SECURITAS SECURITY METHODOLOGY

A Methodological Approach to the Development of Security Solutions

Securitas

SECURITAS SECURITY METHODOLOGY

PREPARED BY
Feramuz ÇALIŞKAN

CONTRIBUTORS
Hüseyin ERİM
Berti BORA
Gökhan USTA
Aygen ÜNDAN
Memet HANLIOĞLU
Emre ERDAL
Adem YÜKSEL
Alp KARABAŞ
Volkan AKSU
Can ULUATAM

PRODUCTION EDITOR
Elif Duygu KOCA

REDACTION
İrem YEŞİL
Tuğçe TOPÇU

DESIGN
Dwt Mandalina

PRINT
Emsal Matbaa Tanıtım

SECURITAS SECURITY METHODOLOGY

A Methodological Approach to the Development of Security Solutions

Securitas

Securitas

Preface

Security is at the forefront of all basic needs, but it is a difficult equation to solve when it comes to providing security to mitigate risks at an affordable cost.

To solve this difficult equation, we have thought, studied, drawn, written, corrected, tested, tried hard, corrected again, and developed the methodology you will find in this book, based on the knowledge and experience we have gained at Securitas over the years.

This is an alive book that will evolve with the new information and experience we are constantly accumulating. As a leading brand in the private security industry, it is our pleasure to share with you the details of our work.

We are also pleased to share that, based on this methodology, the facilities you are responsible for are protected in the smartest way possible.

We hope that Securitas Security Methodology will lead the way and be enthusiastically embraced as the most refined synonym for the “Integration of Knowledge, People and Technology” in the security industry.

Murat Kösereisoğlu

Country President Securitas Turkey

Introduction

As with any business, building a security service with scientific methods and based on experience in the industry is a must. Only a service developed in this way makes it possible to accurately identify the risks of an organisation, develop the appropriate solution to mitigate them, and maintain the quality standards achieved.

Securitas Security Methodology (SSM) aims to explain how a security service should be structured from the start and throughout its lifecycle, how the risks should be identified and scaled, the important concepts that influence the risk management process of organisations, the hierarchy used for developing the appropriate solutions and the practices that help to maintain and increase the quality standards. Anyone working in the security industry, procuring security services or working as an academic in a university can benefit from this methodology regardless of their role. Undoubtedly, in a dynamic and ever-evolving world, this methodology will also evolve and renew itself.

This methodology is the result of the collective experience of Securitas People. Many valuable experts who work at Securitas have made very important contributions to this study. We hope that Securitas Security Methodology, which combines years of experience with the latest technological developments in the industry, will make impacting contributions to the security world.

Feramuz Çalışkan

Deputy Head of Security Processes and Quality

“For efficient business continuity, the security service must be a “system” via a method that includes both pre-service and post-service phases.”

Methodological Approach to Security Solutions

Organisations operate in an increasingly complex and uncertain environment where expectations are also constantly rising. This situation exposes organisations to risks that can significantly affect the outcome of their activities. (Hopkin, 2017) In such complex and uncertain market conditions, the protective security services developed by Securitas aim to eliminate or minimise the risks faced by organisations through optimised solutions.

The security services have an impact on various parties. While the main parties are the recipients of these services (clients) and the security organisation providing the service (Securitas), other parties affected by these activities are the public, the authorities, the Securitas's suppliers, and third parties who are recipients of services at client sites, such as the facility's employees and visitors and those of neighboring facilities.

As market conditions become more challenging and risks diversify, expectations of organisations increase.

Security services are also influenced by numerous factors. Legal obligations, risks, technological developments, business objectives, location and industry are some of the important factors that influence the security service process. Since security service involves several dimensions and phases, it is necessary to structure it with a system or, in other words, a method. Therefore, the security service needs to be configured in a "system" that includes initiation (before),

implementation (during) and quality control (during and after) of the service.

The method to be followed must include the following,

— How the risk will be identified,
— How the solutions can be implemented to mitigate those risks,
— How the quality controls for the implementation are to be carried out.

It is therefore essential for a security organisation to have a methodology for all these processes.

So what is a methodology or a methodological approach in the broader sense?

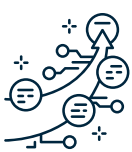
“The methodological approach is a roadmap to guide organisations through their challenging journey.”

What is a Methodological Approach?

Methodology, as it is first called, is the general programme or roadmap that organisations follow to carry out their activities effectively and achieve their multiple objectives.

Methodology as it is first called “is the general program or roadmap that organisations follow to carry out their activities effectively and achieve their multiple objectives”.

This methodology enables Securitas to standardise its understanding of risk and its risk-based approach to solutions globally through a scientific process and to ensure that the results and achievements can be replicated by others at different points in time.



It plays an active role in determining the organisation’s internal dynamics, capabilities, and activities, as well as its ability to coordinate both internally and with the external environment.

What is the importance of methodology in the world of security?

Securitas Security Methodology deals with the analysis, classification and development of risk mitigation solutions based on the collected information on a potential risk and its possible way of occurrence, using a scientific approach that provides the necessary perspective for the most accurate structuring of the security service.

The solutions should ensure that the security service is structured to mitigate risks according to the principles of efficiency and promote confidence among the stakeholders at the same time. This requires a scientific approach that should select the most efficient from a range of activities.

“Increasing competition, changing market conditions, complex and multi-layered security risks require a methodical approach to security services.”

Why is a Methodology Necessary in Security?

A Security Organisation needs a methodological approach in order to;

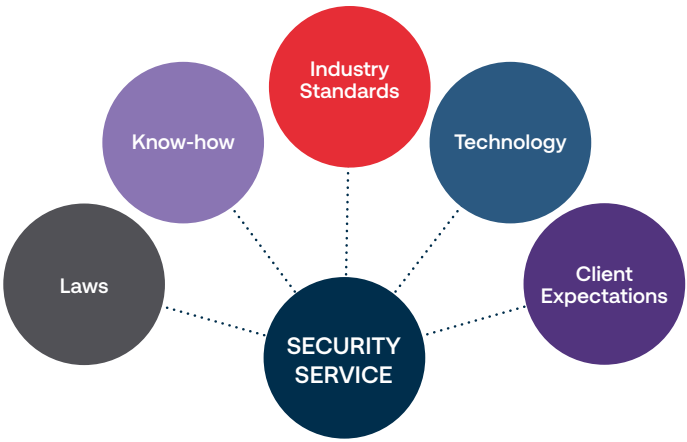
- Contribute to the decision-making process by taking into account the external factors of the organisation,
- Map the decision-making process,
- Be a guide for all those involved in creating a service process,
- Contribute to systematically identify and eliminating factors that could have a negative impact on plans and activities,
- Have a roadmap and guide that helps organisations achieve their business goals,
- Plan business activities and their continuity,
- Improve coordination between stakeholders in structuring, initiating, implementing, and testing the security service,
- Conduct the services in accordance with legislation and national and international industry standards,
- Guide for businesses to properly prepare for their activities.

