Student name : Ahmad Marwan AlMaghaireh

Id :23110205

Contents

[Part 1: Establishing and Implementing an ISMS for SecureLink 1](#_Toc200832805)

[1.1 Critically Analyse What Is Required to Establish and Maintain an ISMS for SecureLink 1](#_Toc200832806)

[1.2 Assess the Elements and Processes Required to Establish and Maintain an ISMS 5](#_Toc200832807)

[1.3 Justify the Steps Required for Implementing an ISMS for SecureLink 8](#_Toc200832808)

[Part 2: ISMS Design, Evaluation, and Comparison 12](#_Toc200832809)

[2.1 ISMS Design Plan and Implementation Map 12](#_Toc200832810)

[2.2 Appraisal Against Organizational Requirements 29](#_Toc200832811)

[2.3 Justification Using Audit Stages 33](#_Toc200832812)

[2.4 Purpose of International ISMS Standards 35](#_Toc200832813)

[2.5 Relationship Between Standards and ISMS Effectiveness 37](#_Toc200832814)

[2.6 Advantages and Disadvantages Compared to International Standards 39](#_Toc200832815)

# Part 1: Establishing and Implementing an ISMS for SecureLink

# 1.1 Critically Analyse What Is Required to Establish and Maintain an ISMS for SecureLink

**An Information Security Managment System (ISMS) is a structured set of policies, proceses, and controls meant to protect and manage an organization’s info assets. For SecureLink Insurance Services, a full digital company that uses AWS cloud and AI fraud detection, an ISMS is key to making sure confidintiality, integrity, and availability (CIA) of data are maintained, while also helping meet laws and regulations, and keeping customer trust in a tough insurance market.**

**1. ISMS Definition & Purpose in SecureLink**

**An ISMS is needed for:**

* **Protecting policyholder info, like health data and payment records.**
* **Stopping cyber threats such as ransomware, phishing, and vendor breaches.**
* **Following compliance (GDPR, PCI-DSS, and local rules).**
* **Supporting SecureLink’s Agile/DevOps and cloud-driven operations.**

**2. Define the Scope of the ISMS**

**The ISMS at SecureLink should clearly define its scope, which includes:**

* **Cloud-based platforms (web/mobile apps, customer portal).**
* **AI fraud detection systems.**
* **Cloud storage and back-end operations on AWS.**
* **APIs and 3rd party vendors that work with the company.**
* **All 3 offices: Amman, Dubai, Riyadh.**
* **Over 300 employees, many of them working remote.**

**This helps make sure no key systems or people are left out of security planning.**

**3. Identify and Classify Assets**

**SecureLink should list and rank the value of:**

* **Customer info (insurance, medical, ID records).**
* **IT systems like servers and cloud platforms.**
* **Devices used by staff (especially remote workers).**
* **Software (like Microsoft 365).**
* **People (employees, vendors, partners).**

**A full asset inventory should be done to link every asset with it’s security risk level.**

**4. Risk Assessment & Treatment**

**According to SecureLink’s risk chart, the ISMS must prepare for:**

* **Common attacks like phishing and weak passwords.**
* **Big-impact risks like cloud ransomware, AI failure, and insecure APIs.**
* **Existing problems such as vendor delays and high IT expenses.**

**Using COBIT 2019 and the ISACA toolkit, SecureLink can:**

* **Find risks and weaknesses.**
* **Measure likelihood and impact.**
* **Choose how to respond (fix, accept, reduce, or transfer the risk).**

**5. Security Controls**

**Controls should be setup using COBIT 2019 and ISO 27001 practices:**

* **Tech controls: like encryption, 2FA, and secure APIs.**
* **Admin controls: role based access, logs, change tracking.**
* **Physical controls: secure office entry, remote device rules.**

**These controls should match the risks found earlier.**

**6. Policies and Rules**

**Policies must be created to cover:**

* **Who can access what data.**
* **How data is stored and shared.**
* **How to handle incidents or breaches.**
* **Working with 3rd parties securely.**
* **Security for cloud services and mobile apps.**

**These rules must be shared with staff and kept updated.**

**7. Awareness and Training**

**To avoid inside mistakes and weak password use:**

* **Training on phishing, password security, and safe coding must be given.**
* **Add security topics to new employee onboarding.**
* **Encourage a strong security culture in line with company goals.**

**8. Monitoring and Auditing**

**SecureLink should:**

* **Monitor for cloud issues or hack attempts.**
* **Track logins, failed access, and system changes.**
* **Audit regularly to meet COBIT and ISO 27001 standards.**

**This helps respond quickly to any incident.**

**9. Documentation**

**SecureLink must document everything like:**

* **Risks and how they were treated.**
* **Who got trained and when.**
* **All rules and policies.**
* **Logs of audits and security events.**

**Good records help pass inspections and fix future problems.**

**10. Continual Improvment (PDCA)**

**To stay effective, SecureLink’s ISMS must follow the Plan-Do-Check-Act method:**

* **Plan: List risks and goals.**
* **Do: Put in place policies and protections.**
* **Check: Run audits and check effectiveness.**
* **Act: Improve and fix weak points.**

**This cycle never ends and helps keep the ISMS ready for new threats.**

**11. CIA Triad Focus**

* **Confidntiality: Using access rules and encryption.**
* **Integrity: Secure data flows and logging.**
* **Availability: Cloud backups, DDoS defenses, and uptime tracking.**

