MESTRADO EM
GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO

TRABALHO DE PROJETO

Self-Scanning Solution in Retail: Risk Assessment

Stanislav Shapovalov

Out – 2017

MESTRADO EM GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO

TRABALHO DE PROJETO

Self-Scanning Solution in Retail: Risk Assessment

Stanislav Shapovalov

ORIENTAÇÃO:

SÉRGIO RODRIGUES NUNES

Professor Auxiliar Convidado

Out - 2017

Index

Abstract - EN

Lidl Shop&Go solution is an innovative self-scanning service being tested in Portuguese stores in a pilot phase. The aim of this project is to evaluate an added risk exposure of the solution itself and its impact on existent infrastructure from Information Security (IS) perspective. To succeed, a review of Risk Assessment (RA) frameworks is performed and Octave Allegro method is selected as the best fit for purpose. The findings of the RA are classified according to their expected probability, business impact, information asset profile and container the information resides in. In the end of the assessment, a suggestion of mitigation measures is presented. In addition to Octave method, these measures are prioritized according to their implementation effort and impact on the number of Threat Scenarios. The resulting list of findings is used together with other evaluation criteria to assess the full-scale deployment of SHOP&GO project in future by management. Main identified topics for improvement are secure communication, improvements in physical security policy, password and patch management revision and awareness of the store personnel / IT personnel. The output of this project can be used as a reference by organizations within the industry, which are planning any similar type of deployment. As this RA involves only the first iteration, its results are sufficiently generic and applicable to other sites and projects with the same scope.

Resumo - PT

A solução Shop & Go da Lidl é um serviço inovador de *self-checkout* testado em lojas portuguesas em fase piloto. O objetivo deste projeto é avaliar a exposição de risco acrescentada que a solução traz juntamente com o seu impacto na infraestrutura existente na perspectiva da Segurança de Informação. Para o projecto suceder foi feita uma revisão de *frameworks* de avaliação de risco e o método Octave Allegro selecionado como a melhor solução para o efeito. As conclusões da avaliação de risco são classificadas de acordo com a probabilidade esperada, o impacto no negócio, o perfil de ativos de informações e o contentor em que a informação reside. No final da avaliação, é apresentada uma sugestão de medidas de mitigação. Além do método Octave, essas medidas são priorizadas de acordo com o esforço de implementação e o impacto no número de cenários de ameaças. A lista de resultados resultante é usada em conjunto com os outros critérios de avaliação para avaliar a implementação em grande escala do projeto SHOP & GO no futuro. Os principais tópicos identificados para melhoria são comunicação segura, melhorias na política de segurança física, revisão de gestão de *passwords* e *patches* e consciência do pessoal da loja / pessoal de TI. Os resultados deste projeto podem ser usados como referência por organizações do setor, que estão planear qualquer tipo de implementação similar. Como esta avaliação de risco envolve apenas a primeira iteração, os seus resultados são suficientemente genéricos e aplicáveis a outros locais e projetos com o mesmo âmbito.

Problem definition

Information security is a kind of risk that is transversal to IT and business areas in an organization. This fact is accepted by the majority of organizations, but few of them effectively align their risk management policies from IT and functional areas. It is not a common practice to apply transversal risk assessment and management policies to the organization as a whole. (Aven, 2016)

Lidl Group is a multinational organization with its Headquarters based in Neckarsulm, Germany. It unites more than 10.000 stores in 30 countries worldwide. A SHOP&GO is a developing self-scanning solution for Lidl customers in the stores – a customer may use his smartphone for item scanning via built-in camera and check out in a more rapid way than at conventional POS. Currently, several countries participate in the pilot phase of the SHOP&GO, Portugal is one of them. This paper describes the process of risk assessment and management recommendations applied to the SHOP&GO project itself, and the attack vectors it adds to an existent store infrastructure.

SHOP&GO rollout adds multiple information containers and infrastructure devices to the baseline configuration of Lidl store. The scope of this study is limited to this added value – added attack vectors through such devices to existent critical information assets at Lidl, like GDPR compliant personal data or PCI DSS compliant payment data, among others.

Lidl International has well defined internal risk assessment policies with proper tools, but as any tools, they have their limitations. First of all, they are IT asset-oriented, and not information oriented. Secondly, the results produced by these tools are not granular enough for comparison purposes between assets what makes a decision making the process difficult.

This project's aim is to select the proper framework and apply it to SHOP&GO project, providing a comprehensive review of its strengths and weaknesses from IS perspective. To achieve this goal, an analysis of existing methodologies (frameworks) is performed, based on studies and support documents of the initial selection of frameworks. Practical output, or main investigation question, is the evaluation of to what extent the implementation of SHOP&GO leverages the risk exposure of the organization. And what can be done to mitigate possible risks and with what effort. The collateral output of this study is the review of evaluated risk assessment frameworks and selection of the best fit for SHOP&GO risk assessment. By using the chosen framework I highlight some strong points and limitations of it as well.

Current State of Risk Assessment Methodologies

> “Risk and risk assessments are a key piece of any successful, comprehensive security strategy. They substantially help in determining what is most valuable and at the most risk, and can often help to determine what must be done to reduce those risks.” (Visintine, 2003)
>
> Risk assessment and risk management are established as a scientific field and provide important contributions in supporting decision-making in practice. Basic principles, theories and methods exist and are developing in a continuous improvement process (Aven, 2016).

In information security, a risk can be defined as the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) normally based on a particular information security vulnerability and the resulting impact (Elky, 2006). Although, the scientific foundation of risk assessment and risk management is still somewhat shaky on some issues and researchers still argue on the very concept of risk itself– whether the probability approach in risk evaluation should be used at all. There is a shift happening from rather narrow perspectives based on probabilities to ways of thinking which highlight events, consequences and uncertainties (Aven 2012, 2016). This shift, however, is still being studied and its benefits or drawbacks are unclear on the frameworks discussed below.

In regard to Risk Assessment and Management frameworks themselves, there is a vast majority of tools available for today's analyst, free and paid, with government or private sector origins (National Cyber Security Center, 2016). Their structure differs significantly, as ones were born before, or gave origin to the others, as well as adopted different output objectives (e.g. quantitative vs qualitative) (The Open Group, 2009). There are several existing studies aiming to compare the most known frameworks, both within industry and academia.

One of the most complex evaluations was performed by Gartner analysts Tomhave & Heidt (2017) regarding the available RA methodologies on the market. Although without clear top pick definition, it provides an important input of features used in framework analysis. Frameworks were evaluated on their type and ease of use, support materials, time on the market among other criteria. The main conclusion the researchers derive is that qualitatively, there is not a great difference in terms of how all of the methods function. The most important factor is so-called cultural fit. The researchers agree that every method on their list, when well performed, will lead to a similar result, as long as it fits analyst and organization profile. Another important conclusion derived is the convergence of all methods being analyzed to ISO 31000 (Tomhave & Heidt, 2017).

Another research held in academia did the similar analysis and applied the top 3 selected frameworks to the case study, for comparable results. They ended up by selecting OCTAVE, IRAM and IT-Grundschutz as the most representative sample of existent model's universe. The authors admit, however, that selection was subjective and accept the fact that dropped models (Mehari, MAGERIT and EBIOS) were excellent candidates as well. The initial universe was composed of 22 models (Macedo & Silva, 2009).

Another evaluation work worth to mention was performed in 2013 and analyzed the methods used by OCTAVE, IRAM and IT-Grundschutz (Haritha et al, 2013). Although last two researches are quite outdated, their results remain valid for selection purposes as none of the 3 frameworks suffered major updates since the publication.

Common frameworks referenced by authors of these studies were selected to be part of initial framework list to be put in practice with given problem. Features attributed by authors were considered in the process of final framework selection, along with support documentation every method provide. The following list was defined for initial triage. Every tool listed in it is considered to be mature and is being used both by business and academia (ISACA, 2017).

- ISO 31000: Risk management – Principles and guidelines, establishes a number of principles that need to be satisfied to make risk management effective (ISO, 2009).
- ISACA COBIT 5: COBIT (formerly Control Objectives for Information and Related Technology) version 5 is a product of ISACA (formerly Information Systems Audit and Control Association) (ISACA, 2017).
- Factor Analysis of Information Risk (FAIR): a quantitative risk analysis method originally created by Jack Jones (CXOWARE), now a standard from The Open Group (FAIR Institute, 2017).
- MAGERIT: Methodology for Information Systems Risk Analysis and Management, a Spanish standard mandated for use by all government agencies (ENISA, 2017).
- NIST SP 800-30: U.S. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 (National Institute of Standards and Technology, 2012).
- OCTAVE Allegro: developed by Carnegie Mellon University Software Engineering Institute's CERT Division; provides a comprehensive risk assessment framework with details about performing risk analysis and includes the ability to incorporate other risk analysis methods (Caralli et al, 2007).

The terms used in this study include risk analysis, assessment and management. The workflow of complete risk management program follows the same direction – risk analysis gives inputs for risk assessment, which enables further management of given risk.

Framework Comparison

I. Compared Features

To compare the list of frameworks a feature list was defined. They are:

a.) Type of tool - method / framework - complete risk assessment, analysis and management framework; or analysis method. Framework defines an overall risk management process, mostly at macro level, including risk assessment and analysis. (e.g. COBIT 5). Method typically is focused on performing a specific set of analysis functions, with good set of instructions, thus more focused on micro level. (e.g. FAIR)

b.) Type of assessment – qualitative vs quantitative (or mixed).

Quantitative risk measurement is easily represented in monetary terms and comprehensive for public. Quantitative risk measurement is the standard way of measuring risk in many fields, such as insurance, but it is not commonly used to measure risk in information systems. Two of the reasons claimed for this are 1) the difficulties in identifying and assigning a value to assets, and 2) the lack of statistical information that would make it possible to determine frequency (Visintine, 2003). ISO organization defines that, most of the risk assessment tools that are used today for information systems are measurements of qualitative risk (International Standard Organization, 2017). Another consideration when comparing qualitative to quantitative is the ability to produce meaningful output for key users and stakeholders: Qualitative methods tend to produce results such as “high, medium, and low” which can be hard to interpret, as opposed to clear quantitative (normally financial) representation (Tomhave, 2014).

c.) Existence of support materials and specialized tools.

OCTAVE Method, for example, comes with spreadsheets to support its process. FAIR, as well, has a selection of automated tools.

d.) Special skills required or Method flexibility. The more prescriptive methods are designed for a general audience without special or extensive knowledge on a subject. The more flexible methods typically require customization and therefore depend on more experienced risk analysts and training (Tomhave, 2014).

e.) Preparation time and cycle time. Time necessary to complete initial preparation and each iteration previewed by the tool. Qualitative methods tend to have shorter preparation times while quantitative methods tend to have longer times. Because they are more qualitative, NIST 800-30 and OCTAVE likely have shorter preparation times. Of the methods reviewed, COBIT 5 has the longest preparation time due to the degree of customization required. NIST 800-30, OCTAVE, and MAGERIT have mid-range preparation times. OCTAVE is considered to be possessing a medium-long cycle time. FAIR has a shorter cycle time once you get through the somewhat longer preparation time. This is due to the use of automated tools. The questionnaire-based methods require only one iteration, generally; while methods with some sort of tool present are more iterative. High impact and high residual risks are almost always going to require additional, more in-depth analysis (Macedo & Silva, 2009).

II. Custom Weighs and Selection

All the features listed in previous chapter received the attributed weigh. “Table I” illustrates custom weight distribution in regard to features evaluated. Their Weigh correspond to priority chosen to fulfill specific requirements of SHOP&GO risk assessment.

Table I

Feature	***Scale explanation***	***Custom Weight***
Framework/ Method	Framework(1) or Method(5) like	0,1
Quantitative/ Qualitative	Mostly Quantitative(1) or Qualitative (5)	0,25
Support tools available	Poor and expensive (1) or full and free (5)	0,25
Special Skills required	No special skills (1) or highly skill dependent (5)	-0,2
Preparation Time	Less time (1) or more time (5) needed	-0,15
Cycle Time	Less time (1) or more time (5) needed	-0,05

1-Custom Weigh Factors

The most relevant features like method being qualitative, with enough support material and without much special skills required were reflected in this way. Features like Special Skills, Preparation and Cycle time got negative weights given the inverse influence of such on the final mark.

The comparison “Table II” was constructed to compare the frameworks. Feature values were filled in using analyzed works in Chapter 3 as one source and individual support documentation of frameworks as the other.

Additional cultural fit feature was left aside from the main evaluation, so it can be considered in case of a draw. OCTAVE is reported to fit well with an engineering and analytical mindset, and FAIR fits well with analysts who are numbers-oriented. (Tomhave, 2014)

Table II

	Framework/ Method	Weighted Score	Quantitative/ Qualitative	Weighted Score	Support tools available	Weighted Score	Special Skills Required	Weighted Score	Preparation Time	Weighted Score	Cycle Time	Weighted Score	**Final Score**
ISO 31000	1	0,1	4	1	3	0,75	4	-0,8	2	-0,3	2	-0,1	**0,65**
ISACA COBIT 5	2	0,2	3	0,75	3	0,75	4	-0,8	1	-0,15	2	-0,1	**0,65**
FAIR	4	0,4	2	0,5	3	0,75	3	-0,6	4	-0,6	4	-0,2	**0,25**
MAGERIT	3	0,3	4	1	2	0,5	3	-0,6	4	-0,6	4	-0,2	**0,4**
NIST SP 800-30	1	0,1	3	0,75	3	0,75	4	-0,8	3	-0,45	3	-0,15	**0,2**
OCTAVE Allegro	4	0,4	4	1	4	1	2	-0,4	4	-0,6	3	-0,15	**1,25**
Custom Weight Factor		**0,1**		**0,25**		**0,25**		**-0,2**		**-0,15**		**-0,05**	

2 - Framework Comparison

OCTAVE Allegro scored the highest rank in the evaluation. This method is well documented and forgiving for less experienced professionals. It has relatively short preparation time, while being very agile in its cycle times (Carali et al, 2007).

