Co-funded by the Erasmus+ Programme of the European Union

secureu
DIGITAL EDUCATION TOOLS FOR SECURITY RISK MANAGEMENT

ERASMUS+ Strategic partnership "Digital education tools for security risk management"
Project number: 2021-1-LV01-KA220-HED-000023056

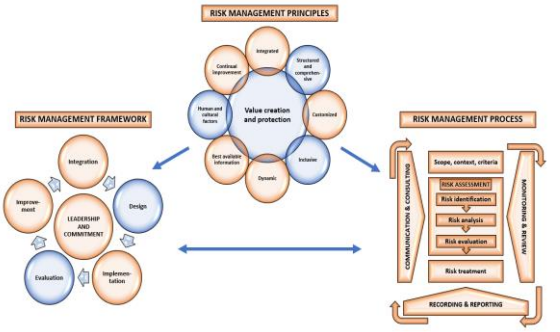
EXERCISE FOR SECURITY STUDENTS

Security Risk Management Cycle and the Administrative Organization (ISO 31000 and COSO)

AUTHORS: Lambert Bambach

BACKGROUND:

The security manager must be aware of the operation of the internal control measures, because he can contribute to the implementation and maintenance of the correct risk control measures based on his specific knowledge of security. Depending on the context and goals of an organisation, is started with one of the building blocks of the ISO 31000:2018 to realize security risk management. The most applicable building block should be chosen for that individual case.

REFERENCE TO ISO 31000 STANDRD According to the ISO 31000 standard, the building block Risk Management Process and the sub-building blocks improvement, integration, implementation, continual improvement, integrated, customized, dynamic, best available information are involved	

GOAL OF THIS EXERCISE:

The students will advise the security division of an organization on the basis of three cases. The advice will be based on Security Risk Management Cycle and the Administrative Organization. They must indicate substantiated:

- What needs to be done with regard to Administrative organization;
- What needs to be done with regard to Information-driven working;
- Where to start in the Security Risk Management Cycle;
- Why do you start there?
- What are you going to do?
- Who will be your allies?

TASK DESCRIPTION FOR STUDENTS:

1. Form groups as instructed by teacher
2. Each group is given three cases to work on
3. Under guidance from teacher, define What needs to be done with regard to Administrative organization: What needs to be done with regard to Information-driven working; Where to start in the Security Risk Management Cycle; Why do you start there?; What are you going to do?; Who will be your allies?
4. Familiarize yourself with the theory of the Administrative organisation and the building blocks of the ISO31000. Also familiarize yourself with the building blocks of your choice which you use for your approach and write down the results of your choice for approach, concerning What needs to be done with regard to Administrative organization: What needs to be done with regard to Information-driven working; Where to start in the Security Risk Management Cycle; Why do you start there?; What are you going to do?; Who will be your allies?
5. Prepare a short presentation for your fellow students in the other groups about the results of your choice for approach, concerning: What needs to be done with regard to Administrative organization: What needs to be done with regard to Information-driven working; Where to start in the Security Risk Management Cycle; Why do you start there?; What are you going to do?; Who will be your allies?
6. Present your presentation for your fellow students in the other groups.
7. Listen the presentations of the fellow students. After each presentation discuss 2 minutes with your group if their approach of the cases would have been applicable for you too. Share your thoughts with the class in your turn. Would your approach per case been different knowing due to the new insides given by the other group(s)?
8. After all presentations discuss in your group which of the presented approaches would be best for each case. Share your thoughts with the class.

TASK DESCRIPTION FOR TEACHER / TRAINER:

1. Before class, estimate the number of students and how many groups of approximately four students they would form.
2. Before class, for each group should have a copy of the ISO 31000: 2018, The case and have read the article on Administrative organisation.
3. Optionally:
    - If you wish the exercise to be carried out in a physical location, make sure you have access and proper facilities within it. You may also want to divide the facilities for the groups beforehand.
4. In class, assign students into groups of approximately four students.

5. Instruct students to familiarize themselves with the ISO 31000:2018; The case and the article on Administrative organisation.