**All 3 are needed since SecureLink offers 24/7 online services.**

# 1.2 Assess the Elements and Processes Required to Establish and Maintain an ISMS

**An Information Security Management System (ISMS) is built using a mix of key elements (what must exist) and operational processes (what actions must be done repeatedly). Together, they help protect information, keep systems secure, and make sure the organisation can meet laws and customer expectations.**

**General Explanation**

**Core Elements of ISMS:**

1. **Information Security Policy – The main document that defines the organisation's security vision, rules, and responsibilities. It must be approved by management and followed by all staff.**
2. **Asset Management – Every data, software, device, and system must be listed and protected. The more valuable an asset, the more it needs protection.**
3. **Access Control – Ensures that people can only access what they are allowed to. It prevents unauthorised access to sensitive information.**
4. **Risk Treatment Plan – After identifying risks, the organisation must decide how to deal with them (avoid, reduce, accept, or transfer).**

**Key Operational Processes:**

1. **Internal Audits – Regular checks to make sure the ISMS is working as intended, and policies are being followed.**
2. **Incident Management – A defined way to report, respond to, and learn from security issues or cyber attacks.**
3. **Awareness and Training – All employees must understand their role in security. Training helps avoid mistakes like falling for phishing or using weak passwords.**

**SecureLink-Specific Example**

**SecureLink Insurance is a fully digital insurance company operating in a high-risk industry, using AWS cloud and AI fraud detection. The following shows how these elements and processes should be applied in their ISMS:**

**Elements in SecureLink’s Case:**

* **Security Policy: SecureLink must have a written policy that covers its use of cloud systems, customer portals, and AI tools. This policy should include rules for handling customer data, especially sensitive health and payment info.**
* **Asset Management: They must keep a full inventory of assets like:**

**Customer data (health, ID, financial).**

**AWS cloud storage buckets.**

**Fraud detection systems.**

**Mobile apps and internal platforms.  
Each asset should be classified by sensitivity and value, so proper protection can be assigned.**

* **Access Control: To reduce insider threats and data leaks, SecureLink should:**

**Use role-based access.**

**Apply multi-factor authentication (MFA).**

**Ensure API connections with partners are secured and limited.**

* **Risk Treatment Plan:**

**For example, ransomware attacks on their cloud environment (rated high impact) should be mitigated using encryption, backups, and incident response tools.**

**Risks like phishing or AI model failure can be reduced by employee training and monitoring AI performance.**

**Processes in SecureLink’s Case:**

* **Internal Audits: Regular checks should be done to see if:**

**Password policies are followed.**

**Security patches are up to date.**

**Cloud configurations are not misconfigured (a risk already noted).  
These audits should be done using the COBIT 2019 framework.**

* **Incident Management:**

**SecureLink must respond quickly to events like phishing attacks or DDoS on their insurance portal.**

**The company must have an incident log, defined escalation rules, and post-incident reviews.**

* **Awareness Training:**

**To stop problems like weak passwords and employee data leaks, SecureLink should hold training every few months.**

**Staff must know how to spot phishing emails and understand the company’s data handling rules.**

# 1.3 Justify the Steps Required for Implementing an ISMS for SecureLink

**Implementing an ISMS for SecureLink must follow a structured lifecycle. Each step is needed to make sure the system is aligned with company goals, protects important assets, and deals with threats effectively. Below are the 3 main phases—Planning, Implementation, and Monitoring—with reasons and examples from SecureLink's case.**

**1. Planning Phase**

**Understanding the Organization**

**Why: Before building anything, you must understand the company’s business model, assets, and threats. SecureLink is a cloud-based, AI-driven insurance company. That means customer data, fraud detection, and uptime are all critical.**

**Example: SecureLink’s use of AWS cloud and AI fraud detection requires identifying technical and operational dependencies.**

**Leadership and ISMS Approval**

**Why: Senior leadership support is needed for resources, decision-making, and policy enforcement. Without their backing, the ISMS won’t be taken seriously.**

**Example: The Managing Director already approved adopting COBIT 2019 — this shows top-level support.**

**Defining ISMS Scope**

**Why: The scope sets what the ISMS will cover — systems, departments, regions, and data types. If the scope is too narrow, risks will be missed.**

**Example: Scope should include customer portals, AI systems, regional offices in Amman, Riyadh, and Dubai, and the cloud infrastructure.**

**Information Security Policies**

**Why: Policies guide behavior and define security expectations. They cover access control, data sharing, and incident response.**

**Example: SecureLink must have a policy on cloud storage handling, remote work, and password strength, especially after noting weak password risks.**

**Risk Management Process**

**Why: This helps find out what can go wrong, how likely it is, and how bad the impact would be. Then plans are made to reduce or control those risks.**

**Example: SecureLink’s ransomware and phishing risks are high—so this process will suggest things like encryption and awareness training.**

**Organizational Structure of Info Security**

**Why: Everyone should know who does what. A clear structure helps with accountability and faster response.**

**Example: The IT security team might include roles for incident response, cloud security, and compliance management.**

**Statement of Applicability (SOA)**

**Why: The SOA links the identified risks with controls and explains why each control was chosen (or not).**

**Example: SecureLink might decide to apply DDoS protection, but not include physical visitor controls at a remote office—this will be explained in the SOA.**

**2. Implementation Phase**

**Design of Security Controls (P&P)**

**Why: These controls help prevent and detect issues. They can be policies (P) or procedures (P), and should match the risk assessment.**