Additional exclusion criteria was the ability of a method to give immediate results, by applying granulated approach. Most organizations do not have a one-size-fits-all risk assessment, given that risk management process is expensive to collect. The solution has to provide the assessment results to fulfill the immediate need along the process as well as create useful data for the future. Such two-tier approach consists of a baseline procedure for general risk assessment and identification (typically qualitative) with more sophisticated methods for deeper analyses of high impact risks that fall outside the baseline (typically quantitative). OCTAVE, compared to FAIR is better suited for such baseline application, as being more quantitative and thus flexible in its application.

Last, but not least factor in favor of OCTAVE method (reflected in "Support Documentation" feature) is its open standard and as such free access to support materials.

It is important to notice once again that the difference in terms of how all of these methods function is not considered to be significant. All the methods tend to converge to international ISO 31000 standard, varying the way they are applied, but targeting the same objectives.

III. Octave Allegro Framework

The OCTAVE Allegro approach is designed to allow broad assessment of an organization's operational risk environment with the goal of producing more robust results without the need for extensive risk assessment knowledge (Alberts & Dorofee, 2009).

OCTAVE Allegro approach differs from previous OCTAVE methods by focusing primarily on information assets in the context of how they are used, where they are stored, transported, and processed, and how they are exposed to threats, vulnerabilities, and disruptions as a result. (Carali et al, 2007).

The work process is divided into 8 sub-processes, falling into 4 activity areas: establishing drivers, profiling assets containers, identifying threats and identifying and mitigating risks. OCTAVE Risk management process cycle follows the next steps:

Step 1 - Establish Risk Measurement Criteria
Step 2 - Develop an Information Asset Profile
Step 3 - Identify Information Asset Containers
Step 4 - Identify Areas of Concern
Step 5 - Identify Threat Scenarios
Step 6 - Identify Risks
Step 7 - Analyze Risks
Step 8 - Select Mitigation Approach

Application of each step is explained and illustrated in the following chapter.

Analysis and Assessment

The following subsections of this chapter will provide general guidance and explanation over the assessment steps performed. Detailed calculations and resulting tables can be found in the Attachments section of this document.

I. Step 1 - Establish Risk Measurement Criteria

The first step in the OCTAVE Allegro process establishes the organizational drivers that will be used to evaluate the effects of a risk to an organization's mission and business objectives. These drivers are reflected in a set of risk measurement criteria that is created and captured as part of this initial step. Risk measurement criteria are a set of qualitative measures against which the effects of a realized risk can be evaluated and form the foundation of an information asset risk assessment (Carali et al, 2007).

In the scope of the current project, Impact Areas' prioritization is conducted in the following way:

Table III

Allegro Worksheet 7	Impact Area Prioritization Worksheet
Priority	**Impact Areas**
1	**Reputation and Customer Confidence**
2	**Safety and Health**
3	**Fines and Legal Penalties**
4	**Productivity**
5	**Financial**

3 – Impact Area Prioritization

As the current assessment is focused on Shop&Go solution itself and not organization as a whole, priorities like Reputation and Safety of the product are elevated in the first place. These are cultural qualities promoted internally by organization and valued as an important asset.

There are 3 Impact Levels defined by Octave Allegro method – Low, Medium and High. This distribution is used to help the assessor(s) in aligning the impact estimation in different areas by linking it to fixed estimated loss. For example, "Low" Impact on Operational Cost in Financial Impact Area may correspond to 5 or less percent of the increase in operating cost. Such mapping permits usage of the same model in different business areas and the delivery of comparable results. It is especially important when two or more people are involved into assessment process, so by performing this step, we can guarantee that everyone "is on the same page" when it comes up to the result comparison.

Other areas like Safety and Health or Reputation are of pure quantitative nature. Detailed Risk Measurement Criteria description can be found in Attachment section: “Attachment I – Risk Measurement Criteria”.

II. Step 2 - Develop an Information Asset Profile

A profile is a representation of an information asset describing its unique features, qualities, characteristics, and value. The methodology’s profiling process ensures that an asset is clearly and consistently described, that there is an unambiguous definition of the asset’s boundaries and that the security requirements for the asset are adequately defined. (Carali et al, 2007).

Information asset profiles mapped in this step are common to the organization as a whole, but they will be used in the universe of Shop&Go instance in a store only. Such strict definition of boundaries is necessary for the next step of Octave Allegro approach – container definition. Information asset as, for example, client data is used and stored in multiple systems/databases. Analyzing their exposure to risk while looking at every possible scenario will go far beyond the target of this project, which is – evaluating added risk by SHOP&GO.

Five main (most critical) information assets are identified:

a) Client and Employee Data

   This type of data is being of, probably, highest criticality to LIDL, given past data loss scandals. It is subject to Private Data regulations imposed by European Union - (EU) 2016/679 - (EU) 2016/680. It is used for billing and Human Resources related processes. Shop&Go product may use such data for identification of customers, their home address for billing purposes, social network account for easy log in etc.

b) Payment Data - PCI DSS compliant

Data Retrieved by cashless payment processes. Used for accounting and controlling purposes, besides payment process itself. Any disclosure or compromise of this data may put in question the PCI DSS certification of LIDL Portugal and harm its reputation.

PCI DSS certification is an ongoing topic for the group and a lot of effort is put into obtaining and maintaining this certification valid. Certain features of SHOP&GO project, as for example mobile payment, may subject compliance with PCI norms.

c) Shop&Go Solution related data

Data type related to Shop&Go solution itself. Being innovative in its nature and still in development, the disclosure of such data may lead to the exposure of known vulnerabilities. The competitors are another concern – statistics from sales and solution architecture are the main topics of interest. Such data will become less important in the long run, but as of the time of this assessment – it remains being a critical asset.

d) Item Related Data

Data related to particular article sold by LIDL, as well as consolidated data of purchases and sales based on time series. It includes everything from manufacturer or supplier contacts to price schedules, campaigns, stock etc. Disclosure of this data may lead to competitive advantage loss, in short or medium term.

e) External Undesirable Data

External Undesirable data is all content type considered illegal or of classified nature and intended to be kept away from LIDL systems. Although external of its nature, control of this information asset is as important as of any internal one. The difference is clear – while we want to keep 4 previous data types within the boundaries of our systems, this type of asset is only welcome on the other side of the virtual border.

Every information asset is mapped with its respective process owner. In the next step, the security requirements of the CIA (Confidentiality, Integrity, Availability) triangle are defined for each asset. In case there are any specific security requirements they are indicated at this step as well. Using the previous example of client data, a specific requirement is the (EU) 2016/679 - (EU) 2016/680 private data regulations. The requirements are then described in terms of necessary availability time, key users, regulatory compliance etc.

Last important action in this phase is the mapping of five assets with the most important security requirement type (CIA) which was defined as follows, according to group's priorities and culture:

Confidentiality: a.) Client and Employee Data; e.) External Undesirable Data

Integrity: b.) Payment Data; c.) Shop&Go Solution related data

Availability: d.) Item Related Data

These priorities are used in the last step of assessment – recommendations. Given all other relevant factors are the same, CIA criteria will be used to prioritize one recommendation over the other. The tables illustrating this step are located in the Attachment section: "Attachment III – Critical Information Asset Profile".

III. Step 3 - Identify Information Asset Containers

Containers describe the places where information assets are stored, transported, and processed. Information assets reside not only in containers within an organization's boundaries but they also often reside in containers that are not under the direct control of the organization. Any risks to the containers in which the information asset lives are inherited by the information asset. (Carali et al, 2007)

In the scope of current assessment, only the containers added or influenced by new solution are analyzed. In other words, all containers existent before SHOP&GO implementation were considered a baseline (e.g. a POS terminal was installed long before the current project, therefore its risk exposure is out of scope; however, identified vulnerabilities and threats added by SHOP&GO deployment and relevant to POS device will include this container in assessment process).

According to solution diagram (can be found in Attachments section: Attachment I – SHOP&GO Network Diagram), the following containers were identified:

- 3rd party Rack - Composed of Router, Switch and Access Points provided by external partner to enable Guest Wireless Network.
- Stiftung's Proxy – Proxy server located in international HQ which allows access to GK Cloud platform
- External VPN connection – connection to Proxy Server in HQ (Germany) through public network, via VPN (managed by PT S.A.).
- Store Switch & Router – Switching and routing devices used for connections within store and WAN. A minimum of two devices is necessary to permit physical segregation of PCI compliant VPN connection.
- Fortinet FW – A firewall device which permits the creation of DMZ for MPOS Server

- S&G Cloud – S&G Servers nested in Cloud
- Mobile Attendant – WinCE application / Windows Mobile OS operated device used by store manager
- MPOS Server – virtual POS server used for billing on SHOP&GO checkouts
- PinPad Terminal – Card Payment terminals provided by Ingenico / SIBS
- Shop&Go App (Android / iOS) – application created for SHOP&GO solution and installed by clients on their devices
- Store BO (Backoffice) Server – Server connected to the HQ VPN and store POS devices. Key element in daily communications and POS operational management.
- Store POS device – device used by store employee for checkout purposes.
- Scale Device – scales introduced for self-checkout purposes and connected to GK Cloud (backoffice management software)
- Paytower Device – device used to enable client checking out, even in absence of store employee.

Additionally, some external containers and people involved are identified at this step as well. Detailed definition is located in the Attachments section: "Attachment IV – Information Containers".

Container´s main role in assessment process is split in two parts. As first one, clear definition of containers helps significantly during the steps of Area of Concern identification (p.5.4). Secondly, this definition is crucial in recommendations part, where particular measures are applied to one or more identified containers.

IV. Step 4 - Identify Areas of Concern

Areas of concern is a definition of possible conditions or situations that can threaten an organization's information asset. These real-world scenarios may represent threats and their corresponding undesirable outcomes. Areas of concern may characterize a threat that is unique to an organization and its operating conditions. The purpose of this step is not to capture a complete list of all possible threat scenarios for an information asset; instead, the idea is to quickly capture those situations or conditions that come immediately to the minds of the analysis team. (Carali et al, 2007)

During the assessment, a total of 43 areas of concern was identified for five information asset profiles. Nearly a half of which (20) are equally spread between Client and PCI DSS compliant data assets. These are the main areas of concern for the organization in the light of upcoming EU regulations in May of 2018. Definition of these areas was done in regard to information containers and, as stated above, real world cases. Certain events in this list are proven to be plausible by previous penetration tests, others are inspired by common vulnerability databases or latest security breaches within the industry. It is important to notice, that the tool I found the most useful at this step is a common sense of the assessor – it is up to him to keep in mind the context of the information asset, its value, possible motives of actors. Historical data and involvement in organizational culture are helpful as well.

High number of areas of concern is explained by the decision of making the first iteration of the assessment as wide as possible. In the next iterations, upon lessons learned and business needs, a more detailed view can be achieved, by adding more threat scenarios (described in next step). Each area of concern is justified by at least one threat scenario. Detailed information about every area of concern and linked threat scenario can be found in Attachments section: "Attachment V-x – Information Asset Risk Worksheet: xxx", where "x" stands for one of 5 information asset profiles.

V. Step 5 - Identify Threat Scenarios

In Step 5, the areas of concern captured in the previous step are expanded into threat scenarios that further detail the properties of a threat. (Carali et al, 2007)

For a better understanding of how Area of Concern is interconnected with Threat Scenario in Octave method the following example can be used:

Information Asset "Client & Employee Data" is subject to one of the areas of concern - "A1R1 - Client data is stolen by Man-in-the-middle (MitM) attack type on customer Wi-Fi network. A threat scenario is in general terms, a detailed definition of "How and why is this possible". In this case, an attacker will most probably position himself in between client-store access point communication by using a Rogue AP technique.

This is a particular Threat Scenario identified. One area of concern can and most likely has more than one threat scenario. It is up to an assessor to decide until what detail level he wants to go; how granular the risk assessment should be. In case of this project, the main focus was on the identification of as many areas of concern, as possible with at least one threat scenario to justify the feasibility of concern.

For continuous improvement of general threat picture, additional iterations of risk assessment are necessary. In this particular case, I find that second iteration in combination with external audit / pen-test will be beneficial to get a more detailed picture of possible threats or confirm the plausibility of identified ones. Unfortunately, it was not possible to elaborate these steps at the moment of writing due to time and resources limitation.

VI. Step 6 - Identify Risks

In Step 5 threats are identified, and in Step 6 the consequences to an organization if a threat is realized are captured, completing the risk picture. A threat can have multiple potential impacts on an organization. The activities involved in this step ensure that the various consequences of risk are captured. (Carali et al, 2007)

After completing this step, it was possible to define a Risk Score (a quantitative representation of impact in Octave Allegro) for every one of 43 identified threat scenarios. These risk scores are based on most probable threat scenario, as described in previous chapter. As an assessor, I cannot guarantee inexistence of other threats in particular area of concern. As instead, I am focusing on the most probable scenario for every area to establish a comparable baseline of risk exposure between them (areas of concern). This approach will create a heat map of major risk areas within the solution.

Allegro method distributes likelihood of an event in three categories – Low, Medium and High. The risk of particular threat scenario is identified by “gut feeling” of the assessor, what can be seen as a sum product of historical data available, common sense, trends in the industry and IS area (like major growing wave of ransomware attacks), latest vulnerabilities or technical difficulty of the attack. Finally yet importantly is a motivation – the value (monetary or not) an attack will generate for the attacker. Not all these factors are taken in consideration (at least not in the direct way) by the Allegro method, therefore I find this step extremely dependent on the assessor experience and objective view. Given that the results of it are one of the major ingredients in final risk matrix, it should be performed with all necessary diligence. From 43 threat scenarios, 15 (or 34,88%) were attributed “High” probability of occurrence in course of assessment. Certain scenarios were proven plausible by successful simulations in course of internal audits and penetration tests.

VII. Step 7 - Analyze Risks

In Step 7 of this assessment, a simple quantitative measure of the extent to which the organization is impacted by a threat is computed. This relative risk score is derived by considering the extent to which the consequence of a risk impacts the organization against the relative importance of the various impact areas, and possibly the probability. (Carali et al, 2007)

As in the previous step, it is up to the assessor to identify the severity of impact in every area identified in the first step of the assessment. However, upon completion of this project, I find it better bounded and audit-ready compared to probability definition. First, because the framework defines in a first step the monetary boundaries of an impact being Low, Medium or High in different areas – Financial, Reputational etc. This serves as a reminder for an assessor and helps to be objective in different assessment areas. Secondly, every impact decision has to be justified in short text. Such simple mechanism permits easy validation by another person involved in process, as it justifies the decision; and indirectly makes an assessor question his decisions along the process and evaluate the impact again.