Thus, a methodological approach helps to set the goals of an organisation and determine its vision and mission, while building and maintaining the identity of the organisation

A security organisation that has a methodology can effectively mitigate the risks. Moreover, the methodology, if

As today's security problems become more multidimensional and complex, solutions also require a multilevel coordination between multiple functions.

successfully implemented with all its aspects, provides the organisation with an important competitive advantage.



For a security company providing security services in different facilities, organisations, businesses and even regions, a systematic approach is required due to applicable legislation, industry standards and client expectations.

As in all industries, it is of great importance for those working in the security industry to know their work thoroughly and to develop new solutions and ideas. In order to have a comprehensive knowledge and to be able to develop innovative ideas. It is indispensable to understand the existing ideas and solutions and to examine them with a systematic approach. Only this approach helps to address the different parts of Security practises holistically.

The methodological approach creates a competitive advantage through;

— Complying with legislation and quality standards,
— Addressing client expectations,
— Being efficient, effective and sustainable,

— Taking into account the contribution and impact of all stakeholders.

To thoroughly understand an organisation and its security needs and to develop innovative ideas for a solution, details must be examined with a systematic approach accompanied by experiential knowledge.

In a methodological approach, it is important that the information gathered on a topic contributes to the development, classification and analysis of an idea. At this point, the "security methodology" serves as a roadmap for the stakeholders, describing the necessary steps for the security service to be created.

Securitas Security Methodology (SSM) describes the steps that need to be taken to ensure that optimal security solutions meet the client's security needs and that they can be produced and maintained. It outlines the security processes and serves as a guide for security professionals.

The processes expressed in the Securitas Security Methodology are of great importance in building long-term, mutually beneficial relationships with clients. Securitas security professionals are therefore expected to adhere to the methodology. SSM, in accordance with local legislation and Securitas policies, is a guide for providing security services to the same high standards.

Securitas' Security Methodology plays an important role in Securitas' ability to build long-term, mutually beneficial relationships with her clients.

“Securitas’ Security Methodology eliminates or mitigates risks that can affect productivity and business continuity.”

Securitas Security Methodology

Securitas has developed the Securitas Security Methodology (SSM) by systematically bringing together the knowledge and experience accumulated over time.

The approach to configuring and implementing security services has been systematised over time at Securitas. Securitas Security Methodology (SSM) aims to eliminate or mitigate the risks to an acceptable level by;

— Responding to the needs of clients in various segments,
— Developing security solutions at optimal cost with high efficiency and added value,
— Striving for integrated security solutions with an emphasis on advanced technologies,
— Ensuring that Securitas' various parties and departments apply the same quality standards at all locations.

Securitas' priority is to provide its clients with highly effective security services at a reasonable cost. Thanks to its ability to deliver solutions that stand out from those of its competitors.

All Securitas' activities are in line with its client-centric and quality-driven strategy. In line with this strategy and in order to offer more effective solutions to its clients, Securitas divides the market in which it operates into different categories characterised by commonalities. These categories are divided into segments and service categories.

For example, "production industries" is a segment for Securitas, while under this segment "factory" is a site category and "warehouse" would be another site category. Segments and site categories allow some common practises to be configured for common needs. While all security services provided in different segments and site categories are based on the common principles within SSM and its framework. The segment- and site-specific operational guidelines are also developed according to the same framework.

The careful implementation of the principles for the execution of services within Securitas Security Methodology and the control of the principles through specific methods contribute to ensuring business continuity.

How can we help make your world a safer place?
Thanks to Securitas' technological capabilities, digital applications, and extensive experience gained over the years, that are in line with her clients' requirements.

Securitas applies Securitas Security Methodology to make its clients' world a safer place.

In line with this objective, Securitas Security Methodology is used to;

— Identify and prioritise the facility's security risks, taking into account the likelihood and impact of those risks,
— Minimise or eliminate risks with the most effective, cost-efficient and sustainable solutions (deterrents),
— Detect and verify the occurrence of risks using the most appropriate methods,
— Delay the magnification of harm in the event of an incident and implementi the appropriate intervention in the most accurate and effective way possible,
— Ensure that the necessary actions are taken collectively by creating solutions, operational improvements, and task development,
— Ensure that processes are properly implemented and corrective actions are taken.

Scope of Securitas Security Methodology

It is assumed that all steps of Securitas Security Methodology will find a more precise implementation possibility in medium and large businesses.

Securitas Security Methodology can be used by all businesses, regardless of industry or size, in setting up and managing security services.

The Securitas Security Methodology can be adapted for use in small businesses or workplaces, but modifications to the steps may be required.

“Securitas Security Methodology, from data collection to areas of improvement, is applied in 5 steps.”

Securitas Security Methodology Steps

Securitas Security Methodology consists of five steps. These steps are as follows:

1. ***Current Situation Analysis (CSA),***
2. ***Security Service Risk Assessment (SSRA),***
3. ***Solutions,***
4. ***Implementation,***
5. ***Quality Control.***

Securitas Security Methodology
Step One:

Current Situation Analysis (CSA)

1. Current Situation Analysis (CSA)

Current Situation Analysis (CSA) is used to identify and recognise the general characteristics of the organisation in which the security services are to be provided.

The purpose of the Current Situation Analysis (CSA) is to get to know and understand the organisation that requires the security service, and then to present the current security status of the organisation clearly within its environment and provide a snapshot of that status. It helps to understand the current security structure and awareness, administrative and operational procedures, as well as the geographical and socio-economic environment and business dynamics. CSA is also the accurate physical examination and reporting of the physical condition of the facilities, areas, and/or structures to be protected.

Each step of the methodology uses the data and results obtained in the previous step. In this context, “Accurate and effective performance of the Current Situation Analysis (CSA) ensures that an accurate and valid security services risk assessment is performed in the next step”. CSA conducted with insufficient observation may result in potential risks that are not being properly understood and assessed, which in turn may lead to missing the necessary security solutions in the third stage.

The data obtained during the Current Situation Analysis is used to determine the risks of the facility and thus to develop the right security solutions.

Current Situation Analysis is a study aimed at taking an up-to-date snapshot of the organisation.

The complete and correct performance of the current situation analysis contributes to the correct construction of the solutions that will be needed in the third step. This is because in order to design the security needs of the organisation and the most appropriate solutions to meet those needs, the conditions under which it lives must be fully and accurately revealed.

