strengthen management policy.

The organization improves data security, reduces the risk and guarantees long -term compliance with regulations by encouraging the active approach to policy control. In addition to the protection of sensitive information, a strong information government supports architectural operations, business integrity and reputation for the company.

11.References.

Internet Society (2023) *Principles for Responsible Data Handling - Internet Society*. Available at: https://www.internetsociety.org/policybriefs/responsible-data-handling/ (Accessed: 16 February 2025).

UK Data Service (2021) *Data Management Basics 2: Ethical and legal issues in data sharing*. Available at: https://dam.ukdataservice.ac.uk/media/622930/datamanagementbasics2finalv2.pdf (Accessed: 16 February 2025).

Improvado (2024) *Ethical Dimensions in Data Analysis: A Comprehensive Guide*. Available at: https://improvado.io/blog/ethical-data-management (Accessed: 16 February 2025).

IBM (2022) *Information Governance and Compliance*. Available at: https://www.ibm.com/security/information-governance-compliance (Accessed: 16 February 2025).

SANS Institute (2022) *Data Protection Officer: Role and Responsibilities*. Available at: https://www.sans.org/reading-room/whitepapers/data-protection-officer-role-responsibilities/ (Accessed: 16 February 2025).

Cybersecurity Ventures (2022) *Employee Data Security: Best Practices for Protecting Sensitive Information*. Available at: https://cybersecurityventures.com/employee-data-security-best-practices/ (Accessed: 16 February 2025).

TechTarget (2022) *IT Security: Protecting Your Organization's Information Assets*. Available at: https://www.techtarget.com/searchsecurity/feature/IT-security-Protecting-your-organizations-information-assets (Accessed: 16 February 2025).

Information Governance Initiative (2022) *Accountability in Information Governance: Ensuring Compliance and Trust*. Available at: https://www.iginitiative.org/accountability-in-information-governance/ (Accessed: 16 February 2025).

Leeds Beckett University (2022) *INFORMATION GOVERNANCE FRAMEWORK*. Available at: https://www.leedsbeckett.ac.uk/-/media/files/policies/information-governance/upig_framework.pdf (Accessed: 16 February 2025).

IBM (2024) *IBM Redbooks*. Available at: https://www.redbooks.ibm.com/?page=1&ps=20 (Accessed: 16 February 2025).

National Law Review (2024) *Predictions for Information Governance in 2024*. Available at: https://natlawreview.com/article/exploring-future-information-governance-key-predictions-2024 (Accessed: 16 February 2025).

ISO/IEC (2024) *Information technology — Governance of IT for the organization*. Available at: https://www.iso.org/obp/ui/en (Accessed: 16 February 2025).

GDPR (2018) *General Data Protection Regulation*. Available at: https://eur-lex.europa.eu

GDPR.EU, 2020. *GDPR.EU.* [Online]
Available at: https://gdpr.eu/what-is-gdpr/
[Accessed 13 February 2025].

GOV.UK, 2018. *GOV.UK.* [Online]
Available at: https://www.gov.uk/data-protection
[Accessed 27 February 2025].

HighTable, 2022. *HighTable.* [Online]
Available at: https://hightable.io/information-classification-and-handling-policy/#:~:text=A%20information%20and%20classification%20handling,are%20appropriate%20for%20the%20business.
[Accessed 27 February 2025].

HM Revenue & Customs, 2023. *ECSH11000 - Data Protection Act 2018/General Data Protection Regulation: data retention and disposal.* s.l.:s.n.

Lee, I., 2020. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet.*

Lopes, I. M. a. G. T. a. O. P., 2019. Implementation of ISO 27001 standards as GDPR compliance facilitator. *Journal of information systems engineering & management,* 4(2), pp. 1--8.

Radiflow, n.d. *Radiflow.* [Online]
Available at: https://www.radiflow.com/ot-cyber-knowledge/national-institute-of-standards-and-technology-cybersecurity-framework/
[Accessed 12 February 2025].

Roy, P. P., 2020. *A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard.* s.l., s.n.

Smallwood, R., 2014. *Information Governance: Concepts, Strategies, and Best Practices.* s.l.:Wiley.

The ISO Council, 2024. *The ISO Council.* [Online]
Available at: https://isocouncil.com.au/plan-do-check-act-iso-27001/
[Accessed 16 February 2025].