Both probabilities and risks scores can be found in the same section of Attachments: “Attachment V-x – Information Asset Risk Worksheet: xxx”, where “x” stands for one of 5 information asset profiles.

Table IV

Relative Risk Matrix			
	Risk Score		
Probability	30-45	16-29	0-15
High	Mitigate	Mitigate/Defer	Mitigate/Defer
Medium	Mitigate/Defer	Mitigate/Defer	Defer/Accept
Low	Defer/Accept	Defer/Accept	Accept

4 – Relative Risk Matrix

After the impact definition is performed, score values are obtained for every one of 43 threat scenarios. These values may range from 0 to 45 in Allegro Relative Risk Matrix. This particular assessment has resulted in values from 20 (minimum) to 36 (maximum). An average Risk Score of 43 Threat Scenarios is 27. Depending on the probability/risk score combination an action approach is suggested – either Mitigate, Defer or Accept the risk.

VIII. Step 8 - Select Mitigation Approach

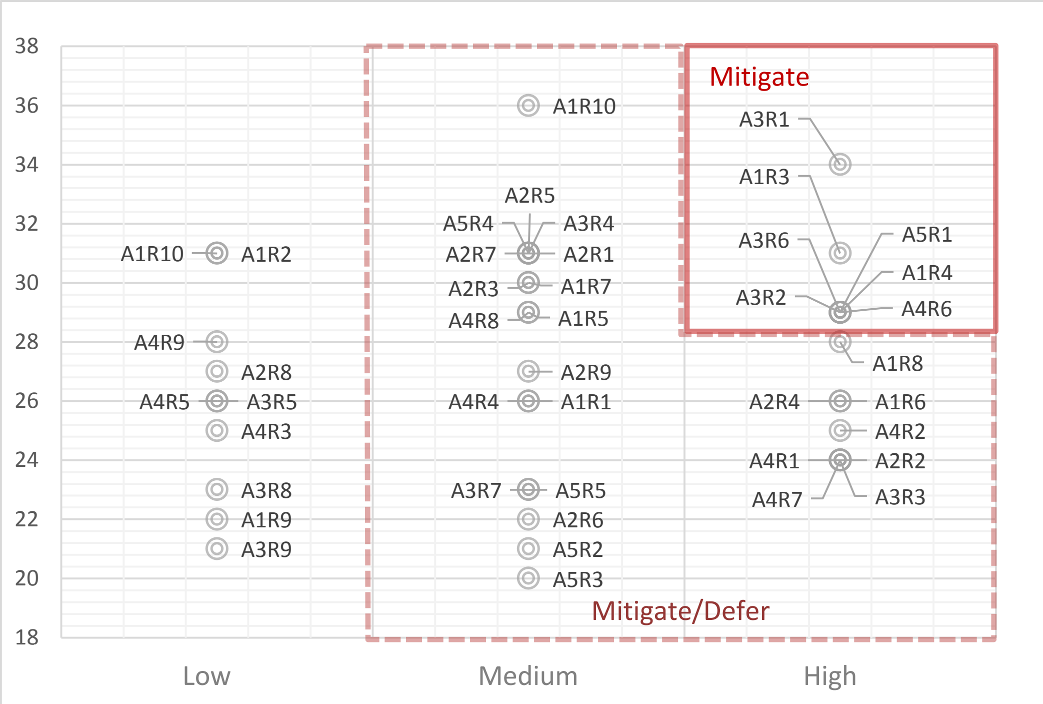
In Step 8, the final step of the OCTAVE Allegro process, organizations determine which of the risks they have identified require mitigation and develop a mitigation strategy for those risks. This is accomplished by first prioritizing risks based on their relative risk score. Once risks have been prioritized, mitigation strategies are developed that consider the value of the asset and its security requirements, the containers in which it lives, and the organization's unique operating environment. (Carali et al, 2007)

In case of mitigation recommendation, the corrective measure is applied to the impact, rather than to a probability of occurrence. All identified high-risk scenarios are matched in this step with a corrective (mitigation) measure, what doesn't mean that a risk evasion approach cannot be taken later on. For example, in case of too high mitigation costs certain system features or components may be re-considered or completely dropped. Same applies to risk acceptance strategy. Current evaluation is limited to identifying highest impact vs probability combination and provisioning of contra-measures (with estimated effort of implementation).

All risk scenarios identified in the previous steps were collected on a single table. It can be found in the Attachment section: "Attachment VI – Threat Scenarios and Mitigation". The table illustrates an area of concern, with its risk score (impact); if the impact of this scenario is challenging the most important security requirement for this information asset (CIA Priority); estimated probability; suggested action and mitigation measures, if applicable.

For visualization purpose, a risk matrix is constructed with "Mitigate" and "Mitigate/Defer" quadrants highlighted by different color areas. It is illustrated in Figure I – Risk Heat Map:

Figure 1



5- Risk Heat Map

There are 7 cases subject to mitigation recommendations, these are, threat scenarios with highest probability and risk score combination. All cases located in “Mitigate / Defer” quadrants are subject to further analysis by the assessor – whether these should be included or not in the mitigation plans. As stated in chapter 5.2 – Most Important Security Requirement (CIA) of every asset profile is used to prioritize some of the threat scenarios over the others. So, for example, two threat scenarios with equal risk score and probability in PCI DSS compliant data asset were treated differently, depending on their Threat Outcome. For this asset profile Integrity was defined as the most important requirement, therefore threat scenario resulting in Destruction or Modification will prevail over the others.

In this way, in addition to 7 Mitigation cases selected, cases from Mitigate / Defer pool were picked as well. Table V illustrates the final list of Threat Scenarios considered to be mission critical and subject to mitigation strategy. They are sorted from most critical to less critical (based on risk score and probability) – from top to bottom.

Table V

Threat Scenario	Mitigation Measure			
A1R3 - Client Data stolen by breaching store LAN	MS11	MS10	MS13	MS14
A3R1 - Insecure Protocols in MBWay Implementation	MS01	MS02		
A1R4 - Client Data stolen by DB Crack	MS07	MS09	MS08	
A3R2 - Insecure Protocols in MBWay Implementation	MS01	MS02		
A5R1 - Unintended Guest Network Usage	MS17			
A5R4 - Illegal / Restricted information stored	MS15	MS16		
A1R8 - Client data sniffed in between APP & Server Communication	MS01	MS10	MS09	
A2R3- Payment Data Availability	MS11	MS10	MS13	MS14
A1R5 - Employee data breach by BO access	MS05			
A3R6 - Application code revealed	MS04	MS10	MS01	
A4R6 - Application functionality modified	MS04	MS10	MS01	
A1R6 - Employee and Client data leaked	MS14			
A1R1 - Client data is stolen by MitM attack type	MS12	MS10		
A4R4 - Delete data on exposed devices	MS09			
A3R7 - S&G configuration data destroyed	MS16	MS15		
A5R2 - Backup / Configuration files	MS03	MS15	MS16	

6 – Threat Scenarios recommended for prioritized mitigation

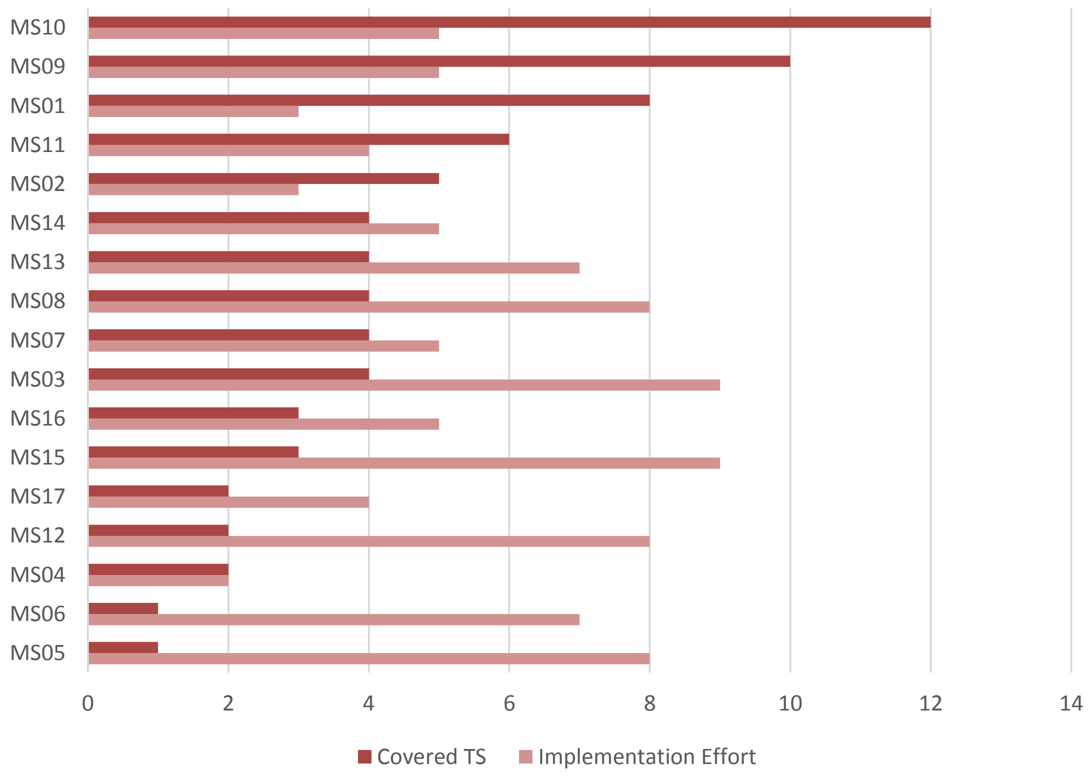
As the last part of Octave Method, the mitigation measures were defined for the complete list of Threat Scenarios, with exception of ones Octave Methodology defines as acceptable (low probability, low risk score quadrant). These measures are linked to the containers defined in Chapter 5.3. Complete Mitigation Measures Matrix can be found in Attachments section: Attachment VI – Threat Scenarios and Mitigation Measures. A more detailed discussion of measures and limitations of Octave Allegro approach at this final step will follow in the next chapter.

Recommendations for risk management

Octave approach does not provide any tool or method for prioritizing one mitigation plan over the other, except Risk Score / Probability combination. It does not take into account the cost of mitigation measures, another important aspect of risk management discipline. Application of Allegro method ends on linking specific mitigation plan to each identified Threat Scenario, as shown in the previous chapter.

To address this problem, a simple priority-based framework is used to provide an alternative solution when it comes up to risk management exercise. It consists of two steps: first, defining so called Implementation Effort, a value on a scale from 0 to 10 representing resource usage to implement a measure; secondly, the biggest part of measures does not contribute to one and only Threat Scenario, so the number of scenarios affected by the measure is also accounted. Certainly, such effort estimation is based on a pure experience of an assessor and is one of the points discussed in the Limitations chapter – the estimation process may be improved in future. Attributed effort value and a number of covered threat scenarios for every measure can be found in Attachments section: Attachment VII – Measures and Containers. The main idea behind this approach is an attempt to guarantee as secure state as possible, while dealing with limited resources (budget restrictions). It doesn´t mean, however, that other measures are irrelevant or less important, as the secure state of any system is equal to its weakest point. The objective is to provide a top-pick of measures by their impact, which can be used as an indicator when decisions have to be taken on what system, policy or control to focus. A graphical representation of this distribution is illustrated below.

Figure 2



7 – Mitigation measure by Implementation Effort / TS Coverage

By visualizing the impact of each measure on the identified threat scenarios, it becomes evident that some measures are transversal to the big part of scenarios. If these, at the same time, do not require significant implementation effort, they should be considered by management as a priority for mitigation measures.

Such presentation of findings gives an easier way to transmit the message to stakeholders, even if the area of their expertise do not include IS. It is flexible and ready for additional measure, containers and threat scenarios input. So the findings of further iterations of Octave Allegro method will be included.

This iteration of risk assessment has identified threat scenarios which can be covered by 17 major measures. The top 5 measures by TS coverage are detailed below:

<u>*MS10*</u> *– "Configure and use encrypted protocols whenever possible. If encryption protocols are not available for some applications, evaluate the possibility of VPN usage"*

It is explained by historical limitations and negligence. Many rudimentary systems within a store are running insecure versions of communication protocols. A number of audits have illustrated this fact. Scan, detect and update to secure versions when possible. Accept the risk when usage of the unsecured protocol is due to a system limitation. Document exceptions.

<u>*MS09*</u> *– "Change all default passwords. Use password management software. Enforce the usage of strong passwords across all company"*

A number of devices operated with default login/password combination. Databases using SYS/ADM accounts with default passwords. Given the pilot stage of the project with its constant changes, configuration and new deployments – it is recommended to pay special attention to password management. Create procedures and cover this topic in awareness programs for involved employees.

<u>*MS01*</u> *– "Use TLS, all pages must be served over HTTPS, The HTTP Strict Transport Security Header must be used, Cookies must be marked as Secure"*

This measure is applied on the SHOP&GO app, which is using HTTP with clear text XML files to communicate with the server, among other severe security flaws. This permits all kinds of data manipulation and eavesdropping. This container works with a number of sensitive data types – personal information, payment data. Run pen-test with independent partners to proof communication security.

MS11 – *“Design and create access policies based on business needs and enforce it using firewalls or native filtering capabilities of network devices”*

A revision of access policies is recommended for the SHOP&GO-ready stores before the rollout. Periodic audits are recommended as well. Usage of protocol and network mapping tools is advised for complete assessment.

MS02 – *“Use OWASP Top10 check / Guarantee AppSecurity through PenTest”.*

Another measure to address the problems of systems exposed to clients. Before it comes to a full-scale rollout a common vulnerabilities pen-testing should be performed on every exposed system (Black Box method). Detected vulnerabilities should be fixed.