CSA is first step and It is crucial that the first step is taken properly to ensure that following steps are taken correctly.

Failure to properly identify the current status can have unintended consequences for both the client and Securitas. Therefore, it is crucial that the first step is taken properly to ensure that the following steps are taken correctly. CSA is presented to the client and confirmed that it is correct and complete.

The following points are considered and carried out in the Current Situation Analysis:

a. Initial preparations are made to get an overview of the facility/building/area where the CSA is to take place. Information from open sources such as the client's website, previous incidents, and damages at similar locations within Securitas service sites, crime statistics of the area where the facility is located, instructions for similar site categories (as post instructions have already been created give an idea on possible risks), Google Earth images of the premises, etc. are reviewed. This preliminary work saves time and helps in planning the activities, which can then be carried out more effectively.

b. Information about the client's requests is initially collected both from Securitas' Client Excellence Program (CEP) and Securitas employees who have initially been in contact with the client representatives.
c. It is highly advised that the client provides a guide for CSA.
d. When conducting the CSA, the segment of the site is identified and each service post such as access control points, perimeters, car parks, production facilities, warehouses office buildings are audited.
e. The security measures available at each service post, best practices based on the measures in place, and any security gaps are identified. The data obtained here is used as the basis for the next step, the risk analysis.

CSA is the first step in implementing Securitas Security Methodology. Since all subsequent steps of the methodology are based on the information gathered at this stage, it is crucial to identify the most accurate and clear information possible about the status of the organisation.

Therefore, the "foundation" of the Current Situation Analysis should be carried out as precisely and in as much detail as possible. Remember that the Current Situation Analysis and Security Service Risk Assessment steps are interlinked.

Securitas Security Methodology
Step Two:

Security Service Risk Assessment (SSRA)

2. Security Service Risk Assessment (SSRA)

Risk,

— Is a probability that expresses uncertainty,
— Reveals uncertainty about the results in the implementation of decisions,
— Is the probability that a planned activity does not take place as desired or that an undesirable event will occur.

According to the Great Larousse, the literal meaning of the term "risk" is the possibility of the occurrence of an event that may lead to harm or danger.

The concept of risk appears as an objective expectation of loss. The loss can sometimes be the loss of materials in a plant or factory such as copper cables, office supplies, valuable documents/money, valuable materials for production, and raw materials. In some cases, it can be the loss of reputation, and in other cases the loss of human life. One should bear in mind that a risk that is considered negligible and therefore ignored can lead to unavoidable damage and crises for the facility, the facility's staff, and even the community. Therefore, it is important to assess each risk and develop the most appropriate measures (solutions) for the risks envisaged within the organisational strategy and acceptable risk appetite. This

process is referred to as Security Service Risk Assessment (SSRA). SSRA, in its simplest sense, is the identification of potential risks that impact the organisation, the frequency of occurrence of these identified risks, and the impact they cause when they occur.

Although the concept of risk appetite will be discussed in the following sections, it is right to mention already now that this concept is important to define the solutions to mitigate the identified risks. Risk Appetite is the level of risk the organisation is willing to take in creating value. Corporate stress causes a difference between the activities that need to be performed and the activities that take place, which often has a negative impact on the organisation. This condition is called corporate stress.

SSRA and the measures (solutions) to be taken are critical in the process of mitigating the risks of the organisation to acceptable limits within the client's risk appetite.

Through the assessment of the organisation's objectives and strategy, any risk that is above the acceptable limits for the organisation and that, if it occurs, may cause losses that are above the limits that the organisation can contemplate and accept, becomes a source of organisational stress.

Stress is a concept that sometimes has positive and sometimes devastating effects. Corporate stress in terms of security practices and risk perception can have an impact not only on management and employees, but also on business processes, suppliers, and other stakeholders who supply inputs or provide services to the organisation. Take a factory during the construction phase. Valuable materials are being installed on the construction site of this factory and there is a project schedule that must be adhered to. The loss or theft of small pieces of wood or small building materials may be considered acceptable by the project management team.

However, the theft of copper cable drums from the construction site can be an unacceptable loss. So for the project management team, the theft of copper cable drums is a risk that exceeds their risk appetite. They should therefore take measures (security solutions) to prevent the theft of these cables. If no precautions are taken for these copper cable drums, this perception of risk becomes a source of stress after a while. In the same example, assume that a copper cable with a very low value is stolen. The occurrence of a risk that exceeds the acceptable risk appetite leads to a significant increase in the stress level in the organisation.

In this case, the risk of theft of cable drums could initially be minimised simply with a lock and/or an outdoor alarm system. However, if a small theft occurs, the stress in the organisation increases, and measures may be taken that go beyond what was originally necessary. This situation should serve as an example of the negative impact of the concept of corporate stress on decision-making processes. Corporate stress can be caused by risk perception as well as by many different factors. Identifying the necessary solutions and implementing them timely will eliminate the source of corporate stress and improve the organisational climate by;

— Careful use of corporate resources,
— Increased productivity,
— Safe and comfortable working environment,
— Strong employee engagement,

which results in achieving targets.

The first step in combating stress in organisations is to know exactly what the source and possible effects of stress are. Security risks, which are one of the factors that lead to organisational stress, can only be managed through an SSRA and the appropriate measures (solutions).

Eliminating all risks affecting the organisation and maintaining a corporate life without risks is not a realistic expectation. Any risk that does not have a potentially negative impact on the organisation in terms of organisational strategies does not require precautionary measures.

Security Service Risk Assessment (SSRA), which focuses on security activities is the process of identifying potential threats to facilities and their planned processes and uncovering the existing vulnerabilities in these structures.

SSRA is the process of identifying the unacceptable risks and the assessment of potential losses such as human lives, property damages, and corporate reputation that may occur due to threats and vulnerabilities.

This is an important step in the process of defining and implementing corporate strategies. All risks that may have an impact on the organisation should be identified. These risks should be assessed and the unacceptable risks for the organisation and the occurrence scenarios (modus operandi) leading to these risks should be determined. If the risks can be correctly determined in this way, they can be addressed with the right solutions unidentifiable risks are an uncertainty for the organisation. SSRA is, in a sense, an attempt to address the security uncertainties of an organisation. In this day and age where we live in a world where technology is evolving at a rapid pace and competition is reshaping itself, the stress that uncertainty imposes on organisations is quite high. Uncertainty, which has chaotic and complex consequences, is something that organisations need to pay attention to and put an end to.

SSRA is the most important tool that is a prerequisite for security solutions to eliminate uncertainty and corporate stress related to security practises.

At this point, it is beneficial to clarify what corporate stress is and what its impact is.


Securitas

a. Corporate stress

Stress is the effect of an event or situation on individuals and/or organisations. In other words, stress is a general reaction to various environmental factors. Stress is an attempt to adapt to material and mental threats.