Wright, G., 2024. *TechTarget.* [Online]
Available at: https://www.techtarget.com/searchsecurity/definition/access-control
[Accessed 13 February 2025].

admin (2024). *Exploring Access Control, MFA and the Principle of Least Privilege*. [online] CYRISMA Cyber Risk Management Platform. Available at: https://cyrisma.com/exploring-access-control-mfa-and-the-principle-of-least-privilege/ [Accessed 2 Mar. 2025].

Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F. and Materne, S. (2022). Cyber Risk and cybersecurity: a Systematic Review of Data Availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, [online] 47(3). doi:https://doi.org/10.1057/s41288-022-00266-6.

CybSafe (2023). *Security awareness: 7 reasons why security awareness training is important in 2023*. [online] CybSafe. Available at: https://www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important/ [Accessed 2 Mar. 2025].

DPC (2018). *Data Protection Impact Assessments | Data Protection Commission*. [online] Data Protection Impact Assessments | Data Protection Commission. Available at: https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments [Accessed 2 Mar. 2025].

Edwards, M. (2017). *ISMS Online*. [online] ISMS.online. Available at: https://www.isms.online/iso-27001/ [Accessed 2 Mar. 2025].

Etheridge, E. (2024). Cyber security measures: Secure your business with digital signatures. *Dataguard.co.uk*. [online] Available at: https://www.dataguard.co.uk/blog/what-is-a-digital-signature-and-how-it-can-secure-your-business/#which-industries-need-digital-signatures-most [Accessed 2 Mar. 2025].

GDPR (2018). *General Data Protection Regulation (GDPR) – Final text neatly arranged*. [online] General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/art-33-gdpr/ [Accessed 2 Mar. 2025].

Information Commissioner's Office (2018). Essential Guide to the General Data Protection Regulation (GDPR). *Guide to the General Data Protection Regulation (GDPR)*. [online] doi:https://doi.org/10.1211/pj.2017.20203048.

Lord, N. (2023). *Data Protection: Data In transit vs. Data At Rest*. [online] Digital Guardian. Available at: https://www.digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest [Accessed 2 Mar. 2025].

National Institute of Standards and Technology (2018). Risk Management Framework for Information Systems and Organizations. *Risk Management Framework for Information Systems and Organizations*, [online] 2(Revision 2). doi:https://doi.org/10.6028/nist.sp.800-37r2.

NCSC (2015). *NIS Guidance Collection*. [online] Ncsc.gov.uk. Available at: https://www.ncsc.gov.uk/staticjson/ncsc-content/files/NIS%20Guidance%20Collection%201.0.pdf [Accessed 2 Mar. 2025].

Rapid7 (2020). *What is Vulnerability Management and Vulnerability Scanning*. [online] Rapid7. Available at: https://www.rapid7.com/fundamentals/vulnerability-management-and-scanning/ [Accessed 2 Mar. 2025].

CrowdStrike (2024) *2024 Global Threat Report*. Available at: https://www.crowdstrike.com/en-us/global-threat-report (Accessed: 18 February 2025).

ENISA (2023) *Phishing: The most common cyber threat*. Available at: https://www.enisa.europa.eu (Accessed: 18 February 2025).

ISO/IEC (2022) *ISO/IEC 27001: Information Security Management Systems (ISMS)*. Geneva: International Organization for Standardization.

NIST (2023) *Cybersecurity Framework Version 2.0*. National Institute of Standards and Technology. Available at: https://www.nist.gov/cyberframework (Accessed: 18 February 2025).

Verizon (2023) *2023 Data Breach Investigations Report*. Available at: https://www.verizon.com/business/resources/reports/dbir/ (Accessed: 18 February 2025).

ISO (2022). *ISO/IEC 27001: Information Security Management Systems.* Geneva: International Organization for Standardization.

NIST (2021). *Cybersecurity Framework.* Gaithersburg, MD: National Institute of Standards and Technology.

European Commission (2018). *General Data Protection Regulation (GDPR).* Available at: https://gdpr.eu (Accessed: 3 March 2025).

HIPAA (1996). *Health Insurance Portability and Accountability Act.* Available at: https://www.hhs.gov/hipaa (Accessed: 3 March 2025).