6. Instruct students to write down the results of their choice for approach this can be done on e.g., post-it notes, on the whiteboard, PowerPoint presentation, in an online environment, etc. Instruct students to prepare to present their results to their fellow students. You can decide the delivery method of the presentation. It is recommended to limit the presentation to max. 5 minutes.

9. While the students discuss their approach, they write down their choice for the approach and prepare their presentation on: What needs to be done with regard to Administrative organization: What needs to be done with regard to Information-driven working; Where to start in the Security Risk Management Cycle; Why do you start there?; What are you going to do?; Who will be your allies? Your task is to facilitate their work and assist if they have questions.

7. Instruct students to present their short presentation for their fellow students in the other groups about the results of your choice for approach, concerning: What needs to be done with regard to Administrative organization: What needs to be done with regard to Information-driven working; Where to start in the Security Risk Management Cycle; Why do you start there?; What are you going to do?; Who will be your allies?

8. During presentations, make sure to chair the discussion and keep the groups within the given schedule. The process is as follows:
    - Approx. max. 10 minutes for one group presentation
    - After each presentation groups should discuss 2 minutes within their groups if the presented approach would have been applicable for their approach.
    - Groups are encouraged to share their thoughts with the class. The key question is: would the choice for approach give you different results?

9. After all presentations, lead all students in a discussion of which of the presented approach would be best.

ADDITIONAL SKILLS THAT THE STUDENT ACQUIRES THROUGH THIS ASSIGNMENT:

- Working in a group
- Working under time pressure
- Giving presentation and arguing their case
- Comparison skills and critical thinking

CASE SECURITY RISK MANAGEMENT AND THE ADMINISTRATIVE ORGANIZATION

The Logistic Organization

Direction

THE LOGISTIC ORGANIZATION has 14 physical stores (the 'stores'), a webshop and one national distribution center warehouse warehouse. THE LOGISTIC ORGANIZATION has a turnover of € 370,000,000 per year, of which € 270,000,000 for the physical stores and € 100,000,000 for the web shop. THE LOGISTIC ORGANIZATION's position in the market is as strong as its relationship with its customers. The long-term relationship with customers is therefore central to its strategy.

Vision

- Customer experience
- Customer centered

- **Mission**
- Empathy (feeling): THE LOGISITIC ORGANIZATION knows the individual needs of the customer.
- Expertise (knowing): THE LOGISITIC ORGANIZATION has the knowledge to meet the individual needs of the customers.
- Experience (can): THE LOGISITIC ORGANIZATION introduces you to the best electronic products

Values

- Customer first
- Do what you say
- Realizing ideas
- Always better

Promises

- Better for the customer
- Better for the employee
- Better for the environment

Business model

- Lower costs
- Strong brands
- Wide range of products

Strategic pillars

- Strong customer loyalty
- Broadening of the range of products available
- Online sales
- Attractive products
- Corporate responsibility
- Good for our people

Ambition

- Always better
- Growth in turnover and profit
- Reduction of losses and costs through better control of primary processes

The service level of THE LOGISITIC ORGANIZATION is high. Short delivery times and lowest price including service ensure that THE LOGISITIC ORGANIZATION looks closely at the contribution that products make to profit.

Developments

- Stock is kept to a minimum. Measurability is essential, whether it's advertising campaigns, inventory control or loss prevention;

- The THE LOGISITIC ORGANIZATION also wants to introduce self-scan of articles to increase convenience for the customer;