Just like individuals, organisations develop a range of responses to situations and events to which they are in or may be exposed. Factors that lead the organisation to behave differently than its routine behavior can be considered corporate risk factors. Stress does not only have negative effects for both individuals and organisations, but also positive, motivating effects. Moderate stress has a motivating, success-enhancing effect. Corporate stress in our security practice context refers to stress that has a devastating effect on the organisation.

Under the impression that the organisation's brand value, assets, employee safety and stakeholders are threatened, corporate stress can also cause the organisation to move away from its expected and intended functions.

Decisions made at critical crossroads can cause one to deviate from one's strategies and direct resources to wrong areas. Some of the negative effects of the concept of corporate stress on the business processes of organisations are as follows;

Corporate stress leads to a discrepancy between planned activities and those that actually take place, which often has a negative impact on the organisation.

— Harming communication,
— Reducing performance,
— High employee turnover,
— Wrong strategic decisions.

All of these can affect the business continuity of the organisation or reduce its profitability and efficiency.

It is important to be aware of the security risks that may threaten the organisation, to recognise the organisation's risk appetite, and to make security adjustments as part of the security practises.

This awareness will minimise security breaches or stress due to uncertainty. Within the risk appetite, acceptable risks are known and solutions are defined for unacceptable risks.

b. The Risk Appetite of Organisations

Risk is a concept that is of great importance to all corporate activities today. To survive, businesses and organisations need to produce goods and services and mitigate the risks that arise or could arise in their processes. Risk management is a form of management that enables organisations to continue their activities by maintaining efficiency and carrying on with their daily operations while protecting their valuable tangible and intangible assets such as lives, goods, reputation, know-how, and experience.

Risk management ensures that unwanted losses are avoided easily, quickly, and at the lowest cost. To avoid losses, businesses need to develop various optimal solutions. Risks vary according to the frequency of realisation and its impact, the industry, the location, the number of employees, and the workload of each organisation.

Although the risks may appear similar for different organisations, the consequences of the risks may be different. In this regard, organisations need to prioritise the risks taking into account their mission, policies, objectives, organisational structure, the industry in which they operate, and the size of the organisation, and try to develop solutions accordingly.

As said, the risks faced by each organisation are different, as is the level of acceptance of these risks. Therefore, the

solutions to these risks may also be different. The level of acceptance is referred to as risk appetite.

Risk appetite is the level of risk that the organisation is willing to accept.

It is unrealistic and unreasonable for an organisation to survive without taking risks and being completely risk-free. Every organisation has to accept a certain level of risk in carrying out its activities. However, the risks and the severity of risks that can be accepted may vary from organisation to organisation. Therefore, the risk appetite of each organisation is different.

Organisations need to prioritise the risks taking into account their mission, policies, objectives, organisational structure and size, the industry in which they operate and try to develop solutions accordingly.

Efficiency aims to achieve ideal results by perfectly planning the use of available resources in terms of time and place in the production of desired goods and services, using the most rational means and methods. This approach is the principle of evaluating resource needs, scaling efficiency, and creating solutions in terms of the size of the loss when the risk occurs. In this approach, the organisation's risk appetite is one of the parameters that represent the threshold for the decision to adopt a security solution.

In addition to the principle of efficiency, another concept that influences the risk appetite of organisations is the principle of security effectiveness. Risk appetite, which is determined by the organisation within the context of the conditions in which it finds itself, requires a balance between effectiveness and efficiency in the security structure.

Some organisations, because of their location, their industry, the nature of their production, their corporate risks, and their corporate strategies, require a more secure facility and a corporate perception. The need to create a 'safer corporate perception" requires increased effectiveness in the security

structure. In some cases, this effort may exceed the limits of efficiency.

In certain cases where such a need exists and the level of risk is high, such that an effective security facility and a highly effective security perception with a deterrent effect are imperative, the risk appetite of the organisation concerned would remain low. This means that risk appetite is limited. For organisations that are sensitive in this way, the need for an effective security structure that goes beyond the limits of efficiency comes to the fore.

In order to implement the business strategy and manage the organisation's resources optimally, it is of great importance to know the organisation's risk appetite.

It is possible to achieve the highest efficiency when resources are used in accordance with corporate strategy and risk appetite. Knowing the risk appetite, creates a balance between unrealistic courage and excessive caution in the corporate strategy. This prevents resources from being used to minimise acceptable risks to the organisation when there is no need for action. This balance plays an important role in the stability and efficiency of the organisation.

The decision-making processes of corporate managers who are unaware of their risk appetite can have consequences, such as missing opportunities at the strategic level that would have allowed the organisation to grow because they are too cautious, or using resources that are not necessary for areas of acceptable risk. At the same time, risks that can impact the business at a strategic level and risks that are accepted without thoroughly assessing the impact can lead to dramatic deteriorations in business processes that have a greater impact than expected.

Organisations that determine and know their own risks and manage to keep them at the level of their risk appetite form an 'adequate security - hence security solutions' for an uncertain and unforeseen future.

Corporate management's knowledge of risk appetite will help:
- ***Structure risk-based budgets properly,***
- ***Control the risk exposure,***
- ***Proper process approvals,***
- ***Ensure business continuity,***
- ***Make transparent decisions.***

Identifying risks, classifying them, and developing security solutions is a process that should be carried out by taking into account the specific circumstances of each organisation.

For example, the security risks of a petrochemical plant site are different from those of an e-commerce warehouse. The risks and risk appetite of two petrochemical plants site may also be different. For example, while the risk of theft and terrorist attacks may be an unacceptable risk for one plant, the risk of terrorist attacks may be an unacceptable risk for the other plant, while theft may be considered as an acceptable risk. According to this information, the risk appetite of one plant is lower than that of the other.

c. Holistic Risk Approach

In order to determine an organisation's risks accurately, their frequency, and impact, it is extremely important to look at the risks as a whole and consider the following points:

- The interaction of security vulnerabilities with each other,
- The frequency with which the risks materialise and the consequences when they do,
- Consideration of industry-specific risk distribution and risk history,
- The impact of current technological developments on the potential risks to the organisation.

Consideration of the above is particularly important to accurately determine the risks and the frequency and potential impact of those risks. This approach can also have a direct impact on the organisation's risk appetite and potential security investments.

Although some risks may be acceptable on their own, they can become unacceptable when combined with other acceptable risks. Therefore, when assessing the risks of an organisation, possible interactions of the risks with each other should also be taken into account.