Other measures identified in course of this assessment are listed below:

- MS03 - Use SIEM solution to detect intrusion / Use honeypots
- MS04 - Application’s code should be obfuscated, for example, with the ProGuard tool.
- MS05 - Store all GDPR compliant data encrypted
- MS06 - Reinforce store infrastructure (add switching / routing devices)
- MS07 - Implement Database Hardening; When possible, disable default SYS-like accounts;
- MS08 - Inventory of applications, versions & owners. Implement or adjust a regular mechanism for installation of security updates.
- MS12 - Implement a Wireless Intrusion Prevention System
- MS13 - Implement Physical Security Monitoring
- MS14 - Use centralized DB console for access control (e.g. Cloud Control)
- MS15 - Use Log-indexing system for version / patching checks
- MS16 - Define and implement internal awareness programs by functional area

- Implement traffic filter / DNS blacklist

Conclusions

The main contribution of this project is an overview it provides on a secure state of Shop&Go solution. It is different in its nature from a traditional pen-testing approach used by organizations, whose main focus on is the identification of vulnerabilities. This study was based and performed around information assets and their value for the organization at one side, and the known and expected vulnerabilities with respective fixes (and estimated effort to implement the fix) at the other. By uniting all possible concerns and estimations in one report, a decision making task becomes easier when it comes up to measure implementation with limited resources.

To address all these problems, an initial study of existing risk assessment frameworks was performed. I have picked Octave Allegro method as the one being the best fit-for-purpose solution for this project. Along the assessment process, I have taken some conclusions about the method itself, its strong points and limitations.

The main findings of risks are related to publicly exposed assets and their services. As one of the first experiences of providing to the end customer an access to internal infrastructure, a number of checks need to be run to secure store readiness. Therefore, a formal procedure is suggested for new implementations, as well as periodic checks of the existing ones (by automated audit tools, for example). Main topics for improvements are secure communication, improvements in physical security policy, password and patch management revision and awareness of the store personnel / IT personnel.

The list of suggested measures can be used as a reference by the organizations within the industry, which are planning any similar type of deployment. As this was the first risk assessment iteration performed, its results are sufficiently generic and applicable to other sites and projects.

Discussion and limitations

In course of this project, only the initial iteration of Octave Allegro method was performed. I find it beneficial to run the second iteration with the involvement of key users from main areas of concern – e.g. Networking, Database Administration. This step was not performed due to limitations of time and resources (such key users are responsible for running business-as-usual and IS normally stays in the last place in their agenda).

Given that SHOP&GO project is run as a proof of concept, resources available for its fixes are limited and hardly accessible. For this reason, many measures suggested in this study may only be applicable in case of project approval and full-scale rollout.

Octave Allegro framework has proven itself efficient and complete with exception of some particular points. I found it extremely dependent on assessor’s experience and common sense when it came up to probability definition. Secondly, I think it may be improved in the very last stage of measure recommendations to include some sort of ranking mechanism for the suggested measures.

To permit such ranking, a simple method of measure distribution was introduced, as described in chapter 6. Its main limitation is the attributed value of estimated effort to implement one measure. This calculation in future assessments may be based on a real monetary value provided by implementing partner, for example. It is important to notice that improvement of this ranking mechanism may change the priority distribution of different measures, but not the validity of measure itself.

Bibliography

Alberts, C. and Dorofee, A. (2009). Managing information security risks. Boston [u.a.]: Addison-Wesley.

APB Consultant. (2017). Information Security Risk Management. [online] Available at: http://isoconsultantpune.com/information-security-risk-management/ [Accessed 6 Oct. 2017].

Aven, T. (2012). The risk concept—historical and recent development trends. Reliability Engineering & System Safety, 99, pp.33-44.

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research, 253, pp.1-13.

Caralli, R., Stevens, J.F., Young, L.R., Wilson, W.R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Carnegie Mellon University - SEI. Available at: https://ru.scribd.com/document/38707815/OCTAVE-Allegro-Risk-Mitigation [Accessed 6 Oct. 2017].

CERT (2017). CERT PODCAST SERIES: SECURITY FOR BUSINESS LEADERS. Comparing IT Risk Assessment and Analysis Methods Available at: http://resources.sei.cmu.edu/asset_files/Podcast/2014_016_102_85656.html [Accessed 6 Oct. 2017].

Computer Security Resources Center NIST. (2017). CSRC - NIST Computer Security Publications. [online] Available at: https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01 [Accessed 6 Oct. 2017].

Elky, S. (2006). An Introduction to Information Risk Assessment. SANS Institute. [online] sans.org. Available at: https://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204 [Accessed 6 Oct 2017]

Enisa.europa.eu. (2017). Magerit — ENISA. [online] Available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_magerit.html [Accessed 6 Oct. 2017].

FAIR Institute. (2017). The Importance and Effectiveness of Quantifying Cyber Risk. [online] Fairinstitute.org. Available at: http://www.fairinstitute.org/fair-risk-management [Accessed 6 Oct. 2017].

Guide for conducting risk assessments. (2012). Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology.

ISACA. (2017). COBIT 5: Enabling Processes. [online] Available at: https://www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Processes-product-page.aspx [Accessed 6 Oct. 2017].

ISO 27k Forum (2010). Iso27k Faq | Information Security | International Organization for Standardization. [online] Available at: https://ru.scribd.com/document/44303469/Iso27k-Faq [Accessed 6 Oct. 2017].

International Standard Organisation. (2017). ISO 31000:2009 Risk management -- Principles and guidelines. [online] Available at: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en [Accessed 6 Oct. 2017].

Macedo, F., Silva, M. (2009) Comparative Study of Information Security Risk Assessment Models. Instituto Superior Técnico – Universidade Técnica de Lisboa.

Masky, M., Young, S. and Choe, T. (2015). A Novel Risk Identification Framework for Cloud Computing Security. 2015 2nd International Conference on Information Science and Security (ICISS).

Mayo, J.W. (2009). Risk Management for IT Projects. ISACA Group. Available at: http://www.isaca.org/Groups/Professional-English/risk-management/GroupDocuments/Effective_Project_Risk_Management.pdf [Accessed 6 Oct. 2017].

National Cyber Security Center (2017).Summary of risk methods and frameworks - NCSC Site. [online] Available at: https://www.ncsc.gov.uk/guidance/summary-risk-methods-and-frameworks [Accessed 6 Oct. 2017].

National Institute of Standards and Technology (2012) Special Publication (SP) 800-30 – NIST Site. [online] Available at: https://www.nist.gov/publications/risk-management-guide-information-technology-systems [Accessed 6 Oct. 2017].

Reddy, L.S.S, Kiran, K.V.D, Haritha, N.L. (2013). A Comparative Analysis on Risk Assessment Information Security Models. International Journal of Computer Applications (0975 – 8887) Volume 82 – No.9

The Open Group (2009). Technical Standard. Risk Taxonomy. The Open Group (2009)

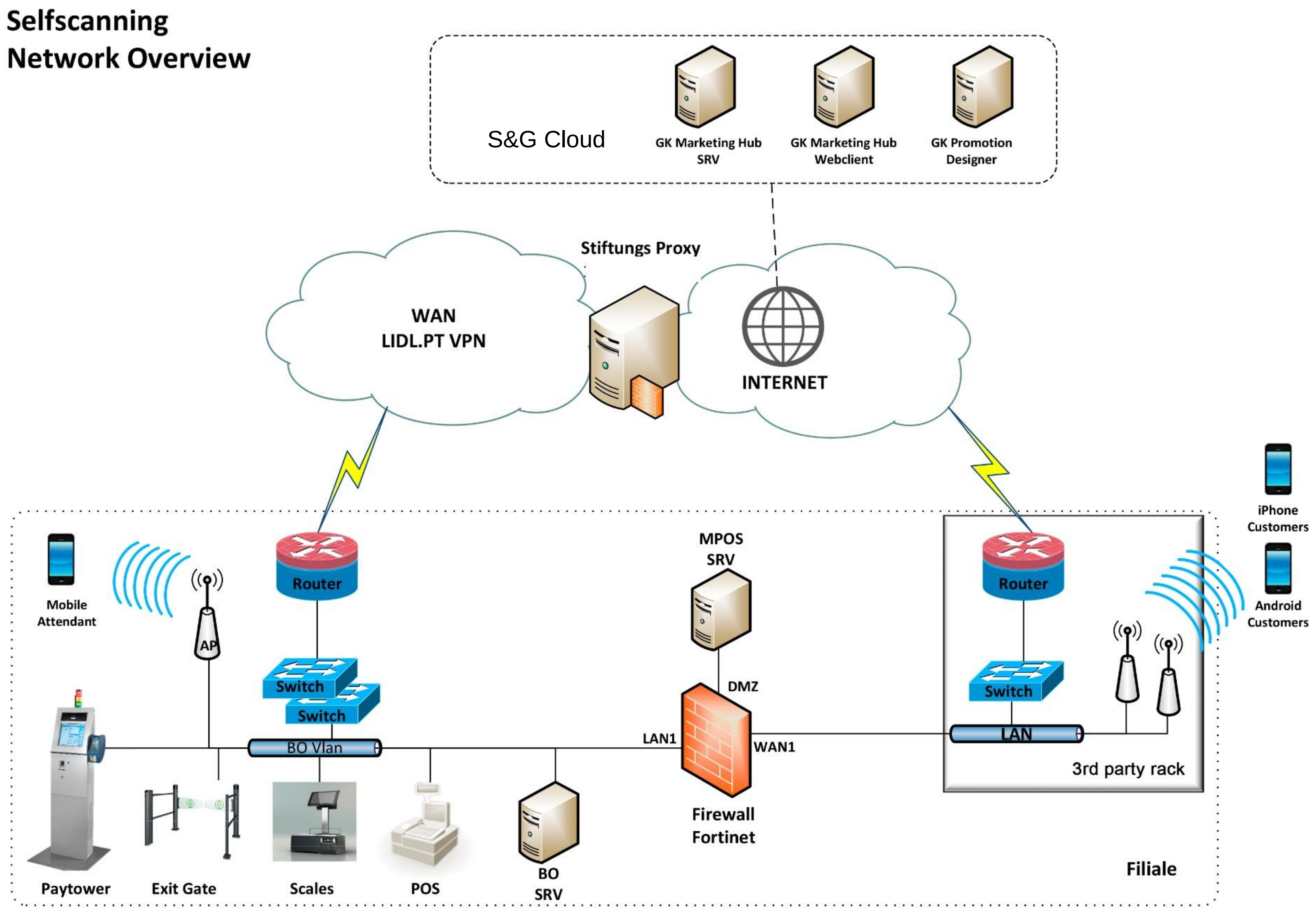
Tomhave, B., Heidt, E. and Robins, A. (2014). Comparing Methodologies for IT Risk Assessment and Analysis. [online] Gartner.com. Available at: https://www.gartner.com/doc/2659816/comparing-methodologies-it-risk-assessment [Accessed 6 Oct. 2017].

Visintine, V. (2003). An Introduction to Information Risk Assessment. GSEC Practical-SANS Institute

Glossary

Access Point (AP)	a networking hardware device that allows a Wi-Fi device to connect to a wired network.
DNS Blacklist	a "blacklist" of locations on the Internet reputed to be harmful or undesireble within company network
Firewall	a technological barrier designed to prevent unauthorized or unwanted communications between computer networks or hosts
GDPR	a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA).
Hardening (IT)	the process of securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions
Honeypot (IS)	a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.
Information Security (IS)	sometimes shortened to InfoSec, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.
Password managemnt	an information security policy aimed to manage and control the lifecycle of passwords within organization
Patch management	a part of Vulnerability management - the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities by application of most recent system updates
PCI DSS	Payment Card Industry Data Security Standard is an information security standard for organizations that handle branded credit cards from the major card schemes.
Pen Test	A penetration test, colloquially known as a pen test, is an authorized simulated attack on a computer system, performed to evaluate the security of the system.
POS	The point of sale (POS) is the time and place where a retail transaction is completed.
Proxy Server	a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.
Risk Assessment (RA)	the determination of quantitative or qualitative estimate of risk related to a well-defined situation and a recognized threat
Risk Score	a quantified impact rating of risk scenario suggested by Octave Allegro method
Router	a networking device that forwards data packets between computer networks.
Shop&Go	internal name of a self-scanning and self-checkout product developed by Lidl Gmbh.
SIEM	security information and event management provide real-time analysis of security alerts generated by applications and network hardware
Switch	computer networking device that connects devices together on a computer network by using packet switchingto receive, process, and forward data to the destination device
VPN	a private network extended across a public network, to enable users to send and receive data as if their computing devices were directly connected to the private network
WAN	wide area network is a telecommunications network or computer network that extends over a large geographical distance/place.
WIPS	a wireless intrusion prevention system is a network device that monitors the radio spectrum for the presence of unauthorized access points and take countermeasures

Attachments



Attachment I – SHOP&GO Network Dia-

Allegro Worksheet 1	**Risk Measurement Criteria – Reputation and Customer Confidence**		
Impact Area	**Low**	**Moderate**	**High**
Reputation (Company)	Reputation of LIDL is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
Reputation (Shop&Go)	Reputation of Shop&Go is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
Customer Loss (Company)	Less than 3% reduction in customers due to loss of confidence	3 to 10 % reduction in customers due to loss of confidence	More than 10 % reduction in customers due to loss of confidence
Users Loss (Shop&Go)	Less than 2% reduction in customers due to loss of confidence	2 to 15 % reduction in customers due to loss of confidence	15 to 30 % reduction in customers due to loss of confidence

Allegro Worksheet 2	**Risk Measurement Criteria – Financial**		
Impact Area	**Low**	**Moderate**	**High**
Operating Costs	Increase of less than 5% in yearly operating costs of Shop&Go Solution	Yearly operating costs increase by 5 to 10 %.	Yearly operating costs increase by more than 10%.
Revenue Loss	Less than 5% yearly revenue of Shop&Go Solution loss	5 to 10% yearly revenue loss	Greater than 10% yearly revenue loss
One-Time Financial Loss	One-time financial cost of less than €10,000	One-time financial cost of €10,000 to €25,000	One-time financial cost greater than €25,000

Allegro Worksheet 3	**Risk Measurement Criteria – Productivity**		
Impact Area	**Low**	**Moderate**	**High**
Staff Hours - affected locations	Staff work hours are increased by less than 5 % for 1 to 14 day(s).	Staff work hours are increased between 5 % and 10 % for 1 to14 day(s).	Staff work hours are increased by greater than 10% for more than 14 days.
Staff Hours - IT	Staff work hours are increased by less than 5 % for 1 to 7 day(s).	Staff work hours are increased between 5 % and 15 % for 1 to 7 day(s).	Staff work hours are increased by greater than 15% for more than 7 days.
Staff Hours - External Partners	Extra work hours required of less than 5 % for 1 to 7 day(s).	Extra work hours required of 5 to 10 % for 1 to 7 day(s).	Extra work hours required of >10% for more than 7 day.