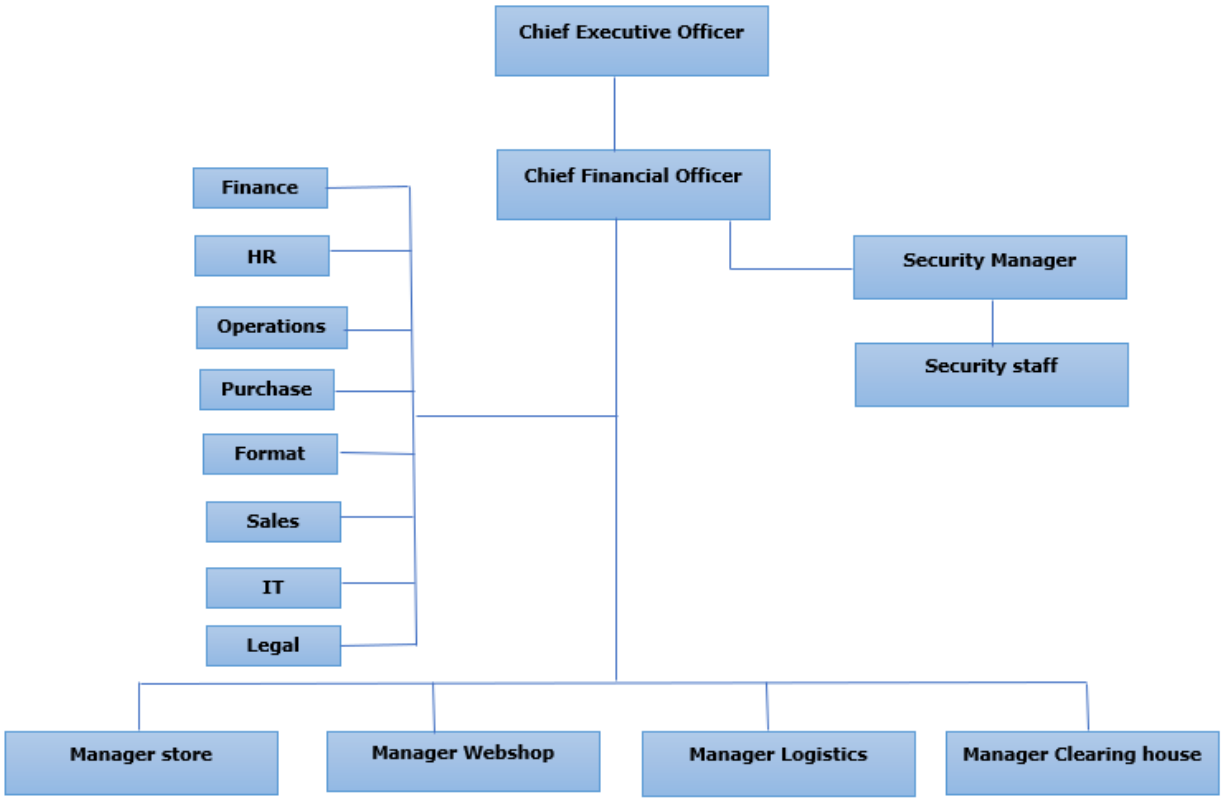
- In addition, THE LOGISITIC ORGANIZATION wants to achieve a growth in profits by increasing online sales;

- In store and online, the same price applies. If a consumer can order the desired product cheaper elsewhere, THE LOGISITIC ORGANIZATION will deliver it for that same price. In this way, THE LOGISITIC ORGANIZATION prevents customers from delaying their buying decision;

- THE LOGISITIC ORGANIZATION delivers within 24 hours after ordering the products;

- THE LOGISITIC ORGANIZATION is currently developing THE LOGISITIC ORGANIZATION - Smart. From these smaller hubs in shopping centers, the electronics chain wants to experiment with express delivery. The Smart stores will be located in larger shopping centers where customers can go for a smaller range of products and advice. In the Smart hubs, omnichannel is becoming the norm. Via invisible walls in the store, customers can check whether a product is available, what it looks like and place orders. As a vision for the future, THE LOGISITIC ORGANIZATION sees that these orders are delivered to the customer's home the same day.

Arrangement



Organization chart of THE LOGISITIC ORGANIZATION

Managers stores, web shop, logistics and distribution center warehouse

As far as is known, the managers have no substantive tasks and responsibilities in the field of security, but are responsible for the management of the employees in the field of safety in the stores, the web shop and the distribution center warehouse.

Manager support departments

As far as is known, the managers of the Finance, Operations, Purchasing, Format, Sales, IT, Legal departments have no substantive tasks and responsibilities in the field of security, but are responsible for managing the employees in their department.