(1) Risk Interaction

It should be considered whether one security risk is a trigger for another risk or whether a vulnerability of low severity in combination with another vulnerability can pose a very high risk. For example, in a facility with 150 perimeter security cameras, it may be considered an acceptable vulnerability

if the image quality of one of the cameras is poor and the view angle is not appropriate. Similarly, it may be considered an acceptable vulnerability that one of the emergency exit doors of the building in that facility is defective and allows uncontrolled access. However, when these two security vulnerabilities are combined, it can pave the way for actions such as theft and sabotage that pose an unacceptable risk to the facility. The “risk of trespass’ which is an acceptable risk from the area where the perimeter image of the property is inadequate may be acceptable to an organisation in itself. However, the risk of trespassing on this property, combined with access to the administration building and executive floor through the defective emergency exit door, may pave the way for significant risks such as “theft”, “sabotage” or “public disorder” that would not be acceptable for the organisation.

When assessing the risks of organisations, they should therefore be evaluated from a holistic perspective;

- The impact of potential risks on each other,
- The interaction of different scenarios with each other that would form the basis for risks to occur,
- The possibility of security breaches triggering each other or amplifying their effects,

need to be considered and known to enable more accurate risk assessment and development of security solutions.

This shows that;

Determining security measures based on organisations’ risk appetite and budget is a more complex, multi-layered, and systematic approach than simply listing, ranking, and implementing measures.

Another aspect to consider in a holistic approach to risk is the impact of technology on businesses.

(2) Impact of Technology On Security Risks

The rapid change and transformation of today’s technological world also have a direct impact on security practices.

Every technological innovation opens up new opportunities for businesses in designing their security structure but also poses new security risks or an exponential increase in the potential impact of existing risks. For this reason, Securitas, when developing security services, should closely monitor developments in technologies. The impact of technology on potential risks and the possibility of incorporating technology into solutions should always be considered.

For example, sabotage is an extremely significant risk with a high potential for damage to industrial facilities and especially to the defense industry. Today, the possibility of sabotage by drones has been added to the risk scenarios (modus operandi). In view of these developments, the technological solutions that would help reduce the risks and their impact must be considered holistically. Raising public awareness on the use of such technologies and solutions in line with relevant legislation is one of the most important aspects of this issue.

What would be the tasks of Securitas from this perspective?

In order to realise corporate strategies and objectives, managers seek the advice and guidance of Securitas security professionals to;

- Determine the Organisation's risk appetite (defining acceptable and unacceptable risks),
- Decide whether efficiency or effectiveness should be prioritised or balanced in structuring the security service,
- Determine the primary and necessary investments for the security needs.

The basis of this consulting and advisory activity to be carried out by Securitas and Securitas professionals is risk analysis.

In this context, to perform a risk analysis;

— Identification of risks,
— Determination of the organisation's risk appetite,
— Holistic consideration of risks and taking into account the influence of technology in the risk assessment,
— Prioritization of risks,
— Planning the organisation's security budget to eliminate or minimize unacceptable risks within the scope of risk appetite,
— Determination of the most appropriate solution for the organisation's resources, strategy, and business plans and ensuring consensus among stakeholders,
— Implementation of the security solutions,
— Implementation of Follow-up and control measures.

It is also important that the risk analysis is repeated in these different steps on the right basis to obtain accurate results continuously:

— During the structuring phase of the security service,
— When a structural change occurs in the organisation and or its environment,
— When an incident occurs,
— At planned intervals.

d. Modus Operandi (Scenario)

Security Service Risk analysis is the measurement of the probability and possible impact of an undesired event.

Security Service Risk Analysis (SSRA) identifies the risks such as fire, robbery, or sabotage and considers the modus operandi - how the risk materialises (scenario). Solutions are based on Modus Operandi.

A Modus Operandi (scenario) should answer three basic questions:

— Where?
— When?
— How?

For example, in defining an attempted robbery of a shop (risk=robbery), the following questions must be answered to create the solution:

Where? - Through the main entrance door,
When? - At night,
How? - By breaking the door lock.

SSRA is carried out in two steps.
These are:

— Analysis of risk realisation scenarios - the modus operandi,
— Identification of the risk as a result of the interaction between the probability of an event and its impact, i.e. the extent of the costs/damages it will cause.

Conducting the risk assessment using specific tools or systems;

Allows the organisation to benefit from the knowledge and experience it has accumulated over the years and to carry out a risk assessment of all using the same standard approach. In addition, the use of these systems makes the analysis and reporting of results more efficient.

SST (Securitas Solutions Tool) used by Securitas is a tool that enables risk assessment followed by the recommendation of a number of appropriate solutions.

For example, the SST (Securitas Solutions Tool) used by Securitas is a tool that enables risk assessment followed by the recommendation of a number of appropriate solutions.

SSRA is an essential process that must be carried out in order to create customised solutions in the next step. The information gained through CSA is used in conducting SSRA. The next step is to develop tailored security solutions for each identified risk.

e. Risk Matrix:

Solutions need to be developed to meet the organisation's primary risks. For this purpose, the creation of a risk matrix that facilitates the identification of primary risks is vital. The following steps should be taken to create the risk matrix.

1. SSRA is based on the site category and the industry specified in the CSA.
2. SST (Securitas Solutions Tool) is used to develop organisation -specific solutions based on industry- specific risks.
3. SSRA must be prepared for each site where security services are provided. These sites shall be assessed for potential risks by the security professional with the assistance of the guide provided by the organisation.
4. If due to changes or new developments at the site there are risks other than those indicated by the organisation, these shall also be included in the assessment.
5. SSRA shall be carried out in the following sequence:
    i. The risk(s) is identified.
    ii. Probability and impact coefficients are determined for each risk.
    iii. The scenarios for each risk are determined.
    iv. The probability and impact coefficients determined for each risk are multiplied to determine a risk coefficient a numeric presentation of the severity magnitude.
    v. A risk matrix is prepared for the facility.

6. The areas that make up the site (entrance, common areas, stairs, parking, etc.) are assessed. The risks that can occur in each area (robbery, fire, trespassing, etc.) are determined and probability and impact coefficients are calculated for each risk. The probability levels are respectively low (1), medium (2), high (3), and very high (4).
    i. A low (1) probability corresponds to an occurrence of once or less in 10 years,
    ii. A medium (2) probability corresponds to an occurrence of once in recent years,
    iii. A high (3) probability corresponds to an occurrence of at least once per year,
    iv. A very high (4) probability corresponds to an occurrence of at least once per month.
7. It may be that the facility to be protected was recently built. In such a case, it is more appropriate to use the historical risk average based on the segment and site category and calculate the risk probabilities for the newly built facility.
8. While the impact of each risk (damage caused if it occurs) is determined, the impact is classified as low (1), medium (2), high (3), or very high (4).
    i. Low impact (damage); minor injuries, minor financial losses, and temporary production interruptions.
    ii. Moderate impacts correspond to; partial reduction in service quality, injuries, high recovery/repair costs and other financial losses, and limited service delivery.
    iii. High impact corresponds to; a permanent reduction in service quality, significant and numerous injuries, and large financial losses.

iv. Very high impact corresponds to; reputational damage, fatal accidents, and events, very high financial losses, significant disruptions, and interruptions in service delivery.

