1 2  9 0 FACULDADE DE CIÊNCIAS E TECNOLOGIA UNIVERSIDADE D COIMBRA

AGC - Assignment #1
Risk Management

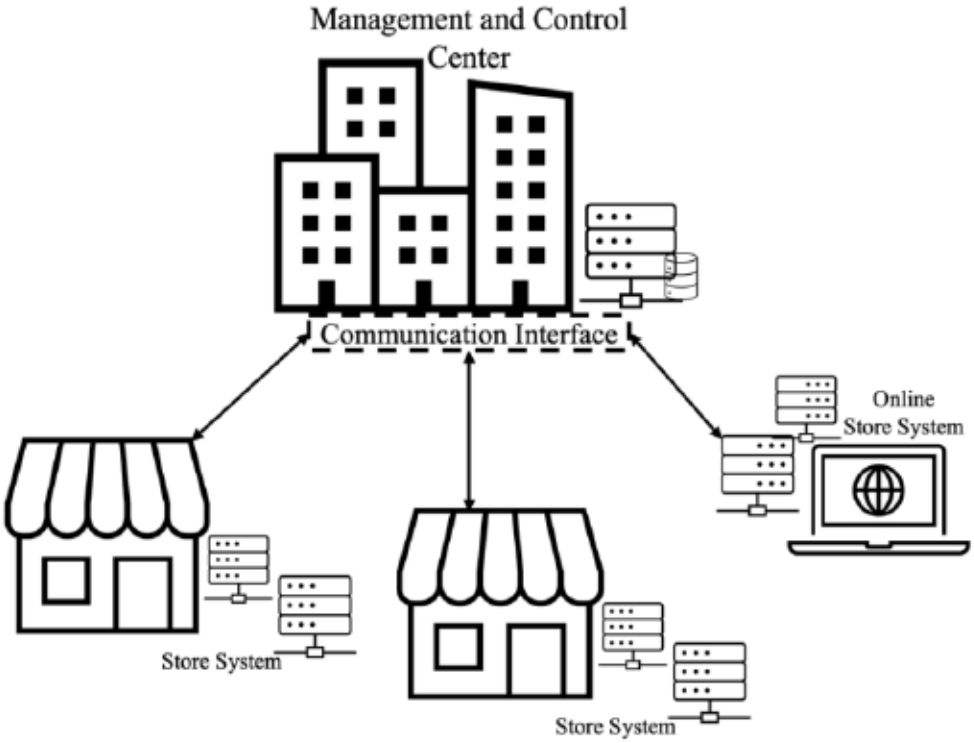

Figure 1 - High-level architecture of the company store.

Leonardo Oliveira Pereira

University of Coimbra, Department of Informatics Engineering, Portugal

uc2020239125@student.uc.pt

1. Introduction

This assignment explores the critical process of risk management within a retail company, focusing on the analysis, evaluation, and strategic planning needed to effectively manage risks. Given the complex nature of the retail sector—with its diverse operations spanning data storage, supply chain logistics, customer information management, and employee data handling—a structured approach to risk management is essential.

The risk management plan includes a series of key steps: **system categorization** (including detailed system descriptions, boundary definitions, and risk tolerance analysis); **risk identification and assessment** (covering asset valuation, threat analysis, and vulnerability assessment); and **risk control strategies** (with examples of recommended security controls). Additionally, the plan incorporates a framework for ongoing monitoring and re-evaluation. By thoroughly categorizing systems, assessing risks, and implementing proactive controls, this approach aims not only to address current vulnerabilities but also to equip the organization to withstand emerging threats in the future.

2. System Categorization

At this stage, Special Publication (SP) 800-60 of the National Institute of Standards and Technology (NIST) will be consulted to guide the categorisation of the system. The system's limits will also be established and the level of tolerance and risk appetite will be analysed.

1a) System Description

The risk management plan is addressed to a company that has has multiple stores, geographically distributed in different countries, and a management and control center responsible for supply chain operations and centralized information storage. Additionally, the company also provides a delivery service. The clients purchase the products using a web application and the closest store that can assure the delivery provides the service.

In the context of the retail company’s multifaceted operations, the system handles the following set of functionalities:

- **Business information storage and sharing:** This functionality involves storing and sharing key business data, such as operational reports, sales analytics, financial data, and inter-

store communications. This centralized information is essential for coordinated decision-making across multiple locations.