**Example: To stop AI fraud detection failure, a policy might be written to ensure AI models are reviewed weekly.**

**Implementation of Security Controls**

**Why: After design, controls must be put in place—technically and operationally.**

**Example: Setting up multi-factor authentication, firewalls, or backup systems for cloud data.**

**Document Management Process**

**Why: Everything must be written down so it can be tracked, shared, updated, and audited later.**

**Example: SecureLink should maintain incident reports, training logs, and audit reports using proper version control.**

**Communication Plan**

**Why: Employees need to know about the ISMS, updates, and what they’re supposed to do.**

**Example: Send monthly updates about policy changes or known phishing attacks to all employees.**

**Training and Awareness Plan**

**Why: People are the weakest link in security. Without training, they might cause accidental leaks or fall for phishing.**

**Example: SecureLink must train staff to avoid phishing emails and use strong passwords (noted as one of the high-risk issues).**

**Operations Management**

**Why: Daily tasks like backup scheduling, access changes, and log reviews must be controlled and secured.**

**Example: All cloud systems on AWS must have automated backups, access logs, and alert systems for high-risk actions.**

**Incident Management**

**Why: When something goes wrong, the company must respond quickly, limit damage, and learn from it.**

**Example: If a DDoS attack hits the portal, the incident response team should act fast, log the issue, notify stakeholders, and review how to stop it in future.**

**3. Monitoring and Review Phase**

**Monitoring, Measurement, and Evaluation**

**Why: Security performance must be tracked using metrics eg : how many attacks were blocked, how many incidents occurred, etc.**

**Example: SecureLink should monitor API logs, AI system performance, and login failures to spot issues early.**

**Internal Audit**

**Why: Audits check if policies are followed and controls are working. Helps find weaknesses.**

**Example: Run quarterly audits to check if cloud security patches are up to date (a known risk area).**

**Management Review**

**Why: Senior management must review audit results and risks regularly to decide on improvements.**

**Example: The MD should review quarterly reports from the security team and approve changes to policies.**

**Problem Treatment and Non-Conformities**

**Why: Any failures must be investigated, documented, and corrected. Root cause analysis helps stop reoccurrence.**

**Example: If employee leaks data, the company must update training, improve access controls, or fire the offender if needed.**

**Continual Improvement**

**Why: Threats change, so the ISMS must evolve. Continual improvement is based on the PDCA (Plan-Do-Check-Act) cycle.**

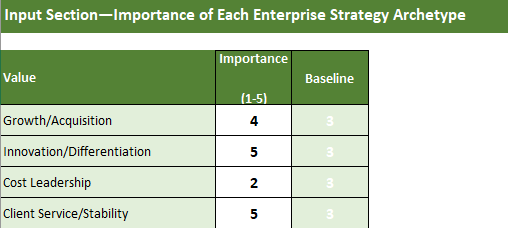
**Example: Add new controls if AI fraud models become less accurate, or if new phishing tactics appear.**

# Part 2: ISMS Design, Evaluation, and Comparison

# 2.1 ISMS Design Plan and Implementation Map

Plan the design of an ISMS for SecureLink, including an implementation map.  
  
resouress, plan for implmintation, and make the desghn ……… here you fininsh the toolkit   
screenshot of the toolkit

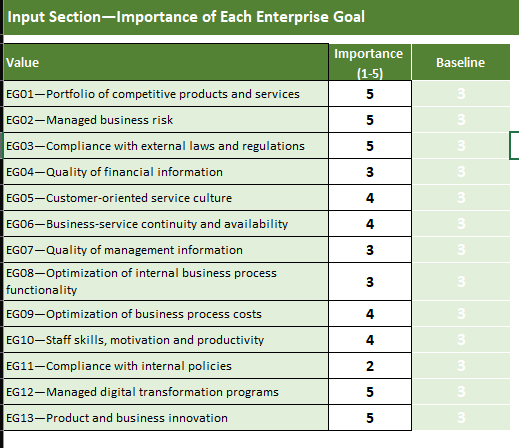
DF1 :



| **Value** | **Importance (1–5)** | **Justification** |
| --- | --- | --- |
| **Growth/Acquisition** | **4** | SecureLink wants to expand in **MENA and Europe**, showing a clear focus on growth. |
| **Innovation/Differentiation** | **5** | Uses **AI fraud detection**, cloud-first design, and plans to launch **new insurance products** — innovation is a core priority. |
| **Cost Leadership** | **2** | While cost is a factor (high IT costs mentioned), the company prioritizes **value and innovation** over being the cheapest. |
| **Client Service/Stability** | **5** | Focus on **building trust**, improving **customer service**, and ensuring **system uptime** (e.g., fixing incident response times). |

DF2:

| **Enterprise Goal (EG)** | **Importance (1–5)** | **Justification Based on SecureLink Scenario** |
| --- | --- | --- |
| **EG01 – Portfolio of competitive products and services** | **5** | SecureLink is launching **new insurance products**, aiming for **market leadership** in MENA and Europe. |
| **EG02 – Managed business risk** | **5** | Multiple risks (phishing, ransomware, insider threat, AI failure) require a **strong risk management focus**. |
| **EG03 – Compliance with external laws and regulations** | **5** | SecureLink must comply with **GDPR**, **PCI-DSS**, and **local laws** in Jordan, UAE, and KSA. |
| **EG04 – Quality of financial information** | **3** | Important for profitability and reporting, but **not emphasized** in the scenario. |
| **EG05 – Customer-oriented service culture** | **4** | SecureLink aims to **build trust** and **improve customer service**, making this moderately important. |
| **EG06 – Business-service continuity and availability** | **4** | Operating in cloud with AI-based systems means **service uptime** is crucial. |
| **EG07 – Quality of management information** | **3** | While valuable, it's not directly discussed in the case, so rated neutral. |
| **EG08 – Optimization of internal business process functionality** | **3** | Some IT process complexity is mentioned, but not a primary goal. |
| **EG09 – Optimization of business process costs** | **4** | The scenario highlights **high IT costs**, so cost control is important. |
| **EG10 – Staff skills, motivation and productivity** | **4** | A strategic goal is to **maintain strong employee culture** and apply recognition programs. |
| **EG11 – Compliance with internal policies** | **2** | Internal policy compliance isn't emphasized as much as **external regulations**. |
| **EG12 – Managed digital transformation programs** | **5** | The company is fully **digital**, cloud-based, and **focused on DevOps**, making this critical. |
| **EG13 – Product and business innovation** | **5** | AI-based fraud detection and new product innovation are at the **heart of SecureLink’s strategy**. |

  
DF3:

| **Risk Scenario Category** | **Impact (1–5)** | **Likelihood (1–5)** | **Justification** |
| --- | --- | --- | --- |
| **IT investment decision making, portfolio management** | 4 | 3 | Decision-making delays and communication gaps are mentioned in the scenario. |
| **Program & projects life cycle management** | 3 | 3 | Agile/DevOps approach helps reduce risk, but complexity exists. |
| **IT cost & oversight** | 5 | 4 | High IT operational costs are an existing pain point for SecureLink. |
| **IT expertise, skills & behavior** | 4 | 3 | Staff culture is strong, but training and skill gaps (like weak passwords) remain. |
| **Enterprise/IT architecture** | 4 | 3 | SecureLink uses cloud and AI—poor architecture could lead to large impact. |
| **IT operational infrastructure incidents** | 5 | 3 | Service outages (e.g., DDoS, slow incident response, cloud misconfigs) are real risks. |
| **Unauthorized actions** | 4 | 3 | Insider threat and weak access policies were listed as medium-high risks. |
| **Software adoption/usage problems** | 3 | 3 | No specific mention, but relevant to API and cloud usage. |
| **Hardware incidents** | 2 | 2 | Not emphasized; company is mostly cloud-based. |
| **Software failures** | 4 | 3 | AI system failure is a key risk with reputational impact. |
| **Logical attacks (hacking, malware, etc.)** | 5 | 5 | SecureLink is a **frequent target** of phishing, ransomware, and DDoS. |
| **Third-party/supplier incidents** | 4 | 4 | Past vendor compliance delays and third-party breach risks are noted. |
| **Noncompliance** | 5 | 3 | GDPR, PCI-DSS, and regional laws make compliance **critical**. |
| **Geopolitical issues** | 2 | 2 | Not mentioned as a concern; low relevance in scenario. |
| **Industrial action** | 1 | 1 | Not relevant for a digital company with 300+ staff. |
| **Acts of nature** | 2 | 2 | No reference; cloud usage may reduce risk further. |
| **Technology-based innovation** | 5 | 4 | Company relies on early adoption (AI/cloud); failure to innovate is risky. |
| **Environmental** | 1 | 1 | Not applicable to a digital company. |
| **Data & information management** | 5 | 4 | Core to SecureLink’s business (insurance data, GDPR, cloud storage, APIs). |

A screenshot of a computer screen

AI-generated content may be incorrect.  
DF4:

| **IT-Related Issue** | **Importance (1–3)** | **Justification** |
| --- | --- | --- |
| Frustration between different IT entities across the organization | **2** | There's mention of **communication gaps**, but not deep conflict across IT units. |
| Frustration between business departments and IT | **3** | The scenario says there are **complex IT models causing delays**, and poor coordination. |
| Significant IT-related incidents (data loss, security breaches, etc.) | **3** | **Ransomware, cloud misconfiguration, DDoS, and phishing** are real threats to SecureLink. |
| Service delivery problems by outsourcers | **2** | Some outsourcing is used (e.g., Microsoft 365), but the core team is **primarily insourced**. |
| Failures to meet IT-related regulatory requirements | **3** | Compliance with **GDPR, PCI-DSS, local laws** is critical and noncompliance is a listed risk. |
| Regular audit findings or poor service reports | **2** | Auditing is mentioned as needed (COBIT-based audit), but no sign of ongoing failures. |
| Hidden or rogue IT spending | **2** | High IT cost is an issue, but nothing suggests **unapproved departmental spending**. |
| Duplicated initiatives or wasted resources | **2** | Not emphasized in scenario, but **could be implied** by complex operations. |
| Inadequate staff or burnout | **2** | They have over 300 FTEs and promote strong culture, but **some training gaps exist**. |
| Projects delivered late or over budget | **3** | The company struggles with **complexity and vendor compliance delays**, impacting delivery. |
| Management reluctance to engage with IT | **1** | The **Managing Director is actively supporting** ISMS and COBIT adoption. |
| Complex IT operating model or unclear decisions | **3** | This is **explicitly stated**: "complex IT model delays decision-making." |
| Excessively high cost of IT | **3** | SecureLink suffers from **high operational IT costs** — it's already materialized. |
| Failed implementation due to architecture/systems | **2** | There are risks of **AI system failure** and misconfiguration, but not frequent failures. |
| Gap between business and technical knowledge | **3** | Stated issue: **communication gaps between IT and business**. |
| Data quality/integration issues | **2** | Cloud systems manage most data, no issue reported — but **must be monitored**. |
| High end-user computing without control | **1** | No evidence in scenario — centralized control seems in place. |
| Business units implementing shadow IT | **1** | No sign of shadow IT; systems appear **centrally managed**. |
| Ignorance of privacy laws | **3** | GDPR and data law **compliance is a priority**, noncompliance is a documented risk. |
| Inability to innovate with technology | **1** | SecureLink is an **early adopter of tech**, focused on AI and digital transformation. |

A screenshot of a computer

AI-generated content may be incorrect.