Security

Security is organized at a central level. Security is a staff service. As far as is known, the Chief Financial Officer has no substantive tasks and responsibilities in the field of security, but is still accountable for the Security department and managing the head of the Security. reports to the Chief Executive Officer. The budget of the Security department is set at group level. Every organizational unit of THE LOGISITIC ORGANIZATION can call on the Security department when it deems it necessary. Expenses for investments and costs of maintenance are borne by the THE LOGISITIC ORGANIZATION.

Security Manager

The Security Manager is responsible for managing, planning and leading the implementation of the security arrangement. This arrangement was developed at the head office, the risk classification process is part of this. In addition, the head of the security department and his department support the national and local management by performing tasks such as conducting investigations, security audits and ensuring that the stores, the web shop and the distribution center warehouse comply with the legal regulations. In addition, the manager oversees THE LOGISITIC ORGANIZATION security standard, instructions, guidelines, etc.

Security staff

Employees of the Security department perform the following tasks:

- Supporting operational management in the field of security;
- Assisting in preparation for audits (internal assessments, investigations) and supporting in the follow-up and measures;
- Collect details of incidents and report them to local management;
- Support in investigations into internal fraud;
- Evaluating industry information and discovering threats;
- Implementing THE LOGISITIC ORGANIZATION security standard, instructions, guidelines, etc. in collaboration with the Security Manager;
- Check installed physical security equipment for possible defects or malfunctions;
- Provide general security information and the Security Awareness For Employees (SAFE) training, and provide this training for local staff;
- Reporting the results of these activities to the head of the Security department;
- Making risk analyses and adjusting measures accordingly.

The Security department is responsible for:

- Background check of new employees and contractors;
- Risk inventory & evaluation (work processes, security);
- Management of the external security guards;
- Toolbox meetings on risks;
- Access control;
- Camera surveillance;
- Incident investigation;
- Business continuity planning;
- Risk management;
- Organizing workshops on awareness, insider threat etc.

Shops, web shop, distribution center warehouse warehouse

The current THE LOGISITIC ORGANIZATION consists of 14 stores, a web shop and a distribution center warehouse which are connected by a logistics process.

THE LOGISITIC ORGANIZATION has its own stores and a franchise formula. Franchisees pay for the use of the formula. For these own stores and franchisees, THE LOGISITIC ORGANIZATION arranges central purchasing, distribution center warehouse, logistics process, publicity, maintenance, security and the web shop. The franchisee arranges personnel matters, opening hours, store location, insurance, etc.

The shops

THE LOGISITIC ORGANIZATION has 14 stores. The stores are high end consumer products retailers. The process in the store is characterized by inbound, storage and removal of products. The flow rate of the goods is tracked by registering old and expired products and products that are still in stock in the store and which need to be reordered. The stores are supplied once a week. The stores have a mixed assortment. All products are for sale in all stores and are in approximately the same place in all stores. The promotions that the store has in certain weeks of the year are placed on the headlines of the store. THE LOGISITIC ORGANIZATION uses an app, a loyalty card and Wi-Fi tracking of customers in the store.

Shop

THE LOGISITIC ORGANIZATION believes in full integration of offline and online. By integrating the web shop and the store, the products can reach the customer quickly at a competitive price, with personal service. In addition, there are internet-only products.

Distribution center warehouse

From the distribution center warehouse, deliveries are made once a week to the stores of THE LOGISITIC ORGANIZATION. In principle, the goods purchased via the web shop are delivered directly from the distribution center warehouse to the customer. If the customers want to pick up the goods ordered online in the store, they will be delivered to the stores via the distribution center warehouse. Those orders are delivered to the stores daily by an external distributor. Just like in the stores, the process in the distribution

center warehouse is characterized by inbound, storage and removal of products. In the distribution center warehouse, pallets are 'picked' and prepared for transport. This complete process requires good cooperation between, among other things, the stores, the web shop and the distribution center warehouse with goods receipt (*inbound*) and goods distribution (*outbound*).