- **Supply chain support to multiple stores in different countries:** This function enables centralized control and oversight of the supply chain across all store locations. It ensures efficient inventory distribution, replenishment, and coordination with suppliers, allowing stores to meet local demand while aligning with global supply chain goals.
- **Stock and delivery management:** This feature handles the inventory within each store and supports real-time tracking and allocation of stock levels. It also manages the fulfillment of online orders, ensuring products are packaged and delivered from the nearest location able to meet the customer's needs.
- **Client's information storage:** This functionality securely stores sensitive customer information, including payment data, addresses, and purchase history. It is critical for personalizing customer service, ensuring smooth transactions, and protecting customer privacy.
- **Employee information:** This feature involves the secure handling and storage of employee data, including personnel records, roles, access permissions, and performance data. It supports HR processes and ensures only authorized access to employee information.
- **Promotions information:** This functionality manages promotional campaigns, including discounts, campaign start and end dates, and other promotional conditions. It ensures consistency across stores and online platforms, giving customers timely access to promotions and marketing offers.

In addition, the organization already has in place some security measures and policies that contribute to an initial organizational structure that is ready to withstand attacks against the system, such as:

- **Network segmentation:** This divides the company's network into smaller, isolated segments, such as separating internal data (e.g., employee or financial data) from customer-facing applications (e.g., the web application for purchases). Network segmentation reduces the potential impact of a breach by containing threats to isolated sections of the network and limiting unauthorized access to sensitive areas.
- **Access control policies:** These policies define who can access specific data or systems based on role-based permissions (e.g.,

managers versus general staff). For example, only HR personnel can access sensitive employee data, while only IT administrators can access certain system configurations. This minimizes unauthorized access and reduces the risk of internal and external breaches.

- **Data encryption:** Encrypting sensitive information, both in transit (as data moves between systems) and at rest (when stored in databases), protects against unauthorized access. If a data breach occurs, encrypted data is more challenging for attackers to interpret, safeguarding critical customer and business information.
- **Data Backup:** Regular backups of critical data are created and stored securely to prevent data loss due to cyberattacks (e.g., ransomware), hardware failure, or other disruptions. These backups allow the company to quickly restore data and resume operations in the event of an incident.
- **Video Surveillance:** Cameras installed at critical points within physical locations (e.g., server rooms, access points) help prevent unauthorized physical access to the company's hardware and infrastructure. This measure provides a deterrent against theft and helps identify unauthorized personnel or suspicious activities.

1b) Boundaries Definition

Boundaries are established to delineate the extent of the system's influence and interaction. These boundaries define the scope of the system and specify what is included and excluded from management activities and risk assessments.

- **Business information storage and sharing:**
  - ❖ **Boundaries:** This functionality includes the centralized storage servers (on-premises or cloud-based) and physical data centers housing business information. It also encompasses secure network devices, such as routers and firewalls, that manage data flows between store locations and the management center.
  - ❖ **Exclusions:** Customer-facing online delivery systems, direct customer interfaces, and physical delivery assets are not part of this boundary, as business information is separate from delivery and customer interaction systems.

- **Supply chain support for multiple stores in differnt countries:**
  - **Boundaries:** This functionality covers the central supply chain management system, physical warehouses, inventory tracking systems in stores, and logistics hubs that manage product flow between countries and locations. It also includes communication lines with third-party suppliers and inventory visibility through the online store.
  - **Exclusions:** Customer payment data, employee HR systems, and promotional data are excluded, as they do not directly interact with supply chain operations.
- **Stock and delivery management:**
  - **Boundaries:** This functionality includes each store's local inventory systems, central stock database, delivery management modules, and physical assets (e.g., vehicles for delivery). Data flows between the central stock system, the online store's order processing infrastructure, and delivery tracking systems.
  - **Exclusions:** HR data, non-operational customer information (e.g., marketing preferences), and internal business reporting systems are not part of this boundary.
- **Clinet's inoformation storage:**
  - **Boundaries:** This functionality encompasses the web application for the online store, customer data storage systems (cloud-based or local databases), and secure payment processing systems.
  - **Exclusions:** Physical delivery assets (e.g., delivery trucks), employee information, and supply chain systems are not part of this boundary, as customer data is kept separate from these operational areas.
- **Employee information management:**
  - **Boundaries:** This functionality includes HR systems for managing employee data, access control systems (both physical and digital), and physical security measures such as ID badge access points and surveillance in HR offices.
  - **Exclusions:** Customer data, supply chain operations, stock data, and delivery management systems are excluded, as employee information remains within HR-specific systems and physical spaces.