DF5:

| **Value** | **Importance (%)** | **Justification** |
| --- | --- | --- |
| **High** | **75%** | SecureLink is in a **high-risk sector** (insurance/financial) and faces **frequent attacks** like phishing, ransomware, and DDoS. However, the company has **some maturity in place** (e.g. AI-based fraud detection, cloud infrastructure, COBIT adoption), which helps reduce the *relative weight* of the threat exposure. |
| **Normal** | **25%** | Some parts of the business, such as internal administrative systems or non-customer-facing operations, may not be under immediate attack, making them **less exposed**. Also, the organization shows commitment to **monitoring, training, and compliance**, which reduces general threat likelihood. |

A screenshot of a pie chart

AI-generated content may be incorrect.

DF6:

| **Value** | **Importance (%)** | **Justification** |
| --- | --- | --- |
| **High** | **70%** | SecureLink operates in **highly regulated regions** (EU, Jordan, KSA, UAE) and must comply with **GDPR**, **local data protection laws**, and **PCI-DSS**. The business handles **health, financial, and personal data**, so compliance is crucial. |
| **Normal** | **25%** | While most operations are sensitive, there are areas (e.g. internal employee tools, or non-customer-facing systems) that still need policy compliance but carry **moderate risk**. |
| **Low** | **5%** | Very few areas in SecureLink are likely exempt from heavy compliance — possibly internal testing systems or low-sensitivity services, so **low importance areas exist but are minimal**. |

A screenshot of a graph

AI-generated content may be incorrect.

DF7:

| **Value** | **Importance (1–5)** | **Justification** |
| --- | --- | --- |
| **Support** | **2** | While IT supports basic operations, SecureLink’s IT is not limited to helpdesk-level tasks. It plays a bigger role in innovation, not just support. |
| **Factory** | **4** | IT is essential for **operational efficiency**, automation, and 24/7 availability of cloud services (customer portals, mobile apps). Systems must run **reliably**, like a production line. |
| **Turnaround** | **3** | There are efforts to **modernize and streamline operations**, especially addressing delays and vendor-related issues, but turnaround isn't the main theme. |
| **Strategic** | **5** | IT is **core to the business strategy**: AI fraud detection, cloud-based infrastructure, DevOps practices, and digital transformation all position IT as a **strategic enabler**. |

A table with numbers and text

AI-generated content may be incorrect.

DF8:

| **Value** | **Importance (%)** | **Justification** |
| --- | --- | --- |
| **Outsourcing** | **20%** | SecureLink does some outsourcing (e.g., Microsoft 365 services, possibly hosting), but **most of its IT is internally controlled**. Outsourcing plays a minor but present role. |
| **Cloud** | **35%** | The business heavily depends on **cloud infrastructure (AWS)** and cloud-based tools for delivering insurance services, AI fraud detection, and scalability. |
| **Insourced** | **45%** | The scenario mentions a **primarily insourced IT team**, especially for core systems, strategy, and development. IT leadership and operational control are kept internally. |

A table with green and white text

AI-generated content may be incorrect.

DF9:

| **Value** | **Importance (%)** | **Justification** |
| --- | --- | --- |
| **Agile** | **50%** | SecureLink emphasizes **customer satisfaction, flexibility, and rapid delivery**, which aligns well with Agile. It’s clearly a major method used in product and platform development. |
| **DevOps** | **40%** | The company uses **cloud infrastructure**, **AI tools**, and focuses on **automation**, which indicates strong reliance on DevOps practices for continuous integration and deployment. |
| **Traditional** | **10%** | Some **administrative or legacy systems** may still follow traditional methods (e.g., documentation-heavy internal projects), but these are limited. |

A table with text and numbers

AI-generated content may be incorrect.

DF10:

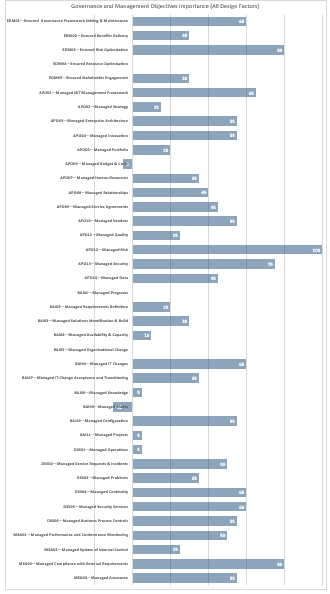
| **Value** | **Importance (%)** | **Justification** |
| --- | --- | --- |
| **First mover** | **70%** | SecureLink is described as an **early technology adopter**, using **AI-based fraud detection**, **cloud-first infrastructure**, and **DevOps**. Innovation is key to their strategy. |
| **Follower** | **25%** | Some systems may be adopted after validation (e.g. Microsoft 365), and the company balances risk before adopting certain tech. |
| **Slow adopter** | **5%** | Only applies to **low-priority internal processes** or legacy areas. The company is clearly not hesitant when it comes to adopting new technologies for competitive advantage. |

A pie chart with numbers and a green text

AI-generated content may be incorrect.