After determining the probability and impact coefficients for each risk, Securitas and the client agree on the risks that should not be accepted.

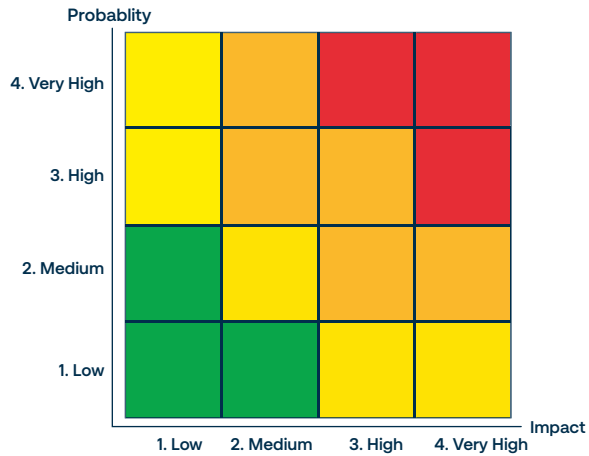


Table 1. The risk is sorted by severity rating.

Colour	Risk Coefficient	Risk Impact
Green	1-2	Low
Yellow	3-4	Medium
Orange	6-9	High
Red	12-16	Very High

Risk Level	Risks**	Risk Probability	Risk Impact	Risk Coefficient	Areas*
Very High	Risk A	4	4	16	Area 1
High	Risk B	3	3	9	Area 2
	Risk C			9	Area 3
	Risk D			9	Area 3
Medium	Risk E			4	Area 1
	Risk F			4	Area 3
Low	Risk G			1	Area 4
	Risk H			1	Area 2

9. Then the “scenarios” of where, when, and how the risk may occur are explained for each unacceptable risk. The scenarios may vary depending on organisation and site-specific variables.
10. It is also necessary to determine whether a security measure has already been taken for risk to understand possible risks that may be overlooked. Photographs are taken of the places where the risk could occur, and additional notes are added if needed.
11. In defining the risk at the end of these procedures, a risk coefficient is determined and a risk matrix is created for the facility by multiplying the probability value and the impact value determined for each risk. In the risk matrix created, risks with a risk coefficient of 2 and lower are classified as low-risk risks, risks corresponding to risk coefficients 3 and 4 are classified as medium-risk risks, risks with a risk coefficient of 6, 8, and 9 are classified as high-impact risks, and risks with risk coefficients of 12 and 16 are classified as very high-impact risks.

Risk Analysis Steps			Development of Solutions
1. Step	Determination of Segment and Service Location	Determining the segment and type of service location will give an idea not only about the facility in question, but also what kind of risks occur in that type of facility, and the impact of these risks. (In Securitas, this information and risk history for the segment / service location comes automatically.)	For each possible scenario, a solution that can completely prevent that scenario of minimize tis effect is determined. When determining the solutions, a hierarchy is followed from the least costly to the higher cost.
2. Step	Detection of Areas	Areas of the site are detected. For example, form the outside of the facility to the interior; The external environment can be divided into areas such as the main guardhouse, emergency, exit corridors, CCTV room, common areas. Naming the areas with the names used in the facility will facilitate the description and understanding.	
3. Step	Identification of Risks	Area – specific risks are determined among the risks in the risk list. There may be more than one risk in an area. Each risk is handled separately. When determining risks, previous events in the facility and the segment of the facility are taken into account.	
4. Step	Determination of Probability and Effects of Risks	For each risk identified in each area, the probability of its occurrence and the effect it will cause when it occurs are determined. A 4-factor risk matrix is used for probability and impact. A value from 1 to 4 is set for probability and effect. Facility history and segment history are taken into account when determining this value.	
5. Step	Creating Risk Matrix	Each risk for the entire facility is placed in the risk matrix according to its probability and impact value. In Securitas Smart Risk Analysis, the risk matrix is created automatically. Accordingly, the risk matrix of the facility that is, the risk map is determined.	
6. Step	Identifying Scenarios	Modus operandi, that is scenarios, which express how each risk in every field will be realized, are determined. There may be more than one scenario for a risk. In this case, each scenario month is specified separately. For example, the risk for “office space” is “theft” scenario-1 stealing valuable documents from the safe, scenario -2 stealing computers from the office, etc.	

Securitas Security Methodology
Step Three:

Solutions

3. Solutions

a. General Principles

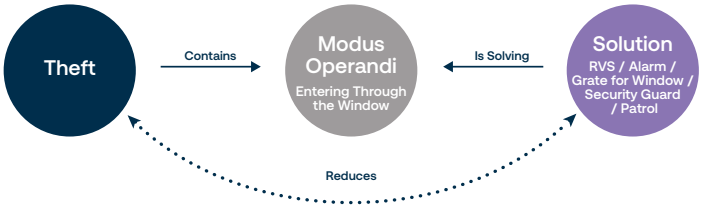
In the previous phases, the client's security needs were understood, and her current risks were analysed. Based on the SSRA, a security solution is devised to mitigate individual risks. At Securitas, the simple approach to developing security solutions is to develop a solution that mitigates the risks at optimal cost.

The optimal solution is the one that meets the organisation's security needs more effectively, efficiently and economically

Securitas' solution approach plays an important role in gaining a competitive advantage over its competitors in the market. Building security by integrating protective services such as technology-based remote, mobile, and or static guarding. When developing integrated security solutions, the optimal solution is the one that meets the organisation's security needs more effectively, efficiently and economically. Securitas' goal is to achieve cost benefits as much as possible by optimising integrated security solutions while increasing the efficiency of the security service in the organisation.

At the end of the risk assessment process, the aim is to eliminate or mitigate the impact of the risks classified and defined for each site with the help of security solutions. This approach is illustrated in the following figure.

The risk is theft through a break-in of a window. The solution developed may include the installation of a camera with video analysis, the installation of an alarm system, a window protection film, the appointment of a security officer, or the deployment of a mobile team. All or some of these measures, based on the risk coefficient, will accurately reduce the occurrence of the risk.



The approach that should be taken in developing security solutions is to provide optimal deterrents to eliminate and/or mitigate risk, but, if a risk is realised, to detect, verify, delay and intervene appropriately to the incident.