Logistics

The stores all have their own stock. To maintain the stock in the stores, three systems are used, namely: SAP, POSFlow and TIB.

To manage the stock, THE LOGISITIC ORGANIZATION uses SAP. SAP is an ERP program with which THE LOGISITIC ORGANIZATION manages all goods flows. All items are recorded in SAP, including the specifications and the purchase, transfer and sales prices.

SAP is linked to POSFlow, the POS system of THE LOGISITIC ORGANIZATION. The POS system makes it possible to process sold goods without delay.

SAP determines on the basis of sales how much need there is for a certain product.

External actors

Two external parties are involved in the ordering and return process: CEVA and DHL

CEVA is one of the world's largest supply chain management companies. CEVA has agreements with THE LOGISITIC ORGANIZATION regarding the storage, shipping and receipt of goods.

DHL is the transport company that transports all goods for THE LOGISITIC ORGANIZATION.

The security manager maintains good contacts with fellow security managers of similar logistics organizations. The security department also has good contact with the national police.

Stock

The Purchasing department determines how much stock should be present in each store. This way of ordering connects to the Internet of Things (IoT), which means that objects connected to the internet communicate with each other and automatically start a process. The IoT is becoming increasingly important for logistics.

THE LOGISITIC ORGANIZATION has two important processes in the supply chain, namely the automatic ordering process and the return process.

The automatic ordering process

The process by which products are automatically ordered by SAP to maintain stock is also called the automatic ordering process. SAP analyzes the sales data and determines the optimal order moment and the optimal order quantity. The moment SAP detects that there are not enough items in stock in a store, SAP automatically creates an order for the store in question. POSFlow provides and SAP with the sales data, so that the stock can be monitored.

The return process

In addition to the automatic ordering process, there is the return process. Every Monday a Return Merchandise Authorization (RMA) is created in the store. An RMA consists of mandatory returns and Death On Arrival (DOA). Dead on Arrival is a term which indicates that an item or merchandise received by a buyer was found defective or broken on arrival. After creating the RMA, DHL picks up the order and sends it to DHL. There, the products are returned to the third party or stored in the warehouse.

Direct deliveries by producers

The automatic ordering process supports the supply of 60% of the stores from the distribution center warehouse. The supply of the remaining 40% of the stores is provided by producers of goods with which THE LOGISITIC ORGANIZATION has concluded a contract. The representatives of these producers themselves go to the stores to inspect and fill the shelves of their products. In addition, they may replenish stocks if the branch needs them. The stores do not check the content of the delivery, they may supplement the shelves with stock that the representatives have delivered there. Employees of the store sign on the packing slip for receipt of the goods and enter the items into SAP. The same products can also be delivered via the distribution center warehouse with the same barcode.

In-store delivery and pick-up

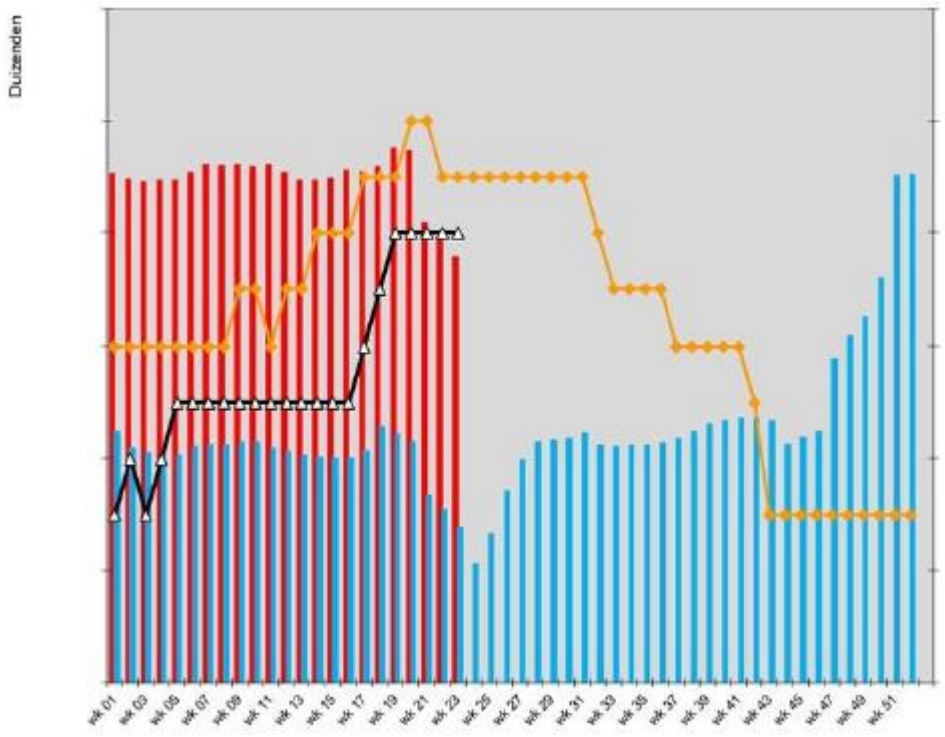
The DHL courier will park the bus as close to the store as possible. He then unloads the necessary goods. The moment he enters the store, everything is recorded by the cameras. The DHL employee walks to an employee of the store and he then goes to the back office to pick up the goods that need to be taken by the courier.