# 2.2 Appraisal Against Organizational Requirements

The planned ISMS design **strongly aligns with SecureLink’s strategic needs and operational risks**, especially in areas such as **risk management**, **security**, **compliance**, and **IT change control**. While most critical issues are addressed, a few areas like **cost control**, **resource optimization**, and **project management** scored low and may require future improvements



| **SecureLink Requirement / Risk** | **COBIT Objective(s)** | **Toolkit Score** | **How the ISMS Design Fulfills This** |
| --- | --- | --- | --- |
| **1. Cyber threats** (phishing, ransomware, DDoS, AI failure) | APO12 (Risk), APO13 (Security), DSS05 (Sec. Services) | 100, 75, 60 | Excellent coverage of security risks and controls with top-tier focus on managed risk and security. |
| **2. Legal compliance** (GDPR, local laws, PCI-DSS) | MEA03 (Compliance), MEA01 (Monitoring), DSS06 | 80, 50, 55 | Compliance needs fully supported with good assurance and external monitoring coverage. |
| **3. Cloud misconfiguration, service continuity, and availability** | DSS04 (Continuity), BAI06 (IT Changes), BAI10 | 60, 60, 55 | Strong scores ensure that downtime and config risks are actively managed. |
| **4. High IT cost and budget overruns** | APO06 (Budget & Costs), EDM04 (Resource Optimization) | -5, 0 | Cost optimization is a **clear weakness**. ISMS must improve in budget/resource tracking. |
| **5. Innovation through AI and fraud detection** | APO04 (Innovation), APO03 (Architecture) | 55, 55 | Solid alignment with SecureLink's strategic technology-driven approach. |
| **6. Managing third-party vendors and external systems (e.g. APIs)** | APO09 (Service Agreements), APO10 (Vendors) | 45, 55 | Strong vendor management objectives support secure third-party integrations. |
| **7. Internal IT communication gaps and complex decision models** | APO08 (Relationships), EDM01 (Governance Framework) | 40, 60 | Clear governance and relationship-building are emphasized to close internal gaps. |
| **8. Customer satisfaction & service request handling** | DSS02 (Requests), DSS03 (Problems), DSS01 (Ops) | 50, 35, 5 | Good on service requests, but general operations may need more focus. |
| **9. Digital transformation and DevOps culture (Agile + Cloud)** | APO01 (IT Mgmt), BAI03 (Build), BAI07 (Transition) | 65, 30, 35 | Reasonable support for change, but room to improve solution delivery agility. |
| **10. Knowledge sharing, documentation, and IT training** | BAI08 (Knowledge), APO07 (HR), MEA02 (Internal Control) | 5, 35, 25 | Some support exists, but **knowledge management is very weak (score 5)**. |

**Overall ISMS Effectiveness Rating**

| **Evaluation Area** | **Assessment** |
| --- | --- |
| **Risk Elimination** | **Very Strong** — major risks (security, compliance, cloud) are well-covered. |
| **Strategic Goal Alignment** | **Strong** — innovation, transformation, and trust-building are clearly supported. |
| **Operational Gaps** | **Moderate** — budgeting, resource optimization, and project planning need enhancement. |
| **Support Processes** | **Weak in some areas** — documentation, asset tracking, and knowledge sharing are low. |

**Final Judgment**

The planned ISMS is **highly effective** in addressing SecureLink’s **core risks and strategic goals**, especially in:

* **Risk and security management**
* **Legal compliance**
* **Innovation enablement**

However, to be fully comprehensive, the ISMS should be **expanded in future iterations** to:

* Improve cost and budget controls (APO06)
* Enhance knowledge/documentation handling (BAI08)
* Strengthen internal operations support (DSS01, BAI05)

# 2.3 Justification Using Audit Stages

**The planned ISMS for SecureLink can be fully justified using the audit process stages as taught in class. The COBIT-based ISMS design aligns with the standard audit lifecycle, helps guide evidence collection, and supports continous complience.**

**IS Audit Process and How the ISMS Helps**

| **Audit Stage** | **How the ISMS Design Supports It** |
| --- | --- |
| **1. Planning Phase** | **SecureLink defined it’s goals clearly by targeting risks like phishing, AI failure and ransomware. EDM01 (Governance – 60) and APO01 (IT Mgmt – 65) show strong planing.** |
| **2. Fieldwork & Documentation** | **Controls like DSS05 (Security Services – 60) and APO13 (Security – 75) help security team collect data, test controlls, and document issues properly.** |
| **3. Reporting & Followup** | **Results are sent to leaders using MEA03 (Compliance – 80) and MEA01 (Monitoring – 50). Weaknesses can be tracked and improved in future audits.** |

**How ISMS Helps in Audit Phases**

| **Component** | **How ISMS Design Helps** |
| --- | --- |
| **Security Testing** | **DSS05 and APO13 help with technical testing like penetration test or vuln scan.** |
| **Assessment** | **APO12 (Risk – 100) and DSS04 (Continuity – 60) help do a full risk based review.** |
| **Audit Reporting** | **MEA03 and MEA04 help make sure audit result are shared with management and regulators.** |

**Audit Strategy & Planning**

**The ISMS lets the audit team:**

* **Set goals that match real threats (ransomware, DDoS, etc)**
* **Choose scope like AWS cloud, AI systems, and APIs**
* **Involve department managers early (supported by APO01, EDM01)**