- **Promotions Information Management:**
  - **Boundaries:** This functionality includes marketing and promotional data systems, the online store's interface where promotions are displayed, and physical assets such as in-store digital signage and POS systems to apply discounts. The online infrastructure supports consistent promotional offers across all locations and customer channels, and promotional data flows between the central management center, the online store, and store-specific systems.
  - **Exclusions:** Physical delivery infrastructure, employee-specific systems, and supply chain data are excluded, as promotional information is directed solely toward customer-facing elements of the business.
- **Physical Assets:**
  - **Boundaries:** Physical assets include all tangible items essential for the company's operations, such as data centers, on-site servers, store hardware (POS systems, computers, routers), security equipment (e.g., video surveillance cameras, access control systems), and delivery vehicles. The boundary also includes warehouses and inventory storage areas, where products are stored and processed for delivery.
  - **Exclusions:** Digital infrastructure (e.g., online applications, databases), customer-facing systems, and promotional information management systems are outside this boundary as they involve non-physical elements that do not require direct physical handling.
- **Online Store:**
  - **Boundaries:** The online store includes the e-commerce web application, customer interface, backend systems supporting product listings, shopping carts, and order processing infrastructure. It also includes payment processing gateways, customer account management systems, and the infrastructure for promotional data display.
  - **Exclusions:** Physical delivery assets and in-store systems (such as physical POS systems and in-store stock management) are outside this boundary, as the online store operates within a purely digital environment.
- **Online delivery management infrastructure:**

- **Boundaries:** This functionality includes the software and systems for order fulfillment, delivery routing, real-time tracking, and coordination between warehouses and delivery teams. The boundary encompasses online applications that allow customers to track their orders, internal systems for dispatching orders to the closest store or warehouse, and inventory visibility across stores. Additionally, GPS tracking devices in delivery vehicles, delivery scheduling tools, and customer notification systems (e.g., SMS or email alerts) are part of this infrastructure.
- **Exclusions:** In-store inventory systems, customer service data (such as customer inquiries unrelated to deliveries), and employee-specific HR data are excluded, as delivery management is solely focused on the logistics of order fulfillment and delivery tracking.

1c) Risk Tolerance Analysis

The risk tolerance analysis should evaluate the organization's capacity to withstand potential attacks and incidents. This entails assessing the level of risk the organization is willing to accept before its operations are significantly impacted. Given that the organization has already implemented some security measures, we can reasonably conclude that its risk tolerance ranges from moderate to low. This is evidenced by their commitment to investing in robust security solutions to safeguard their operations.

System categorization serves as a crucial initial step in formulating an effective risk management plan. With this foundation in place, the next step focuses on risk identification and assessment. This step will encompass asset valuation, threat assessment, and vulnerability assessment.

3. Risk Identification and Assessment

Identification, valuation and categorization of information systems assets are critical tasks of the process to properly develop and deploy the required security control for the specified IT assets.

For this stage, an excel presented during the risk assessment classes was used as a guideline and the link to the tables is the following (The sheets were also delivered in the work submission): https://docs.google.com/spreadsheets/d/1Lc6f3t6Vmd_WSZbndYOLCy5_kqMYuhYo/edit?gid=129065518#gid=129065518

In order to minimize the amount of subjectivity in the work, here are all the assumptions made during the work:

- → The analyzis is on a yearly basis
- → The company does not have training programs to keep staff up-to-date on new procedures, technology and emergency protocols
- → The company is regularly victim of attempted Cyberattacks
- → The video cameras are connected to the power of the building and they don't have failure protection mechanisms
- → The company has a well-functioning access control system and logging system that handles, respectively, staff permissions and attendance register
- → The backup databases are isolated from the normal databases, and only the person responsible for restoring the system has the authorization to access it
- → Transport vehicles are owned by the company and are stored in the Management and Control Center Building
- → Transport vehicles are driven by staff from the company
- → The store is in Porto and the probability of an earthquake of magnitude 8 on the Ritcher scale is 10%
- → The hospital has outdated cybersecurity measures to protect against ransomware attacks, data breaches, or unauthorized access to sensitive information
- → The company has is own server and is running on a physical location like the Management and Control Center.

All the decisions made were thought out in such a way as to consider different points of view.

4. Risk Control Strategies

Risk control strategies are approaches that organizations use to manage, mitigate, or eliminate risks identified during the risk assessment process. These strategies are designed to reduce both the likelihood and potential impact of risks, enabling the organization to function smoothly and meet its goals.