For example, posting signs to indicate 24/7 surveillance with security cameras and visibly placing cameras is a preventive measure to deter theft. But in case of an attempt, the detection of movements and verification of the images resulting from an alarm are as said detection and verification, and the remote acoustic intervention followed by the deployment of mobile patrol officers is called intervention.

b. Optimisation:

Among the risks identified and scaled during the creation of the solution, priority is given to mitigating the main risks of the organisation that have the highest probability of occurrence and the greatest impact. The optimisation to be achieved in this way consists of implementing a solution that is sufficient to eliminate the risk at the lowest possible cost.

In this context, the following should be considered.

1. A specific order of priority is followed in developing solutions to each risk. Efforts to eliminate or reduce the impact of risk according to this order of priority also serve to ensure that the organisation's resources are properly deployed. This order is also referred to as the risk mitigation plan.

The solutions to be developed aim to completely eliminate or limit the impact of risks and optimised in such a way that the resources of the organisation are used effectively.

2. The first step is to ensure that the security solutions planned are sufficient enough to mitigate the risk. Then an optimisation approach is used starting from the less costly to the more costly solutions to manage the risk. If the low-cost protective measure is deemed insufficient to manage the risk, then further other protective services are evaluated additionally.

The cost/benefit hierarchy of measures is as follows;

Detailed and carefully applied instructions and rules have a preventive, restrictive and deterrent effect on risks.

(1) Procedures & Rules:

The most basic deterrent measures for organisations are to establish rules, communicate those rules to staff and visitors, and ensure that those rules are followed. The rules of the organisation are established to reduce potential risks by eliminating the modus operandi. Establishing and following rules are the least costly - even free - measures.

For example, office windows left open for ventilation during the day become a security risk after office hours. Putting iron bars on these windows is a physical precaution. However, instructing the office staff to close the windows when leaving the office rooms and the security team to check these windows as soon as working hours are over and strictly enforcing this instruction is also an effective measure. This measure reduces the likelihood and impact of risks such as ‘burglary and/or theft’ associated with the ‘open window burglary’ scenario. This regular security check also has a deterrent effect on many security risks. Therefore, if a risk can be eliminated by establishing a procedure or a rule and ensuring compliance with that rule, this implementation is the optimal solution for that risk.

(2) Take Physical Precautions:

Depending on the rules established, some physical measures may be required. To avoid some risks, it may be necessary to support the procedures and rules with physical measures. Walls and/or wire fences, doors with different features, locks, windows that are difficult to crack, etc. are some examples of physical measures. Such equipment and materials used for physical measures have a long life span, are harder to damage, and have a longer depreciation period. Therefore, their annual/monthly cost is quite low.

(3) Using Technological Solutions:

After physical measures, card or biometric access control systems are used for access control, detectors (gas, motion, fire, etc.), or cameras with analytics for detection. These technological solutions also have a long service life. Depending on the technology, alarm systems and detectors can work efficiently for up to ten years.

Technological solutions are tools that contribute significantly to the efficiency of an organisation.

(4) Remote Monitoring:

The above technologies enable detection and verification and intervention by sending signals and information to remote monitoring centers. Operators can verify the threat by interpreting signals from alarms or images from cameras, and they can intervene remotely via devices if appropriate technologies are available. Technologies for remote monitoring and intervention when needed are a less costly solution than permanent security guards in the facility. Moreover, they are solutions and systems that contribute significantly to increasing the effectiveness of corporate security.

(5) Provision of Mobile Patrols:

Depending on the risk and the measures taken, a patrol in the facility or in the region for on-site verification can both check the incoming signals in connection with the remote monitoring centres and intervene depending on the competence, training, and equipment. As this measure requires human resources, it is more costly than the previous measures, but less costly than a permanent guard service. The risk and the intervention method may make these measures necessary.

(6) Assign a Permanent Security Officer:

Even if some or all of the above measures are taken, depending on the risk and the intervention plan, it may be necessary to appoint a permanent security officer. A permanent security officer may be necessary for assessing different and more complex situations, communicating with people, and responding faster. Assigning a permanent security officer can be costly and sometimes less consistent due to human nature.

All the above together is a methodological approach for optimising solutions.

— Solution optimisation involves identifying solution packages based on the most cost-effective and appropriate solution components in order to use the organisation's resources as effectively as possible. In this approach, permanent guarding is the last and final choice. This is because permanent guarding is one of the most costly solution methods due to ongoing labour costs, financial commitments, and administrative and operational requirements. Physical solutions such as barriers, traps, and wire fences cost less than technical solutions such as cameras and alarm systems. These products

also incur installation, depreciation, and maintenance costs over a period of time that varies depending on the product. If a risk can be addressed with a change in procedures and rules, the best solution would be to choose this alternative instead of using physical, technical products and systems or security officers. This is because changing procedures and rules is the most cost-effective solution.

— Optimisation aims not only to reduce costs but also to try to mitigate risk at the lowest possible cost. This may in some cases require the use of more than one set of measures, putting together is the solution.
— In the optimisation process, effective and low-cost solution tools are first included in the risk mitigation plan. Depending on the risk coefficient, several measures may be applied together to improve risk reduction. Therefore, an old-school approach that only proposes permanent guarding and physical measures may not be an optimal solution, while technology and remote services can help to create optimised solutions with changes in procedures.
— When the long-term (e.g. five-year) costs of the measures are shared with the client, it becomes clear how and which risks are reduced at what cost. As the costs of the proposed measures become clearer, the organisations risk appetite may increase and there may be a tendency to take more risks rather than make the initial investment. During this decision-making process, the cost of the abandoned solution and the potential cost of the risk that may occur depending on the abandonment of that solution must be estimated.
— By the time this process is completed, the unacceptable risks originally envisaged may have changed, so the parties need to agree in writing on which risks will

be eliminated or mitigated and by what means. This step is followed by the implementation of the solution.

The solution developed for each scenario must be highly deterrent, allowing early detection, having clear verification, sufficient delay, and correct intervention.

c. Hierarchy of Solutions

One of the main purposes of private security services is to prevent an undesirable event before it occurs, in order to deter malicious individuals through the perception of the safe space created. However, in cases where deterrence efforts are not sufficient and an incident occurs, it is necessary to progressively detect, verify, delay, and intervene.

The compliant and correct execution of all these activities are essential for;

- Ensuring that officers fulfill their duties and responsibilities as stipulated in the relevant legislation,
- Protecting the lives and property of people properly on the site,
- Ensuring the safety of the security team,
- Maintaining the confidence of the clients,
- Protecting the reputation of the organisation.