**Also, DSS02 and DSS06 help collect evidence, and DSS03 helps with problem tracking after audit.**

**Post Audit Stage: Continous Compliance**

**Once audit is done, the ISMS helps SecureLink stay ready for next inspection and fix any problems.**

| **Phase** | **ISMS Design Support** |
| --- | --- |
| **Corrective Actions** | **DSS06 and MEA01 help track changes and make sure problems are fixed.** |
| **Ongoing Complience** | **MEA03 (80) helps make sure laws like GDPR are followed over time.** |
| **Assurance & Monitoring** | **MEA04 (Assurance – 55) helps provide final proof that system is secure and compliant.** |

**The ISMS desgin make auditing much easyer and supports all audit stages:**

* **In planning, risk areas and assets are already defined**
* **In fieldwork, all controlls are linked to real threats**
* **In reporting, objectives like MEA03 and APO08 help track and fix problems**
* **In followup, the ISMS connects to complience rules directly**

# 2.4 Purpose of International ISMS Standards

**International ISMS standards, specialy ISO/IEC 27001, are used to give a globaly accepted way of protecting information and managing information security risk in a orginazation — no matter it’s size or industry type.**

**Why ISO 27001 is Important**

| **Purpose** | **Explenation (with example)** |
| --- | --- |
| **Standardization** | **Makes sure every company follow a systematic method to secure data. SecureLink for example has multiple branches, so this helps keep all working same way.** |
| **Risk-Based Security** | **ISO 27001 helps in identify and handle risks (like Clause 6, Planning). SecureLink have risk like cloud error, phishing, ransomwares, and all of these can be managed using ISO based ISMS.** |
| **Compliance** | **It supports following of GDPR, PCI and laws. Clause 9 and 10 make sure your policies are watched and updated.** |
| **Audit Readiness** | **Helps orginization to be ready for audits. SecureLink can show its documents and prove it follows the rules by ISO requirements.** |
| **Reputation & Trust** | **Having the ISO certificate make customers and partners trust you. SecureLink can show it protects personal data properly.** |
| **Operational Efficiency** | **ISO reduces confusion and helps respond quickly in attacks (Clause 8 – Operation). It makes sure trained people handle security (Clause 7 – Support).** |

**PDCA Model in ISO 27001**

**ISO 27001 follow the Plan-Do-Check-Act (PDCA) model, which help company keep improving all the time:**

| **Stage** | **What It Means** | **SecureLink Example** |
| --- | --- | --- |
| **Plan** | **Think about risk, write policy, set goals** | **SecureLink plan for AI failing or DDoS** |
| **Do** | **Setup the security stuff** | **Start employee training, access control, MFA** |
| **Check** | **Check if controls working, audit it** | **Run test on cloud systems, internal audit** |
| **Act** | **Fix and make better** | **After finding API weakness, they patch and test again** |

**Other ISO 27000 Family Standards**

**Some other ISO standerds that help support ISO 27001:**

* **ISO 27002 – How to use the 114 controls (Annex A)**
* **ISO 27005 – About risk management**
* **ISO 27017 / 27018 – Cloud & privacy data protection**
* **ISO 27701 – Extends to privacy system (PIMS)**

**SecureLink can use these to protect user data on cloud, manage 3rd party vendors, and follow privacy laws.**

**Final Thoughts (Realistic Style)**

**ISO 27001 is like the back bone of a strong ISMS. For SecureLink, using ISO 27001 helps:**

* **Keep insurence data and customer info safe**
* **Spot risks early and fix them quick**
* **Avoid getting fined from GDPR or local rules**
* **Make people trust the company**
* **Be always ready for audits**

**Without using ISO, SecureLink would be disorganized and can’t fight big risks like AI fail, cloud problem or phishing. But with ISO 27001, and the PDCA model, they keep improving and staying safe all the time.**

# 2.5 Relationship Between Standards and ISMS Effectiveness

**Analyse the Relationship Between Standards and an Effective ISMS**

**Building an effective Information Security Managment System (ISMS) is not just about writing policies — it needs to follow a clear structure, and that's where international standerds like ISO 27001 help. These standerds give a strong foundation for how to design, run, and improve an ISMS that really protects an organization.**

**How Standards Support the ISMS**

| **Standard** | **How It Helps the ISMS** |
| --- | --- |
| **ISO/IEC 27001** | **Gives the main framework and structure for a complete ISMS.** |
| **ISO/IEC 27002** | **Guides how to apply the 114 controls in Annex A — this makes security practical.** |
| **ISO/IEC 27005** | **Helps in doing risk assessment and risk treatment — which are at the heart of any ISMS.** |
| **ISO/IEC 27701** | **Extends the ISMS to manage privacy and personal data (PIMS).** |
| **Other 27000 Series** | **Help in auditing, cloud security, incident managment, and more.** |

**Relationship Explained**

**An ISMS needs to:**

1. **Identify risks (internal and external)**
2. **Setup controls and policies to handle them**
3. **Train people and monitor results**
4. **Keep improving over time**

**Without a standard, every org might do this in a different way — some will miss things, or focus on wrong areas. But standards make sure the ISMS covers all important areas like:**