CASES

CASE I

Suspicion of loss due to organized crime

There are suspicions that organized crime is a problem for the organization. The Chief Financial Officer wants security measures to be taken. The financial analyst indicates that undefined leakage is a major problem within THE LOGISTIC ORGANIZATION. Theft accounts for 33% of the entire leakage. There is a large increase in the area of undefined leakage compared to last year. Undefined leakage indirectly affects the mapping of organized crime. Undefined leakage means that the leak has not been mapped by THE LOGISTIC ORGANIZATION and is only detected later. This creates a less concrete picture of what the leakage figures consist. This contributes to the inability or impairment of organized crime. If (more than) half of the leakage cannot be mapped, it cannot be clearly described how big the impact of organized crime actually is on the leakage figures. Overall leakage rates have increased by 6.41% compared to the same period last year. The LOGISTIC ORGANIZATION has a target of 0.20% in terms of leakage. That is the total amount (at purchase price) that was stolen divided by the total gross turnover.



Sales 2023 Sales 2022 Shrinkage 2023 Shrinkage 2022

The figure shows that the percentage of leakage is lower compared to last year, but that this is due to the increased turnover. In absolute terms (amounts), thefts, and therefore leakage, have increased. If the turnover this year had been the same as last year, the leakage rate might have doubled.

CASE II

Registration of deviations

It appears that the procedures are not being followed structurally at the moment. In some cases, the reports do not go through the Logistics department. As a result, they are not always aware of these reports. In other cases, the Logistics Department does not follow through on the reports for various reasons. These factors influence the registration of deviations in such a way that a precise number of deviations cannot be mentioned by all parties. Logically, this entails dark numbers.

Goods are regularly booked by an 'unauthorized' person. An unauthorized person is understood to mean a flex worker who books goods using the store's login details. Just as with booking, the booking must be done by an employee with his or her own cash register code. It is not checked whether the stores still use the shop login. It is noteworthy that the RMA number is not communicated to DHL. The remarkable thing about this is that there is no control mechanism.

Case III

Risk inventory

There is no security-oriented risk inventory. The organization monitors its risks with the security audit. However, this instrument does not provide specific information on the nature and extent of risks. This means that no analysis is made of the threats and what damage they can cause to THE LOGISTIC ORGANIZATION.

There is also no method by which external information and knowledge are inventoried, analyzed and translated into policy. For example, there is a lack of a method with which information or research about crime in the retail sector is translated into security policy. This creates a gap between the development in the field and the position of THE LOGISTIC ORGANIZATION in the field of security.

Due to the lack of an extensive process of a threat and risk inventory, the organization is unable to effectively align security measures with the security risks that the organization runs. The risk inventory is currently not leading when making choices for security measures. There is a lack of a complete record of regular inspections and observations.