As in the previous section, here is the link to a wide range of selected controls that can protect all assets from different vulnerabilities, https://docs.google.com/spreadsheets/d/1Lc6f3t6Vmd_WSZbndYOLCy5_kqMYuhYo/edit?gid=330509641#gid=330509641

Here's an explanation of each control and its importance to the retail company:

- **Data Operation Policies (Authentication, Encryption)**: Implementing and monitoring policies for secure data handling, such as strong authentication and encryption, helps protect sensitive information like customer payment details and employee data. This control minimizes the risk of data breaches and unauthorized access, safeguarding the company's reputation and customer trust.
- **Fire Detection System**: Installing a fire detection system in stores, warehouses, and data centers helps identify fire hazards early, protecting valuable assets, including inventory, physical records, and IT equipment. Early detection reduces the risk of major disruptions and asset loss.
- **Fire Extinguishers**: Having fire extinguishers readily available allows employees to quickly respond to fires, preventing them from spreading and causing severe damage. This control is critical for ensuring employee safety and protecting physical assets.
- **Regular Software Updates/Patching**: Regularly updating and patching software helps address known security vulnerabilities, reducing the likelihood of cyberattacks. This control protects the company's IT infrastructure, including point-of-sale (POS) systems and customer-facing applications, from malware and other threats.
- **Security System (Anti-theft, Alarm)**: An anti-theft security system with alarms deters theft and unauthorized access to physical assets in stores and warehouses. This control is vital for preventing financial losses from theft and protecting high-value inventory.
- **Intrusion Detection System (IDS)**: An IDS monitors network traffic for suspicious activities, such as unauthorized access attempts or malware. Early detection of intrusion attempts allows the company to respond quickly, minimizing potential damage to sensitive data and IT systems.
- **Security Training for Employees**: Educating employees on security best practices helps reduce human error, a common vulnerability in security. Training employees on topics like

phishing, password management, and physical security enhances their awareness and minimizes risks.

- **Outsourcing Online Store Hosting**: Hosting the online store with a reputable third-party provider offloads security responsibilities, such as server maintenance and data protection, to a specialized team. This control ensures the online store is maintained with high-security standards, reducing operational risks and enhancing uptime.
- **Monitoring Network Traffic**: Continuous network monitoring enables the early detection of anomalies or potential threats, allowing for quick intervention. This control is crucial for protecting customer and business data, maintaining network integrity, and avoiding downtime.
- **Uninterruptible Power Supplies (UPS)**: UPS systems provide emergency power during outages, allowing the company to protect sensitive electronic equipment and maintain critical operations. This is especially important for point-of-sale systems and IT infrastructure that support real-time operations.
- **Multi-Factor Authentication (MFA)**: MFA strengthens access controls by requiring additional verification (e.g., SMS code, app prompt) beyond passwords. This control reduces unauthorized access to sensitive systems, protecting customer data and business information.
- **Regular Equipment Maintenance**: Scheduling routine maintenance for inventory equipment, such as barcode scanners and POS systems, ensures they function optimally and securely. This helps avoid disruptions, equipment breakdowns, and security vulnerabilities due to outdated hardware.
- **Security Audits and Assessments**: Regular audits and assessments help identify weaknesses in the company's security framework, such as outdated software or policy gaps. These evaluations provide actionable insights, helping the company proactively strengthen its security posture and mitigate potential risks.

Together, these controls form a comprehensive strategy to protect the company's assets, maintain operational continuity, and enhance its ability to respond to potential threats. Effective risk control strategies may combine multiple approaches, customized to address specific situations and risk types. Organizations should regularly review and update these strategies to adapt to evolving environments and emerging threats.

5. Malicious attack on the Management and Control Center

After the risk management analysis has been completed, it is asked to discuss a malicious attack on the management and control center and how it would affect the normal operation of the stores and how the controls and security measures implemented would help to reduce its impact.

Three scenarios are considered for analysing the magnitude of the intrusion resulting from the attack.

First Scenario: Minimal Intrusion

In this scenario, the attackers gain limited access to the management center's network, such as viewing non-sensitive business information or low-level operational data. While no highly confidential data is accessed, this scenario still has the potential to disrupt operations.

- **Security Properties Affected**: Confidentiality and integrity are slightly impacted, as unauthorized viewing of data may expose minor operational insights or scheduling information.
- **Impact on Business**: Minor disruptions might occur if attackers slightly alter inventory records or operational data, leading to errors in store replenishment schedules or delayed product availability. Since the attackers only have limited access, this attack would be relatively easy to execute, possibly through phishing or weak access controls.
- **Risk to Organization**: The risk in this scenario is moderate; operational disruptions could affect the efficiency of some store functions without significantly impacting customers.
- **Countermeasures**:
  - **Intrusion Detection Systems (IDS)**: IDS helps detect unusual activity in real-time, enabling swift identification and response to unauthorized access attempts, minimizing disruptions.
  - **Multi-Factor Authentication (MFA)**: MFA on all access points adds an additional layer of security, reducing the likelihood of unauthorized access by verifying user identity beyond a simple password.