**Confidentiality**

**Integrity**

**Availability**

**Legal compliance**

**Operational readiness**

**Standards like ISO 27001 also help make the ISMS auditable, repeatable, and trusted by customers and regulators.**

**Example: SecureLink Case**

**SecureLink is a digital insurance company. They deal with:**

**Customer data**

**Cloud platforms**

**AI systems**

**Following ISO 27001 ensures SecureLink's ISMS can:**

**Meet GDPR and other laws**

**Address threats like ransomware, phishing, and cloud errors**

**Apply correct controls from Annex A**

**Be improved using audits (Clause 9 & 10)**

**Use PDCA cycle to keep evolving**

**So, the standard is not just a guideline — it becomes the blueprint for how SecureLink builds and runs its ISMS.**

**The relationship between standards and ISMS is strong and important. Without the standard, the ISMS may be random or weak. But with it, the ISMS becomes structured, tested, and trusted. That’s why most serious companies, like SecureLink, follow ISO 27001 and its related standards to make their ISMS work the right way.**

# 2.6 Advantages and Disadvantages Compared to International Standards

The planned ISMS for SecureLink, which is desgned using the COBIT 2019 framework and ISACA toolkit, has many areas that **closely align with international standards** like **ISO/IEC 27001**. However, when examined critically, there are both strong advantages and clear disadvantages when comparing the planned system to the ISO standard.

One **major advantage** of the planned ISMS is how it supports **auditing activities**. With COBIT’s clear objectives (like APO12 for Managed Risk and APO13 for Security), the ISMS creates **measurable performance indicators**, which makes it easier for internal and extrnal auditors to track, validate, and document how SecureLink manages information security. This directly supports the auditing clauses in ISO 27001, like Clause 9 for **Performance Evaluation** and **Internal Audits**. So in this case, the ISMS is not only helping the organization manage risk — it's also **making the audit process faster and more trustable**, which is critical when dealing with third-party regulators or ISO certification auditors.

In terms of alignment, the SecureLink ISMS **achieves most of the ISO 27001 principles**. For example, it uses the **Plan-Do-Check-Act (PDCA)** cycle, which is core to ISO. Planing is covered in the tolkit through goals, risk profiling, and scope setting. Doing is shown in the design of controls and implementation map. Checking and acting is done by mapping complance (MEA03) and improvement (DSS06). Furthermore, the ISMS also supports the three pillars of information security: **confidentiality, integrity, and availability**. This can be seen through strong scores in risk, continuity, and compliance.

However, there are some **disadvantages and critical issues**. First, while COBIT offers a flexible and business-focused approach, it is **not a certifiable standard** like ISO 27001. That mans SecureLink may face challenges if it ever wants formal ISO 27001 certification, since it would need to adjust its ISMS to meet **all 114 controls in Annex A** and comply with every clause from 4 to 10. This might require **redoing some parts of the framwork**, which could waste time or cause confusion.

Second, the toolkit results revealed **low performance in areas like APO06 (Budget & Cost: -5)** and BAI08 (Knowledge: 5). These are critical to long-term ISMS sustainability. Without proper budget tracking and knowledge sharing, the ISMS could become a checklist system that fails during real-world threats or staff turnover. These weak areas also go against the ISO values of **sustanability and continual improvment**, especially Clause 10 (Improvement).

Another limitation is that the ISMS focuses more on **internal risk management** and less on external communication or stakeholder engagement. For example, EDM05 (Stakeholder Engagement) scored only 30, which shows the ISMS might not be addressing **extrnal trust or transparency** well — something ISO 27001 requires, especially when dealing with interested parties and data subjects.

To enhance the planned ISMS and bring it even closer to ISO-level maturity, SecureLink should:

Increase focus on **resource and cost optimization** so that the ISMS becomes more efficient and sustainable.

mprove **documentation, knowldge sharing**, and internal communication (APO07, APO08, BAI08) to support audit readiness and long-term improvements.

Consder a **mapping exercise** that aligns COBIT controls directly with ISO 27001’s Annex A, to prepare for future certification without starting from zero.

In conclusion, while SecureLink’s planned ISMS provides a **strong operational structure** that mets most practical and auditing needs, it must address gaps in compliance, cost control, and staeholder transparency to fully match the depth and **global acceptance** of ISO 27001. If thse enhancements are done strategically, the ISMS will not just meet standards it will exced them in effectiveness and flexibility.

# References

1. **What is an ISMS?** – ISO 27001 Institute  
   https://www.iso27001security.com/html/27001.html  
   Explains what an ISMS is, why it’s needed, and how to define scope, assets, risks, and controls.
2. **What are the elements of an ISMS?** – IT Governance UK  
   https://www.itgovernance.co.uk/isms  
   Covers core ISMS components like policy, asset management, risk treatment, and internal auditing.
3. **ISO 27001 Implementation Checklist** – Advisera  
   https://advisera.com/27001academy/knowledgebase/iso-27001-implementation-checklist/  
   Breaks down the practical steps and lifecycle for setting up and maintaining an ISMS.
4. **What is ISO 27001?** – NQA Global  
   https://www.nqa.com/en-gb/certification/standards/iso-27001  
   Explains ISO 27001 structure, purpose, PDCA, and its benefit to organizations.
5. **Understanding ISO 27001 Clauses** – ISMS.online  
   https://www.isms.online/iso-27001/clauses/  
   Gives clause-by-clause breakdown, including PDCA, leadership, planning, support, and improvements.
6. **Benefits of ISO 27001 Certification** – BSI Group  
   https://www.bsigroup.com/en-GB/iso-27001-information-security/  
   Covers the business case for using ISO 27001 and why it is a globally accepted ISMS framework.