Allegro Worksheet 4	**Risk Measurement Criteria – Safety and Health**		
Impact Area	**Low**	**Moderate**	**High**
Life	No loss or significant threat to customers' or staff members' lives	Customers' or staff members' lives are threatened, but they will recover after receiving medical treatment.	Loss of customers' or staff members' lives
Health	Minimal, immediately treatable degradation in customers' or staff members' health with recovery within four days	Temporary or recoverable impairment of customers' or staff members' health	Permanent impairment of significant aspects of customers' or staff members' health
Safety	Safety questioned	Safety affected	Safety violated

Allegro Worksheet 5	**Risk Measurement Criteria – Fines and Legal Penalties**		
Impact Area	**Low**	**Moderate**	**High**
Fines	Fines less than €5,000 are levied.	Fines between €5,000 and €50,000 are levied.	Fines greater than €50,000 are levied.
Lawsuits	Non-frivolous lawsuit or lawsuits less than € 50,000 are filed against the organization, or frivolous lawsuit(s) are filed against the organization.	Non-frivolous lawsuit or lawsuits between €50,000 and €500,000 are filed against the organization.	Non-frivolous lawsuit or lawsuits greater than €500,000 are filed against the organization.
Investigations	No queries from government or other investigative organizations	Government or other investigative organization requests information or records (low profile).	Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices.

Attachment II – Risk Measurement Criteria

Allegro Worksheet 8	Critical Information Asset Profile					
(1) Critical Asset	*What is the critical information asset?*	Client and Employee Data - Private (Personal) Data	Payment Data - PCI DSS compliant	Shop&Go Solution related data.	Item Related Data (Purchase - Sale)	External Undesirable Data
(2) Rationale for Selection	*Why is this information asset important to the organization?*	Client Data is valuable not only for correct billing purposes, but for marketing and other reporting activities. Disclosure of such data had long going consequences for LIDL group in the past, therefore, this information asset is treated with as much attention as possible. Employee data is subject to the same regulations, being private in its type.	Data Retrieved by cashless payment processes. Used for accounting and controlling purposes. Any disclosure or compromise of this date may put in question the PCI DSS certification of LIDL Portugal and harm its reputation.	Data type related to Shop&Go solution itself. Being innovative in its nature and still in development, disclosure of such data may lead to further vulnerabilities exposure.	Data related to particular article sold by LIDL. Everything from its manufacturer or supplier, price programming, campaigns, stock etc. Disclosure of this data may lead to competitive loss.	External Undesirable data is all content type considered illegal or of classified nature and intended to be kept away from LIDL systems. Although external of its nature, control of this information asset is as important as of any internal one.
(3) Description	*What is the agreed-upon description of this information asset?*	This Data information type consists of all the registries linkable to individual client or employee of organization, such as VAT number, contact information, salary etc. Private Data is everything falling under Personal Data category in terms of upcoming Data Protection regulations (EU2018)	Data falling under PCI DSS classification. Data regarding realized transactions is supposed to be stored for 5 years by legal norms. It is subject to internal and external (government) audits.	Data related to the project. Everything from IP addresses and ports, protocol types, access credentials and passwords used by solution to high level strategy plans and statistical reports.	Critical data from individual items sold in stores, which has value to competition. It is used by many modules of ERP system. It is required for correct functioning of stores in the first place and all support departments like Purchase or Retail.	All data not intended to be stored on LIDLs systems, as for example illegal content downloaded by employees or users of open networks provided by LIDL.
(4) Owner(s)	*Who owns this information asset?*	Data Protection Officer (DPO), HR HQ	ISO	ISO	Sales Dpt. (VK), Purchase dpt. (EK)	unidentified
(5) Security Requirements *What are the security requirements for this information asset?*						
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Store Personnel with access rights to Clients data. Store manager with limited access rights to employee data.	Store employee on the moment of transaction, "read" rights of particular transaction.	IT personell	Store Personell and Manager	Nobody is intended to have access to this information.
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Store employee, only regarding variable client data: Name, VAT number, address.	Information should not be modified.	IT personell	Only Sales Manager can modify certain fields of this information.	Any LIDL employee may modify this information.
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	Store personnel for billing purposes, Store manager for planning purposes (HR data).	Information should be available until	IT Personell	Store Personell	Nobody is intended to have access to this information.
	This asset must be available for:	20h, 7 days a week, 52 weeks a year. Client/HR Data may not be available in a short window of 4 hours a day for system's maintenance purposes.	20h, 7d/w, 52w/y.	24h/d, 5d/w,52w/d	20h, 7d/w, 52w/y.	0h, 0d/w, 0w/y
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	It must respect EU Data Protection and Private Data Regulations (EU) 2016/679 - (EU) 2016/680	PCI DSS regulation	General Information Security Practices	-	Civil and Criminal Law regulation
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		**Confidentiality**	**Integrity**	**Integrity**	**Availability**	**Confidentiality**

Attachment III – Critical Information Asset Profile

Technical Containers

	Client and Employee Data - Private (Personal) Data		Payment Data - PCI DSS compliant		Shop&Go Solution related data.		Item Related Data (Purchase - Sale)		External Undesirable Data	
	Allegro Worksheet 9a	**Information Asset Risk Environment Map**	**Allegro Worksheet 9a**	**Information Asset Risk Environment Map**	**Allegro Worksheet 9a**	**Information Asset Risk Environment Map**	**Allegro Worksheet 9a**	**Information Asset Risk Environment Map**	**Allegro Worksheet 9a**	**Information Asset Risk Environment Map**
Internal	Container Description	Owner(s)	Container Description	Owner(s)	Container Description	Owner(s)	Container Description	Owner(s)	Container Description	Owner(s)
	Store Switch & Router	IT Department HQ	Store Switch & Router	IT Department HQ	Store Switch & Router	IT Department HQ	Store Switch & Router	IT Department HQ	Fortinet FW	IT Department HQ
	Fortinet FW	IT Department HQ	Fortinet FW	IT Department HQ	Mobile Attendant	IT Department INT	POS device	IT Department HQ	MPOS Server	IT Department HQ
	Mobile Attendant	IT Department INT	Paytower Device	IT Department HQ	MPOS Server	IT Department HQ	MPOS Server	IT Department HQ	PinPad Terminal	IT Department HQ
	MPOS Server	IT Department HQ	MPOS Server	IT Department HQ	Shop&Go App (Android / iOS)	IT Department INT	Shop&Go App (Android / iOS)	IT Department INT	Store BO (Backoffice) Server	IT Department HQ
	Shop&Go App (Android / iOS)	IT Department INT	Shop&Go App (Android / iOS)	IT Department INT	Store BO (Backoffice) Server	IT Department HQ	Store BO (Backoffice) Server	IT Department HQ	POS device	IT Department HQ
	Store BO (Backoffice) Server	IT Department HQ	PinPad Terminal	IT Department HQ	Scale Device	IT Department INT	Scale Device	IT Department INT	Store Switch & Router	IT Department HQ
	Scale Device	IT Department HQ			Paytower Device	IT Department HQ			Scale Device	IT Department INT
External	*Container Description*	*Owner(s)*	*Container Description*	*Owner(s)*	*Container Description*	*Owner(s)*	*Container Description*	*Owner(s)*	*Container Description*	*Owner(s)*
	3rd party Rack	Frederix Gmbh	External VPN connection	UNICRE S.A.	3rd party Rack	PT S.A., third party provider	Stiftungs Proxy	PT S.A., third party provider	3rd party Rack	PT S.A., third party provider
	Stiftungs Proxy	Lidl INT			Stiftungs Proxy	Lidl INT	S&G Cloud	GK Software	S&G Cloud	GK Software
	S&G Cloud	GK Software			S&G Cloud	GK Software			External VPN connection	PT S.A.

Physical Containers

	Client and Employee Data - Private (Personal) Data		Payment Data - PCI DSS compliant		Shop&Go Solution related data.		Item Related Data (Purchase - Sale)		External Undesirable Data	
	Allegro Worksheet 9b	**Information Asset Risk Environment Map**	**Allegro Worksheet 9b**	**Information Asset Risk Environment Map**	**Allegro Worksheet 9b**	**Information Asset Risk Environment Map**	**Allegro Worksheet 9b**	**Information Asset Risk Environment Map**	**Allegro Worksheet 9b**	**Information Asset Risk Environment Map**
Internal	Container Description	Owner(s)	Container Description	Owner(s)	Container Description	Owner(s)	Container Description	Owner(s)	Container Description	Owner(s)
	1. Paper Prints	Store Manager	-	-	1. Internal manuals and guidelines	IT Department HQ	1. Daily price prints	Store Manager	1. Undesired information prints	Store Staff
	2. Sell Receipts	Store Manager								
External	*Container Description*	*Owner(s)*	*Container Description*	*Owner(s)*	*Container Description*	*Owner(s)*	*Container Description*	*Owner(s)*	*Container Description*	*Owner(s)*
	-	-	-	-	1. Instalation manuals	Third Party	-	-	1. Undesired information prints	Third Party Partners

People

	Client and Employee Data - Private (Personal) Data		Payment Data - PCI DSS compliant		Shop&Go Solution related data.		Item Related Data (Purchase - Sale)		External Undesirable Data	
	Allegro Worksheet 9c	**Information Asset Risk Environment Map (People)**	**Allegro Worksheet 9c**	**Information Asset Risk Environment Map (People)**	**Allegro Worksheet 9c**	**Information Asset Risk Environment Map (People)**	**Allegro Worksheet 9c**	**Information Asset Risk Environment Map (People)**	**Allegro Worksheet 9c**	**Information Asset Risk Environment Map (People)**
Internal Personnel	Name or Role / Responsibility	Department or Unit	Name or Role / Responsibility	Department or Unit	Name or Role / Responsibility	Department or Unit	Name or Role / Responsibility	Department or Unit	Name or Role / Responsibility	Department or Unit
	1. Store Employee	Store Instance	1. Store Employee	Store Instance	1. Store Manager	Store Instance	1. Store Employee	Store Instance	1. Store Employee	Store Instance
	2. Store Manager	Regional Center	2. IT Employee	HQ	2. IT Employee	HQ	2. Store Manager	Regional Center	2. Store Manager	Store Instance
	3. IT Employee	HQ			3. Project Manager	HQ	3. IT Employee	HQ	3. IT Employee	HQ
	4. Regional Manager	HQ					4. Regional Manager	Regional Center	4. Regional Manager	Regional Center
External Personnel	Name or Role / Responsibility	Department or Unit	Name or Role / Responsibility	Department or Unit	Name or Role / Responsibility	Department or Unit	Name or Role / Responsibility	Department or Unit	Name or Role / Responsibility	Department or Unit
	1. Support Agent	External Partner	1. Partner company tecnician	Third Party	1. Instalation Tecnician	Third Party			1. Instalation Tecnician	Third Party

Attachment IV – Information Containers

Allegro - Worksheet 10.1	Information Asset Risk Worksheet
Information Asset	**Client / Employee Personal Data**

A1R1

Area of Concern	*A1R1 - Client data is stolen by MitM attack type*
(1) Actor	External Attacker
(2) Means	Create a fake WiFi acess point and sniff the client data being transferred
(3) Motive	Get access to sensitive personal data
(4) Outcome	**Disclosure**
(5) Security Requirements	GDPR compliance
(6) Probability	**Medium**

(7) Consequences	Impact Area	Value	Score
In case of disclosure and becoming public fact will lead to heavy fines and loss of reputation for the whole group.	Rep. & Customer Confidence	Medium	10
No big impact is expected	Safety & Health	Low	4
In case of disclosure and becoming public fact will lead to heavy fines and loss of reputation for the whole group.	Fines & Legal Penalties	High	9
No big impact is expected	Productivity	Low	2
Reduction of turnover is possible due to reputational loss	Financial	Low	1

Relative Risk Score 26

A1R2

Area of Concern	*A1R2 - Client data stolen by LWL-M WLAN crack*
(1) Actor	External Attacker
(2) Means	Gain access to LWL-M WLAN by using common password
(3) Motive	Get access to secure store network, used for communication between devices; access files/databases stored on devices
(4) Outcome	**Disclosure**
(5) Security Requirements	GDPR compliance
(6) Probability	**Low**

(7) Consequences	Impact Area	Value	Score
In case of disclosure and becoming public fact will lead to heavy fines and loss of reputation for the whole group. Given that breach occur on internal network whole security policy may be questioned.	Rep. & Customer Confidence	High	15
No big impact is expected	Safety & Health	Low	4
In case of disclosure and becoming public fact will lead to heavy fines and loss of reputation for the whole group.	Fines & Legal Penalties	High	9
No big impact is expected	Productivity	Low	2
Reduction of turnover is possible due to reputational loss	Financial	Low	1

Relative Risk Score 31

A1R3

Area of Concern	*A1R3 - Client Data stolen by breaching store LAN*
(1) Actor	External/Internal Attacker
(2) Means	Gain access to LAN by using scale's TP connection (and spoofing its MAC address)
(3) Motive	Get access to secure store network, used for communication between devices; access files/databases stored on devices
(4) Outcome	**Disclosure**
(5) Security Requirements	GDPR compliance
(6) Probability	**High**