Second Scenario: Attempted Arson in the Management and Control Center

In this scenario, an individual attempts to start a fire inside the management and control center, which houses critical infrastructure for supply chain operations, centralized data storage, and coordination across multiple stores. A fire in this location could disrupt the entire network of stores and impact both online and in-store operations.

Such an event could result from intentional arson or accidental ignition, but in this case, it's considered malicious intent.

- **Security Properties Affected**: Availability, integrity, safety, and confidentiality are impacted. A fire could render critical systems unavailable, disrupt access to essential operational data, and compromise the integrity of centralized information. Confidentiality is also at risk if backups and data storage are destroyed, potentially exposing sensitive customer, employee, and business data. Additionally, the immediate safety of employees is at risk, requiring quick evacuation and emergency response.
- **Impact on Business**: A fire in the management and control center would likely have a widespread impact, halting inventory coordination, delaying order processing, and affecting communication across stores. This disruption could lead to revenue loss, customer dissatisfaction, and potential data recovery challenges. If customer data is affected, the company might face reputational damage and possible regulatory consequences.
- **Risk to Organization**: The risk level is severe, as the management and control center is a critical hub for operations. A fire here could lead to extensive downtime, data loss, and significant financial and reputational repercussions. The organization may also face regulatory penalties if customer or employee data is compromised.
- **Countermeasures**:
  - ❖ **Fire Detection System**: Early detection through smoke or heat sensors enables a swift response, automatically alerting fire services and center control management. Fast detection minimizes the fire's spread, limiting potential damage and helping to protect employees and customers.

- ❖ **Fire Extinguishers and Training:** Equipping stores with accessible fire extinguishers and training employees in their proper use allows for immediate action in the event of a small fire. This preparedness can prevent fires from escalating, especially in high-risk areas like servers room.

Third Scenario: Severe Intrusion

In this scenario, attackers gain extensive access to sensitive systems within the management center, including customer information, supply chain operations, and employee data. This level of intrusion could result from a combination of sophisticated phishing, exploiting unpatched vulnerabilities, or gaining access through third-party service providers.

- **Security Properties Affected**: Confidentiality, integrity, and availability are all heavily impacted. Attackers may access and steal sensitive customer or employee data, alter supply chain records, or even disrupt key services.
- **Impact on Business**: A severe intrusion could halt inventory coordination, disrupt order processing, and lead to breaches of customer data, which could harm customer trust and damage the company's reputation. This level of attack could potentially bring store operations to a standstill if communication with the control center is interrupted.
- **Risk to Organization**: The risk is high, as a severe intrusion can lead to data breaches, financial losses, customer trust damage, and regulatory consequences due to compromised data.
- **Countermeasures**:
  - ❖ **Data Encryption and Backup**: Encrypting sensitive data at rest and in transit ensures that data cannot be easily read by attackers. Regular backups support quick data restoration, minimizing downtime and loss.
  - ❖ **Security Training for Employees**: Comprehensive security training mitigates the risk of phishing and other social engineering attacks by equipping employees with the knowledge to recognize and report suspicious activities.

6. Conclusion

In conclusion, this risk management plan for the retail company establishes a comprehensive approach to identifying, assessing, and controlling risks across the organization. By systematically categorizing key functionalities, this plan defines the boundaries necessary to apply selected security controls. The company's moderate to low risk tolerance, along with its existing security measures, reflects its commitment to protecting sensitive information, ensuring business continuity, and maintaining customer trust.

Implementing a combination of defence, mitigation, transfer, and acceptance controls provides a balanced approach to managing identified risks. Defensive measures like multi-factor authentication, fire detection systems, and intrusion detection systems protect critical assets, while mitigation controls such as regular software updates and network monitoring reduce vulnerabilities. Outsourcing the online store hosting offloads some risk, while regular audits and training programs enhance the overall security posture by promoting awareness and adaptability among employees.

Such a risk management plan structuring allows the company to arm itself with greater security against a constantly changing threat environment, enhancing its ability to withstand and recover from threats, and ensuring compliance with modern security regulations. Going forward, monitoring, periodic reassessments, and adaptive strategies will be vital to ensuring that enterprise-wide protection is responsive to new risks.