(7) Consequences	Impact Area	Value	Score
Large chunks of client data can be obtained after successful breach of store LAN. Data may become unavailable (low impact on one store only) or disclosed (big impact - fines and reputation loss)	Rep. & Customer Confidence	Medium	15
	Safety & Health	Low	4
	Fines & Legal Penalties	High	9
No big impact is expected	Productivity	Low	2
	Financial	Low	1

Relative Risk Score 31

A1R4

Area of Concern	*A1R4 - Client Data stolen by DB Crack*
(1) Actor	External/Internal Attacker
(2) Means	After successful breach get access to ERP DB by using common login/pwd combination
(3) Motive	Obtain data stored in internal databases
(4) Outcome	**Disclosure**
(5) Security Requirements	Lidl internal Access Control Policies
(6) Probability	**High**

(7) Consequences	Impact Area	Value	Score
In case of disclosure and becoming public fact will lead to heavy fines and loss of reputation for the whole group.	Rep. & Customer Confidence	Medium	10
No big impact is expected	Safety & Health	Low	4
In case of disclosure and becoming public fact will lead to heavy fines and loss of reputation for the whole group.	Fines & Legal Penalties	Medium	6
After successful breach an attacker will most likely drop the database to harden the audit	Productivity	High	6
	Financial	High	3

Relative Risk Score 29

A1R5

Area of Concern	*A1R5 - Employee data breach by BO access*
(1) Actor	External Attacker
(2) Means	After successful breach get access to store Back Office server due to unsecure protocols
(3) Motive	Access to employee information, administrative accounts and passwords
(4) Outcome	**Disclosure**
(5) Security Requirements	Lidl internal Access Control Policies
(6) Probability	**Medium**

(7) Consequences	Impact Area	Value	Score
Disclosure will lead to reputation loss.	Rep. & Customer Confidence	Medium	10
No big impact is expected	Safety & Health	Low	4
Disclosure most probably will originate moderate fines.	Fines & Legal Penalties	Medium	6
After successful breach an attacker will most likely drop the database to harden the audit	Productivity	High	6
	Financial	High	3

Relative Risk Score 29

A1R6

Area of Concern	*A1R6 - Employee and Client data leaked*
(1) Actor	External/Internal Attacker
(2) Means	After inrusion to network it is possible to manipulate S&G scales due to unsecure BO app
(3) Motive	Take pictures of employees or clients, espionage
(4) Outcome	**Disclosure**
(5) Security Requirements	GDPR: LIDL Internal Data Protection Policy
(6) Probability	**High**

(7) Consequences	Impact Area	Value	Score
In case of disclosure and becoming public fact will lead to heavy fines and loss of reputation for the whole group.	Rep. & Customer Confidence	High	15
No big impact is expected	Safety & Health	Low	4
	Fines & Legal Penalties	Low	3
	Productivity	Low	2
Reputation loss of this kind most probably will turn significant number of clients away from the brand.	Financial	Medium	2

Relative Risk Score 26

A1R7

Area of Concern	*A1R7 - Client Data Destroyed*
(1) Actor	External Attacker
(2) Means	Ransomware injection through S&G infrastructure
(3) Motive	Blackmail / Intentionall will to harm the organization
(4) Outcome	**Destruction**
(5) Security Requirements	Lidl Access Control & Usage Policies
(6) Probability	**Medium**

(7) Consequences	Impact Area	Value	Score
In case of disclosure and becoming public fact will lead to heavy fines and loss of reputation for the whole group.	Rep. & Customer Confidence	High	15
No big impact is expected	Safety & Health	Low	4
	Fines & Legal Penalties	Low	3
Destruction of data will turn impossible for certain type sales through S&G	Productivity	High	6
Medium impact is expected on sales drop, as S&G share of total sales is relatively low (15 to 20%).	Financial	Medium	2

Relative Risk Score 30

A1R8

Area of Concern	*A1R8 - Client data sniffed in between APP & Server Communication*
(1) Actor	External Attacker / Internal Employee
(2) Means	By usage of insecure HTTP protocol everyone with access to network can see in clear text the transactions
(3) Motive	Internal employee collecting critical information to harm organization /External espionage
(4) Outcome	**Disclosure**
(5) Security Requirements	Lidl Software Development Requirements; Secure Development Best Practices
(6) Probability	**High**

(7) Consequences	Impact Area	Value	Score
In case of disclosure and becoming public fact will lead to loss of reputation for the whole group.	Rep. & Customer Confidence	Medium	10
	Safety & Health	Low	4
	Fines & Legal Penalties	Medium	6
Access to such data will permit attacker alter it and use to his own advantage, leading to losses	Productivity	High	6
	Financial	Medium	2

Relative Risk Score 28

A1R9

Area of Concern	*A1R9 - Employee Data Modification*
(1) Actor	Internal Employee
(2) Means	Modify Database entries due to shared accounts / permissive filtering with DBs access
(3) Motive	Information modification for own benefit
(4) Outcome	**Modification**
(5) Security Requirements	Lidl internal Access Control Policies
(6) Probability	**Low**

(7) Consequences	Impact Area	Value	Score
No big impact is expected	Rep. & Customer Confidence	Low	5
Certain data modification may compromise safety & health requirements	Safety & Health	Medium	8
No big impact is expected	Fines & Legal Penalties	Low	3
Access to such data will permit attacker alter it and use to his own advantage, leading to losses	Productivity	Medium	4
	Financial	Medium	2

Relative Risk Score 22

A1R10

Area of Concern	*A1R10 - Client Information unavailable*
(1) Actor	External Attacker
(2) Means	Order or execute a DDoS attack on S&G Cloud servers to turn information unavailable.
(3) Motive	Access to employee information, administrative accounts and passwords
(4) Outcome	**Interruption**
(5) Security Requirements	LIDL Information Security Policy; S&G SLA
(6) Probability	**Low**

(7) Consequences	Impact Area	Value	Score
Significant loss of reputation is expected in case of service unavailability	Rep. & Customer Confidence	High	15
No big impact is expected	Safety & Health	Low	4
	Fines & Legal Penalties	Low	3
DDOS attack will disable S&G functionality and lead to unoperational state	Productivity	High	6
	Financial	High	3

Relative Risk Score 31

Attachment V-I – Information Asset Risk Worksheet: Client & Personal Data

Allegro - Worksheet 10.2	Information Asset Risk Worksheet
Information Asset	**PCI-DSS Compliant Data**

A2R1

Area of Concern	*A2R1 - Insecure Protocols in MBWay Implementation*
(1) Actor	Internal / Third-Party employee with access to store LAN
(2) Means	By sniffing insecure traffic between user device and Payment Terminal
(3) Motive	User payment data collection, possible future fraud
(4) Outcome	**Disclosure**
(5) Security Requirements	PCI-DSS Compliance
(6) Probability	**Medium**

(7) Consequences	(8) Severity: Impact Area	Value	Score
In case of disclosure and becoming public fact will lead to heavy fines and loss of reputation for the whole group.	Rep. & Customer Confidence	High	15
No big impact is expected	Safety & Health	Low	4
In case of disclosure and becoming public fact will lead to heavy fines and loss of reputation for the whole group.	Fines & Legal Penalties	High	9
No big impact is expected	Productivity	Low	2
	Financial	Low	1
	Relative Risk Score		**31**

A2R2

Area of Concern	*A2R2 - Payment data availability*
(1) Actor	Internal / External Employee
(2) Means	By using dedicated PCI VLAN / Switch. Using it for other connections.
(3) Motive	Unawareness / Negligence
(4) Outcome	**Interruption**
(5) Security Requirements	PCI-DSS Compliance / Internal Policy
(6) Probability	**High**

(7) Consequences	(8) Severity: Impact Area	Value	Score
No big impact is expected	Rep. & Customer Confidence	Low	5
	Safety & Health	Low	4
In case of disclosure and becoming public fact will lead to heavy fines and loss of reputation for the whole group.	Fines & Legal Penalties	High	9
Impact on store productivity due to unavailablity of certain devices	Productivity	Medium	4
Reduction of turnover is possible due to reputational loss	Financial	Medium	2
	Relative Risk Score		**24**

A2R3

Area of Concern	*A2R3- Payment Data Availability*
(1) Actor	External/Internal Attacker
(2) Means	Gain access to LAN by using scale's TP connection (and spoofing its MAC address), inject ransomware
(3) Motive	Blackmail / Intentionall will to harm the organization
(4) Outcome	**Destruction**
(5) Security Requirements	PCI-DSS Compliance / Internal Policy
(6) Probability	**Medium**

(7) Consequences	(8) Severity: Impact Area	Value	Score
Large chunks of client data can be obtained after successful breach of store LAN. By launching a locker application local data may become unavailable / destroyed.	Rep. & Customer Confidence	High	15
	Safety & Health	Low	4
	Fines & Legal Penalties	Low	3
Productivity fall in case of encrypted servers/POS devices	Productivity	High	6
Financial Loss due to lost sale oportunities	Financial	Medium	2
	Relative Risk Score		**30**

A2R4

Area of Concern	*A2R4 - Payment Data lost due to DB crack*
(1) Actor	External/Internal Attacker
(2) Means	After successful breach get access to ERP DB by using common login/pwd combination
(3) Motive	Obtain data stored in internal databases
(4) Outcome	**Disclosure**
(5) Security Requirements	PCI-DSS Compliance / Internal Policy
(6) Probability	**High**

(7) Consequences	(8) Severity: Impact Area	Value	Score
In case of disclosure and becoming public fact will lead to heavy fines and loss of reputation for the whole group.	Rep. & Customer Confidence	Medium	10
No big impact is expected	Safety & Health	Low	4
In case of disclosure and becoming public fact will lead to heavy fines and loss of reputation for the whole group.	Fines & Legal Penalties	Medium	6
After successful breach an attacker will most likely drop the database to harden the audit	Productivity	Medium	4
	Financial	Medium	2
	Relative Risk Score		**26**

A2R5

Area of Concern	*A2R5 - PinPad physical substitution*
(1) Actor	External Attacker / Third Party employee
(2) Means	Switching of PinPads in store to modified ones, which communicate card data to the attacker
(3) Motive	Steal card data
(4) Outcome	**Disclosure**
(5) Security Requirements	PCI-DSS
(6) Probability	**Medium**

(7) Consequences	(8) Severity: Impact Area	Value	Score
In case of disclosure and becoming public fact will lead to heavy fines and loss of reputation for the whole group.	Rep. & Customer Confidence	High	15
No big impact is expected	Safety & Health	Low	4
Disclosure most probably will originate moderate fines.	Fines & Legal Penalties	High	9
No big impact is expected	Productivity	Low	2
	Financial	Low	1
	Relative Risk Score		**31**

A2R6

Area of Concern	*A2R6- CDE Interruption*
(1) Actor	Internal Employee
(2) Means	Physically disconnecting network appliances to disrupt service
(3) Motive	Sabotage of S&G solution
(4) Outcome	**Interruption**
(5) Security Requirements	LIDL CP 3.3.2
(6) Probability	**Medium**

(7) Consequences	(8) Severity: Impact Area	Value	Score
Medium reputational loss due to solutions unavailability	Rep. & Customer Confidence	Medium	10
No big impact is expected	Safety & Health	Low	4
	Fines & Legal Penalties	Low	3
Medium productivity loss due to S&G service unavailability	Productivity	Medium	4
No big impact is expected	Financial	Low	1
	Relative Risk Score		**22**

A2R7

Area of Concern	*A2R7 - Phishing by providing false APP*
(1) Actor	External Attacker
(2) Means	Fake QR codes for downloadable APP in store
(3) Motive	Steal card details in APP
(4) Outcome	**Disclosure**
(5) Security Requirements	PCI DSS; LIDL CP 3.3.2
(6) Probability	**Medium**

(7) Consequences	(8) Severity: Impact Area	Value	Score
In case of disclosure and becoming public fact will lead to heavy fines and loss of reputation for the whole group.	Rep. & Customer Confidence	High	15
	Safety & Health	Low	4
May generate fines by being responsible for delivery of unsecure APP	Fines & Legal Penalties	Medium	6
No big impact is expected	Productivity	Medium	4
Reputational shock may reduce sales of S&G system.	Financial	Medium	2
	Relative Risk Score		**31**

A2R8

Area of Concern	*A2R8 - Disclosure by accessing BO*
(1) Actor	External Attacker / Internal Employee
(2) Means	Weak / Shared passwords. SNMP traffic between DBs and listeners
(3) Motive	Espionage / Blackmail on payment transactions
(4) Outcome	**Disclosure**
(5) Security Requirements	PCI DSS; LIDL CP 3.3.2
(6) Probability	**Low**

(7) Consequences	(8) Severity: Impact Area	Value	Score
In case of disclosure and becoming public fact will lead to loss of reputation for the whole group.	Rep. & Customer Confidence	Medium	10
	Safety & Health	Low	4
	Fines & Legal Penalties	Medium	6
After successful breach an attacker will most likely drop the database to harden the audit	Productivity	High	6
No big impact is expected	Financial	Low	1
	Relative Risk Score		**27**

A2R9

Area of Concern	*A2R9 - Exfiltration of daily report data*
(1) Actor	External attacker
(2) Means	Highjack a priviledged user account / Use new store infrastructure for LAN access
(3) Motive	Use data for espionage or blackmail purposes
(4) Outcome	**Disclosure**
(5) Security Requirements	PCI DSS; LIDL CP 3.3.2
(6) Probability	**Medium**

(7) Consequences	(8) Severity: Impact Area	Value	Score
In case of disclosure and becoming public fact will lead to loss of reputation for the whole group.	Rep. & Customer Confidence	Medium	10
No big impact is expected	Safety & Health	Low	4
May originate legal fines	Fines & Legal Penalties	Medium	6
After successful breach an attacker will most likely drop the database to harden the audit	Productivity	High	6
	Financial	Low	1
	Relative Risk Score		**27**

A1R10

Area of Concern	*A2R10 - Forwarding of card data from POS*
(1) Actor	External Attacker
(2) Means	Use RAM Scraper to forward data to HTTP server
(3) Motive	Steal of card data
(4) Outcome	**Disclosure**
(5) Security Requirements	PCI DSS; LIDL CP 3.3.2
(6) Probability	**Medium**

(7) Consequences	(8) Severity: Impact Area	Value	Score
Significant loss of reputation is expected in case of service unavailability	Rep. & Customer Confidence	High	15
No big impact is expected	Safety & Health	Low	4
May originate legal fines	Fines & Legal Penalties	High	9
Functionality and security of all POS devices must be requalified	Productivity	High	6
	Financial	Medium	2
	Relative Risk Score		**36**

Attachment V-II – Information Asset Risk Worksheet: PCI-DSS Compliant Data

Allegro - Worksheet 10.1	Information Asset Risk Worksheet
Information Asset	**Shop&Go Related Data**

Information Asset Risk

A3R1

Threat	
Area of Concern	*A3R1 - Insecure Protocols in MBWay Implementation*
(1) Actor	Internal / Third-Party employee with access to store LAN
(2) Means	By sniffing insecure traffic between user device and Payment Terminal/Marketing Hub server due to weak encryption
(3) Motive	App data collection, communication protocols, XML structures for espionage or own adwantage
(4) Outcome	**Disclosure**
(5) Security Requirements	PCI-DSS Compliance
(6) Probability	**High**

(7) Consequences	(8) Severity Impact Area	Value	Score
In case of disclosure and becoming public fact will lead to heavy fines and loss of reputation for the whole group.	Rep. & Customer Confidence	High	15
No big impact is expected	Safety & Health	Low	4
High fines due to PCI requirements violation (collateral)	Fines & Legal Penalties	High	9
Medium impact on functionality of S&G solution is expected, therefore leading to productivity and financial losses	Productivity	Medium	4
	Financial	Medium	2
	Relative Risk Score		34

A3R2

Threat	
Area of Concern	*A3R2 - Insecure App Build*
(1) Actor	External Attacker
(2) Means	Create a fake WiFi acess point and sniff the data / HTTP with weak keys
(3) Motive	App data collection, communication protocols, XML structures for espionage or own adwantage
(4) Outcome	**Modification**
(5) Security Requirements	LIDL NI 3.2.2
(6) Probability	**High**

(7) Consequences	(8) Severity Impact Area	Value	Score
In case of disclosure and becoming public fact will lead to heavy fines and loss of reputation for the whole group.	Rep. & Customer Confidence	High	15
No big impact is expected	Safety & Health	Low	4
No big impact is expected	Fines & Legal Penalties	Low	3
Medium impact on functionality of S&G solution is expected, therefore leading to productivity losses. High financial impact can be expected due to fraudulent oportunities which open to attacker	Productivity	Medium	4
	Financial	High	3
	Relative Risk Score		29

A3R3

Threat	
Area of Concern	*A3R3 - S&G Network architecture disclosed*
(1) Actor	External/Internal Attacker
(2) Means	Gain access to LAN by using scale's TP connection (and spoofing its MAC address - optional)
(3) Motive	Get access to secure store network, used for communication between devices; access files/databases
(4) Outcome	**Disclosure**
(5) Security Requirements	LIDL NI 3.2.2
(6) Probability	**High**

(7) Consequences	(8) Severity Impact Area	Value	Score
No big impact is expected	Rep. & Customer Confidence	Low	5
	Safety & Health	Low	4
Medium penaltis expected as collateral to such breach	Fines & Legal Penalties	Medium	6
High impact on productivity due to competitive advantage loss	Productivity	High	6
High impact on financial side due to information leak to competitors	Financial	High	3
	Relative Risk Score		24

A3R4

Threat	
Area of Concern	*A3R4 - S&G Network interruption*
(1) Actor	External/Internal Attacker
(2) Means	Access AP management backoffice and interrupt/modify functionality
(3) Motive	Sabotage/ Revenge seeking
(4) Outcome	**Interruption**
(5) Security Requirements	LIDL NI 3.2.2
(6) Probability	**Medium**

(7) Consequences	(8) Severity Impact Area	Value	Score
High reputational impact due to network availability issues	Rep. & Customer Confidence	High	15
No big impact is expected	Safety & Health	Low	4
No big impact is expected	Fines & Legal Penalties	Low	3
Gaining access to BO application of Access Points will permit an attacker disabling or modifing functionality of equipment, thus turning service unoperational. Financial impact will be high due to customers drop as well.	Productivity	High	6
	Financial	High	3
	Relative Risk Score		31

A3R5

Threat	
Area of Concern	*A3R5 - Unavailability of S&G Cloud Servers*
(1) Actor	External Attacker
(2) Means	DDOS attack on publicly alllocated servers
(3) Motive	Interruption of service for sabotage purposes
(4) Outcome	**Interruption**
(5) Security Requirements	LIDL NI 3.2.2
(6) Probability	**Low**

(7) Consequences	(8) Severity Impact Area	Value	Score
Unavailability will turn away certain ammount of active service customers (exact impact depends on unavailability time)	Rep. & Customer Confidence	Medium	10
No big impact is expected	Safety & Health	Low	4
No big impact is expected	Fines & Legal Penalties	Low	3
By making MH servers unreachable an attacker will drop the whole service pipeline. High productivity and financial impact.	Productivity	High	6
	Financial	High	3
	Relative Risk Score		26

A3R6

Threat	
Area of Concern	*A3R6 - Application code revealed*
(1) Actor	External/Internal Attacker
(2) Means	Application code reveal by means of reversed engineering
(3) Motive	Replication of application for fraud/espionage purposes
(4) Outcome	**Disclosure**
(5) Security Requirements	Lidl Software Development Requirements; Secure Development Best Practices
(6) Probability	**High**

(7) Consequences	(8) Severity Impact Area	Value	Score
Upon becoming public fact may lead to heavy reputationa drop by unavalability of group to provide secure APP	Rep. & Customer Confidence	High	15
No big impact is expected	Safety & Health	Low	4
No big impact is expected	Fines & Legal Penalties	Low	3
Significant productivity drop due necessary urgent bug fixes	Productivity	Medium	4
	Financial	High	3
	Relative Risk Score		29

A3R7

Threat	
Area of Concern	*A3R7 - S&G configuration data destroyed*
(1) Actor	Internal employee/Third party employee
(2) Means	Reset of configuration/misconfiguration
(3) Motive	Unintentional / Intentional will to harm the organization
(4) Outcome	**Destruction**
(5) Security Requirements	LIDL NI 3.2.2
(6) Probability	**Medium**

(7) Consequences	(8) Severity Impact Area	Value	Score
In case of disclosure and becoming public fact will lead to loss of reputation	Rep. & Customer Confidence	Medium	10
No big impact is expected	Safety & Health	Low	4
No big impact is expected	Fines & Legal Penalties	Low	3
Destruction of data will turn impossible certain type of sales through S&G	Productivity	Medium	4
	Financial	Medium	2
	Relative Risk Score		23

A3R8

Threat	
Area of Concern	*A3R8 - S&G data lost due to ransomware*
(1) Actor	External Attacker / Internal Employee
(2) Means	By using open ports/permissive filtering/active services
(3) Motive	Blackmail / Revenge seeking
(4) Outcome	**Destruction**
(5) Security Requirements	LIDL NI 3.2.2
(6) Probability	**Low**

(7) Consequences	(8) Severity Impact Area	Value	Score
In case of disclosure and becoming public fact will lead to loss of reputation for the whole group.	Rep. & Customer Confidence	Medium	10
	Safety & Health	Low	4
No big impact is expected	Fines & Legal Penalties	Low	3
Destruction of data will turn impossible certain type of sales through S&G	Productivity	Medium	4
Medium impact is expected on sales drop, as data is backuped on weekly basis	Financial	Medium	2
	Relative Risk Score		23

A3R9

Threat	
Area of Concern	*A3R9 - S&G data disclosed by IT staff*
(1) Actor	Internal Employee
(2) Means	Aware or unaware disclosure of information critical to project
(3) Motive	Unintended / Information Sale
(4) Outcome	**Disclosure**
(5) Security Requirements	LIDL AC 3.1.2
(6) Probability	**Low**

(7) Consequences	(8) Severity Impact Area	Value	Score
No big impact is expected	Rep. & Customer Confidence	Low	5
No big impact is expected	Safety & Health	Low	4
No big impact is expected	Fines & Legal Penalties	Low	3
Disclosure will influence the competitive advantage organization has with this project	Productivity	High	6
	Financial	High	3
	Relative Risk Score		21

Attachment V-III – Information Asset Risk Worksheet: Shop&Go Related Data

Allegro - Worksheet 10.1	Information Asset Risk Worksheet
Information Asset	**Purchase & Sale Data**

Information Asset Risk

A4R1

Threat	
Area of Concern	*A4R1 - Regular Price dumps*
(1) Actor	External attacker
(2) Means	By using flaws in protocol's security (HTTP) can see in clear text and request data from the server
(3) Motive	Espionage
(4) Outcome	**Disclosure**
(5) Security Requirements	PCI-DSS Compliance
(6) Probability	**High**

(7) Consequences	(8) Severity: Impact Area	Value	Score
In case of disclosure and becoming public fact may lead to loss of customer reputation	Rep. & Customer Confidence	Medium	10
No big impact is expected	Safety & Health	Low	4
No big impact is expected	Fines & Legal Penalties	Low	3
In long run will lead to financial and productivity losses due to lost competitive advantage.	Productivity	Medium	4
	Financial	High	3
	Relative Risk Score		**24**

A4R2

Threat	
Area of Concern	*A4R2 - Switch item prices*
(1) Actor	External Attacker
(2) Means	Modify application code and modify item names locally.
(3) Motive	Purchase expensive items for cheaper price
(4) Outcome	**Modification**
(5) Security Requirements	LIDL APP 3.2.5
(6) Probability	**High**

(7) Consequences	(8) Severity: Impact Area	Value	Score
No big impact is expected	Rep. & Customer Confidence	Low	5
May impact safety issues due to incorrect inventory I / O	Safety & Health	Medium	8
No big impact is expected	Fines & Legal Penalties	Low	3
High impact in both areas as substituting prices will lead to big losses and inventory problems	Productivity	High	6
	Financial	High	3
	Relative Risk Score		**25**

A4R3

Threat	
Area of Concern	*A4R3 - Price/Item Pictures modification*
(1) Actor	External/Internal Attacker
(2) Means	Gain access to LAN by using scale's TP connection (and spoofing its MAC address - optional)
(3) Motive	Get access to secure store network, used for communication between devices; access files/databases
(4) Outcome	**Modification**
(5) Security Requirements	LIDL NI 3.2.2, LIDL ATA 3.1.7
(6) Probability	**Low**

(7) Consequences	(8) Severity: Impact Area	Value	Score
Will impact cutomer confidence in medium terms (scale prices only)	Rep. & Customer Confidence	Medium	10
No big impact is expected	Safety & Health	Low	4
No big impact is expected	Fines & Legal Penalties	Low	3
High impact on productivity due to additional job needed for restore	Productivity	High	6
High impact on financial side due to lost profits	Financial	Medium	2
	Relative Risk Score		**25**

A4R4

Threat	
Area of Concern	*A4R4 - Delete data on exposed devices*
(1) Actor	External Attacker / Internal Employee
(2) Means	By using defalt password / Login combination delete functinal data
(3) Motive	Intentional or unintentional sabotage
(4) Outcome	**Interruption**
(5) Security Requirements	LIDL ATA 3.1.7
(6) Probability	**Medium**

(7) Consequences	(8) Severity: Impact Area	Value	Score
Will impact cutomer confidence in medium terms (scale prices only)	Rep. & Customer Confidence	Medium	10
No big impact is expected	Safety & Health	Low	4
No big impact is expected	Fines & Legal Penalties	Low	3
Gaining access to scales management interface attacker may disable or modify individual scale, but repeat this process for other scales in shop	Productivity	High	6
	Financial	High	3
	Relative Risk Score		**26**

A4R5

Threat	
Area of Concern	*A4R5 - Prices unavailability*
(1) Actor	External Attacker
(2) Means	DDOS attack on publicly alllocated servers
(3) Motive	Interruption of service for sabotage purposes
(4) Outcome	**Interruption**
(5) Security Requirements	LIDL NI 3.2.2, LIDL ATA 3.1.7
(6) Probability	**Low**

(7) Consequences	(8) Severity: Impact Area	Value	Score
Unavailability will turn away certain ammount of active service customers (exact impact depends on unavailability time)	Rep. & Customer Confidence	Medium	10
No big impact is expected	Safety & Health	Low	4
No big impact is expected	Fines & Legal Penalties	Low	3
By making MH servers unreachable an attacker will drop the whole service pipeline. High productivity and financial impact.	Productivity	High	6
	Financial	High	3
	Relative Risk Score		**26**

A4R6

Threat	
Area of Concern	*A4R6 - Application functionality modified*
(1) Actor	External/Internal Attacker
(2) Means	Application code reveal and modified by means of reversed engineering
(3) Motive	Replication of application for fraud/espionage purposes
(4) Outcome	**Disclosure**
(5) Security Requirements	LIDL APP 3.2.5; Secure Development Best Practices
(6) Probability	**High**

(7) Consequences	(8) Severity: Impact Area	Value	Score
Upon becoming public fact may lead to heavy reputationa drop by unavalability of group to provide secure APP	Rep. & Customer Confidence	High	15
No big impact is expected	Safety & Health	Low	4
No big impact is expected	Fines & Legal Penalties	Low	3
Significant productivity drop due necessary urgent bug fixes	Productivity	Medium	4
	Financial	High	3
	Relative Risk Score		**29**

A4R7

Threat	
Area of Concern	*A4R7 - Unintended price modification*
(1) Actor	Internal employee
(2) Means	By using BO application change of prices on national level intentionally or due to error of input
(3) Motive	Intentional harm or error of input - no integratoin mechanisms
(4) Outcome	**Modification**
(5) Security Requirements	LIDL NI 3.2.2
(6) Probability	**High**

(7) Consequences	(8) Severity: Impact Area	Value	Score
In case of disclosure and becoming public fact will lead to loss of reputation	Rep. & Customer Confidence	Medium	10
No big impact is expected	Safety & Health	Low	4
No big impact is expected	Fines & Legal Penalties	Low	3
Significant productivity drop due necessary urgent price fixes	Productivity	Medium	4
	Financial	High	3
	Relative Risk Score		**24**

A4R8

Threat	
Area of Concern	*A4R8 - Exfiltration of promotion data*
(1) Actor	External attacker
(2) Means	Highjack a priviledged user account / Use increased store infrastructure for LAN access
(3) Motive	Use data for espionage or blackmail purposes
(4) Outcome	**Disclosure**
(5) Security Requirements	LIDL NI 3.2.2, LIDL ATA 3.1.7
(6) Probability	**Medium**

(7) Consequences	(8) Severity: Impact Area	Value	Score
In case of disclosure and becoming public fact will lead to loss of reputation for the whole group.	Rep. & Customer Confidence	Medium	10
No big impact is expected	Safety & Health	Low	4
May originate legal fines	Fines & Legal Penalties	Medium	6
After successful breach an attacker will most likely drop the database to harden the audit	Productivity	High	6
High impact due to competitive loss	Financial	High	3
	Relative Risk Score		**29**

A4R9

Threat	
Area of Concern	*A4R9 - Disclosure by accessing BO*
(1) Actor	External Attacker / Internal Employee
(2) Means	Weak / Shared passwords. SNMP traffic between DBs and listeners
(3) Motive	Espionage / Blackmail on daily sales for statistical purposes
(4) Outcome	**Disclosure**
(5) Security Requirements	LIDL NI 3.2.2, LIDL ATA 3.1.7
(6) Probability	**Low**

(7) Consequences	(8) Severity: Impact Area	Value	Score
In case of disclosure and becoming public fact will lead to loss of reputation for the whole group.	Rep. & Customer Confidence	Medium	10
No big impact is expected	Safety & Health	Low	4
May originate legal fines	Fines & Legal Penalties	Medium	6
After successful breach an attacker will most likely drop the database to harden the audit	Productivity	High	6
	Financial	Medium	2
	Relative Risk Score		**28**

Attachment V-IV - Information Asset Risk Worksheet: Purchase & Sale Data

Allegro - Worksheet 10.1	Information Asset Risk Worksheet
Information Asset	External Undesirable Data

A5R1

Information Asset Risk		
Threat	Area of Concern	*A5R1 - Unintended Guest Network Usage*
	(1) Actor	Client / Store Employee
	(2) Means	Accessing illegar information through client WiFi AP
	(3) Motive	Use-as-proxy, Unawareness
	(4) Outcome	**Disclosure**
	(5) Security Requirements	National Content Regulations / Criminal Law, LIDL AC 3.1.2
	(6) Probability	**High**

(7) Consequences	(8) Severity Impact Area	Value	Score
In case of disclosure and becoming public fact may lead to loss of customer reputation	Rep. & Customer Confidence	Medium	10
No big impact is expected	Safety & Health	Low	4
May lead to heavy fines in case LIDL name gets associated with illegal content access provisioning	Fines & Legal Penalties	High	9
In case of scandal, Client WiFi Infrastructure will have to be revisioned, which may lead to service stop	Productivity	Medium	4
	Financial	Medium	2
	Relative Risk Score		**29**

A5R2

Information Asset Risk		
Threat	Area of Concern	*A5R2 - Backup / Configuration files*
	(1) Actor	Internal / Third Party Employee
	(2) Means	Discovey of Configuration/Backup Files with sensitive information on Network Shares by attacker
	(3) Motive	Unawereness / Negligence
	(4) Outcome	**Disclosure**
	(5) Security Requirements	LIDL B&R 3.1.3
	(6) Probability	**Medium**

(7) Consequences	(8) Severity Impact Area	Value	Score
No big impact is expected	Rep. & Customer Confidence	Low	5
	Safety & Health	Low	4
	Fines & Legal Penalties	Low	3
High impact in both areas as access to this information will give larger autonomy to the attacker	Productivity	High	6
	Financial	High	3
	Relative Risk Score		**21**

A5R3

Information Asset Risk		
Threat	Area of Concern	*A5R3 - Unnecessary Software / Lack of Hardening*
	(1) Actor	External/Internal Attacker
	(2) Means	By using installed applications with known security issues
	(3) Motive	Access to internal network to escalate privilidges and get access to information
	(4) Outcome	**Modification**
	(5) Security Requirements	LIDL APP 3.2.5 , LIDL CS 3.2.3
	(6) Probability	**Medium**

(7) Consequences	(8) Severity Impact Area	Value	Score
No big impact is expected	Rep. & Customer Confidence	Low	5
	Safety & Health	Low	4
	Fines & Legal Penalties	Low	3
High impact in both areas as access to this information will give larger autonomy to the attacker	Productivity	High	6
	Financial	Medium	2
	Relative Risk Score		**20**

A5R4

Information Asset Risk		
Threat	Area of Concern	*A5R4 - Illegal / Restricted information stored*
	(1) Actor	Internal / Third party employees
	(2) Means	Downloaded or copied files which origin is illegal or compromising the organization
	(3) Motive	Unawereness / Negligence
	(4) Outcome	**Disclosure**
	(5) Security Requirements	LIDL ATA 3.1.7
	(6) Probability	**Medium**

(7) Consequences	(8) Severity Impact Area	Value	Score
High reputation drop in case fact of storage becomes public	Rep. & Customer Confidence	High	15
No big impact is expected	Safety & Health	Low	4
Elevated fines in case the fact of storage becomes public	Fines & Legal Penalties	High	9
No big impact is expected	Productivity	Low	2
	Financial	Low	1
	Relative Risk Score		**31**

A5R5

Information Asset Risk		
Threat	Area of Concern	*A5R5 - Malware Distribution by fake WiFi AP*
	(1) Actor	External Attacker
	(2) Means	Usage of fake client AP to distribute malware
	(3) Motive	Blackmail / Reputational attack
	(4) Outcome	**Interruption**
	(5) Security Requirements	LIDL NI 3.2.2
	(6) Probability	**Medium**

(7) Consequences	(8) Severity Impact Area	Value	Score
Unavailability will turn away certain ammount of active service customers (exact impact depends on unavailability time)	Rep. & Customer Confidence	Medium	10
No big impact is expected	Safety & Health	Low	4
No big impact is expected	Fines & Legal Penalties	Low	3
By making MH servers unreachable an attacker will restrict clients' access to the service	Productivity	Medium	4
	Financial	Medium	2
	Relative Risk Score		**23**

Attachment V-V – Information Asset Risk Worksheet: External Undesirable Data

Area of Concern	Risk Score	CIA Priority?	Probability	Suggested Action	Suggested Measures			
A1R1 - Client data is stolen by MitM attack type	26	CIA Priority	Medium	Mitigate/Defer	MS12	MS10		
A1R2 - Client data stolen by LWL-M WLAN crack	31	CIA Priority	Low	Defer/Accept				
A1R3 - Client Data stolen by breaching store LAN	31	CIA Priority	High	Mitigate	MS11	MS10	MS13	MS14
A1R4 - Client Data stolen by DB Crack	29	CIA Priority	High	Mitigate	MS07	MS09	MS08	
A1R5 - Employee data breach by BO access	29	CIA Priority	Medium	Mitigate/Defer	MS05			
A1R6 - Employee and Client data leaked	26	CIA Priority	High	Mitigate/Defer	MS14			
A1R7 - Client Data Destroyed	30	No Priority	Medium	Mitigate/Defer	MS03	MS09		
A1R8 - Client data sniffed in between APP & Server Communication	28	CIA Priority	High	Mitigate/Defer	MS01	MS10	MS09	
A1R9 - Employee Data Modification	22	No Priority	Low	Defer/Accept				
A1R10 - Client Information unavailable	31	No Priority	Low	Defer/Accept				
A2R1 - Insecure Protocols in MBWay Implementation	31	No Priority	Medium	Mitigate/Defer	MS01	MS02	MS10	
A2R2 - Payment data availability	24	No Priority	High	Mitigate/Defer	MS06	MS17		
A2R3- Payment Data Availability	30	CIA Priority	Medium	Mitigate/Defer	MS11	MS10	MS13	MS14
A2R4 - Payment Data lost due to DB crack	26	No Priority	High	Mitigate/Defer	MS07	MS09	MS08	
A2R5 - PinPad physical substitution	31	No Priority	Medium	Mitigate/Defer	MS08	MS03		
A2R6- CDE Interruption	22	No Priority	Medium	Mitigate/Defer	MS13			
A2R7 - Phishing by providing false APP	31	No Priority	Medium	Mitigate/Defer	MS02	MS10		
A2R8 - Disclosure by accessing BO	27	No Priority	Low	Defer/Accept				
A2R9 - Exfiltration of daily report data	27	No Priority	Medium	Mitigate/Defer	MS11	MS10	MS13	MS14
A1R10 - Client Information unavailable	31	No Priority	Low	Defer/Accept				
A3R1 - Insecure Protocols in MBWay Implementation	34	No Priority	High	Mitigate	MS01	MS02		
A3R2 - Insecure Protocols in MBWay Implementation	29	CIA Priority	High	Mitigate	MS01	MS02		
A3R3 - SHOP&GO Network architecture disclosed	24	No Priority	High	Mitigate/Defer	MS11	MS09		
A3R4 - SHOP&GO Network interruption	31	No Priority	Medium	Mitigate/Defer	MS09	MS10		
A3R5 - Unavailability of GK Cloud Servers	26	No Priority	Low	Defer/Accept				
A3R6 - Application code revealed	29	No Priority	High	Mitigate	MS04	MS10	MS01	
A3R7 - SHOP&GO configuration data destroyed	23	CIA Priority	Medium	Mitigate/Defer	MS16	MS15		
A3R8 - SHOP&GO data lost due to ransomware	23	CIA Priority	Low	Defer/Accept				
A3R9 - SHOP&GO data disclosed by IT staff	21	No Priority	Low	Defer/Accept				
A4R1 - Regular Price dumps	24	No Priority	High	Mitigate/Defer	MS01	MS10	MS09	
A4R2 - Switch item prices	25	No Priority	High	Mitigate/Defer	MS01	MS02		
A4R3 - Price/Item Pictures modification	25	No Priority	Low	Defer/Accept				
A4R4 - Delete data on exposed devices	26	CIA Priority	Medium	Mitigate/Defer	MS09			
A4R5 - Prices unavailability	26	CIA Priority	Low	Defer/Accept				
A4R6 - Application functionality modified	29	No Priority	High	Mitigate	MS04	MS10	MS01	
A4R7 - Unintended price modification	24	No Priority	High	Mitigate/Defer	MS09	MS11		
A4R8 - Exfiltration of promotion data	29	No Priority	Medium	Mitigate/Defer	MS09	MS11	MS10	MS07
A4R9 - Disclosure by accessing BO	28	No Priority	Low	Defer/Accept				
A5R1 - Unintended Guest Network Usage	29	CIA Priority	High	Mitigate	MS17			
A5R2 - Backup / Configuration files	21	CIA Priority	Medium	Mitigate/Defer	MS03	MS15	MS16	
A5R3 - Unnecessary Software / Lack of Hardening	20	No Priority	Medium	Mitigate/Defer	MS08	MS07		
A5R4 - Illegal / Restricted information stored	31	CIA Priority	Medium	Mitigate/Defer	MS15	MS16		
A5R5 - Malware Distribution by fake WiFi AP	23	No Priority	Medium	Mitigate/Defer	MS12	MS03		

Attachment VI – Threat Scenarios and Mitigation Measures

Suggested Measures			Containers																
Measure Id	Short Name	Measure Description	3rd party Rack	Cisco ASA FW / IDS	External VPN connection	Fortinet FW	S&G Cloud	Mobile Attendant	MPOS Server	PinPad Terminal	Shop&Go App (Android / iOS)	Store BO (Backoffice) Server	POS device	Store Switch & Router	Scale Device	Paytower Device	Other	**Implementation Effort**	**Covered TS**
MS01	TLS/HTTPS	Use TLS, All pages must be served over HTTPS, The HTTP Strict Transport Security Header must be used, Cookies must be marked as Secure					X	X	X		X							**3**	8
MS02	OWASP10	Use OWASP Top10 check / Guarantee AppSecurity through PenTest	X				X	X	X		X	X	X					**3**	5
MS03	SIEM	Use SIEM solution to detect intrusion / Use honeypots	X	X		X						X		X				**9**	4
MS04	Code_Obfr	Application’s code should be obfuscated, for example, with the ProGuard tool.						X			X							**2**	2
MS05	Data_Encr	Store all GDPR compliant data encrypted	X	X	X		X	X	X	X	X	X	X	X	X	X		**8**	1
MS06	Infrastructure	Reinforce store infrastructure (add switching / routing devices)												X				**7**	1
MS07	DB Hard	Implement Database Hardening; When possible, disable default SYS-like accounts;							X			X			X			**5**	4
MS08	Asset Mng	Inventory of applications, versions & owners. Implement or adjust a regular mechanism for installation of security updates.		X		X		X	X	X	X	X	X	X	X	X		**8**	4
MS09	PSSWRD	Change all default passwords. Use password management software. Enforce the usage of strong passwords across all company	X	X		X	X	X	X	X	X	X	X	X	X	X		**5**	10
MS10	Protocols	Configure and use encrypted protocols whenever possible. If encryption protocols are not available for some applications, evalu-ate the possibility of VPN usage	X	X	X		X	X	X	X	X	X	X	X	X	X		**5**	12
MS11	Access Policies	Design and create access policies based on business needs and en-force it using firewalls or native filtering capabilities of network devices	X	X		X			X			X		X		X		**4**	6
MS12	WIPS	Implement a Wireless Intrusion Prevention System	X	X														**8**	2
MS13	Phys_Mon	Implement Physical Security Monitoring						X		X			X				X*	**7**	4
MS14	CloudControl	Use cenralized DB console for access control (e.g. Cloud Control)							X			X						**5**	4
MS15	Log Indexing	Use Log-indexing system for version / patching checks	X	X		X			X	X		X	X	X	X			**9**	3
MS16	Awareness	Define and implement internal awareness programms by functional area															X**	**5**	3
MS17	Traffic filter	Implement trafic filter / DNS blacklist	X			X	X											**4**	2

*physical security of app-related info, QR codes in shop, dow nload links etc.

**aw arness programms for store employees, related to solution security

Attachment VII – Measures and Containers