In order to prevent the occurrence of a security risk and to intervene as effectively as possible, the following steps exist;

1. Deterrence
2. Detection
3. Verification
4. Delay
5. Intervention

(1) Deterrence

"Deterrence" in the context of security practises means deterring malicious persons from their actions without the need to use force or intervention. The measures taken and the perception of the safe space created are intended to convince potential threats that their potential behavior will have consequences and that it is better not to behave maliciously. In this context, every security measure is a part of the deterrence effort. No thief wants to break into a facility that provides a strong perception of security, to steal something.

When evaluated on the axis of costs and benefits, the most desirable outcome is to deter malicious individuals from their activities before they take action.

Methods of deterrence in this context include, for example, the following;

- Implementing security measures in accordance with instructions and procedures, etc.
- Posting signs "This facility is monitored 24/7 with security cameras",
- Not leaving any open and accessible material in the facility,
- Physical obstruction systems,
- Security cameras and alarm systems,
- Conducting patrols with security officers,
- Hiring of permanent security guards.

Taking measures to deter malicious persons before a risk materialises is the most effective and cost-efficient practice.

(2) Detection

In cases where deterrence is not enough, individuals who pose a threat attempt their malicious activities.

For instance, in the area with exposed scrap metal where copper cable drums are visible from the outside, malicious persons will want to enter the factory for theft if it does not have adequate physical barriers. The risk of theft in this plant is "likely" and the "impact" will be high when it occurs. This is where initial deterrent measures need to be taken. The first measure to be taken is to move the copper coils from the outside storage to the inside storage, strengthen physical measures, improve lighting, and set up a detection system with cameras and alarms.

Sometimes security vulnerabilities become a security risk due to the influence of external factors. For example, in warehouses where flammable materials are stored, fires can be started by cigarette butts, glass, and sunlight. The first step can be to interrupt the chain reaction by restricting smoking in the area and ensuring good cleaning. In addition, fire detection systems should be installed in case a fire breaks out. In this case, the fire detection system is an important and necessary measure. Early detection of such situations is crucial, and the ability to detect them depends on the presence of appropriate systems in the facility. Detection is the first step toward effective intervention.

Any threat and/or vulnerability that is not detected in time will lead to an increase in damage.

Accurate and effective operation of detection systems is the first and most important step in threat detection. For example, if cameras with motion-detecting video analytics systems at the perimeter of a facility generate too many false alarms, after a while no alarm will be verified. This is equivalent to not having a detection system. When an alarm is detected, it must be verified that it is a real threat.

(3) Verification

Verification of an incident that has occurred is important to respond to the event in a timely manner with the correct methods.

> ***Verification from important to understand the incident and its magnitude and to determine the appropriate team and course of action.***

If verification is delayed or not done correctly, the incident can deteriorate quickly and dramatically. To understand the incident, verification from all possible sources is a must. For example, if an alarm is received from the external alarm system (EAS) at an outer boundary line, visual confirmation must be obtained from the cameras covering the area and information from the security team working near the area. Similarly, fire alarms coming from a fire detection system must be verified by the cameras covering the area and by officers located at nearby posts.

> ***Verification by multiple sources ensures that the event is understood as accurately as possible. The accurate verification of the incidence ensures the safety of the response team and the plan and scope of the intervention.***

Depending on the type and size of the event, the right intervention officer/team should be deployed. Misdirection by security managers or security dispatchers can lead to troubling incidents that negatively impact the course of the event, damage the organisation's reputation, and result in loss of property or life. For example, a fire detected by the fire alarm system should be verified by the cameras monitoring that area, confirmed by officers at nearby posts, and more importantly, directing the firefighters or officers that are trained in firefighting to the scene. Otherwise, incorrect intervention, action inappropriate to the nature of the fire, or ignorance of the correct procedures by those involved in the incident may result in the spreading of the fire further and even potentially threatening lives.

Briefing the intervention officer/response team according to the nature and extent of the incident immediately after verification is essential to minimise potential casualties and bring the incident under control quickly.

After the verification of an incident, the security team often needs some time to intervene. The threat needs to be slowed down, delayed, to allow time to intervene.

(4) Delay

When developing solutions to eliminate risks or mitigate their effects, the "solution" should include detection, verification, delay and intervention. In other words,

Solutions must be time-saving for the verification and the physical intervention of the security team. and intervention. This is because a certain amount of time is required from the detection and verification phase to the intervention of the response teams.

At this point, the measures taken should be able to prevent the current situation from worsening until the intervention takes place.

This means that the time between detection and intervention is supplemented by measures appropriate to the nature of the risk. This is because a certain amount of time elapses between the time when the risk is first detected and verified by various means and the time when the first responders intervene in the incident. During this time, additional measures should be taken to prevent the damage from escalating. The analysis of the realisation scenario (modus operandi) must include how the course of an incident would develop and how much time is needed for intervention.

The solution developed for each Modus Operandi (scenario) must be highly deterrent allowing early detection, clear verification, sufficient delay, and correct intervention.

The risk of "trespassing on a property" can occur in many scenarios. In this example, we assume that this risk arises through the emergency exit door. To avoid this risk through this scenario, the solution should provide detection, verification, delay as well as intervention. Once the above risk is verified, time is needed to intervene. The security measures should be enough to delay the threatening element in time to intervene.

In the designed solution, a magnetic contact on the door is connected to an alarm system, a camera and a loudspeaker are connected to the remote monitoring room and a mobile patrolling team is nearby. When an intruder walks through the door, the magnetic contact detects the wing of the door is separated from its casing and alerts the monitoring room, the intrusion is verified by the camera, and the first intervention is made by the operator in the remote monitoring center who uses the loudspeaker and tries to delay further activities of the intruder, and time is bought for the intervention of the mobile officers.

Another example, after a fire is detected and verified, it takes a while for the firefighting team or fire brigade to be called to action. Fire is a disaster that grows very quickly in the first few minutes. The spread and growth of the fire must be delayed until fire extinguishing intervention. The use of fire-resistant materials such as paint, doors, and automatic ventilation locks saves time and slows the spread of the fire. The use of sprinklers or FM200 systems is both an intervention and a suppression system to delay the expansion of the fire before the intervention of the fire brigade.

(5) Intervention

Incidents can damage physical property as well as all those involved in the facility, and the brand value of the organisation. The focus of intervention is to respond and recover as quickly as possible to minimise the impact of the incident on facilities and stakeholders. The more accurately and effectively the preparation time for the intervention is managed with the necessary training and practice, the more likely it is that the intervention will be on the right footing. One of the most important factors for effective and correct intervention is the level of preparation and the activities at the time of intervention.

Even a small event that is not intervened in time with a proper method can grow and cause significant damage.

During the preparation period; actions such as the following will ensure that the intervention is executed most accurately at the time of the incident.

— To identify the specific intervention methods for each possible incident,
— To develop appropriate procedures and instructions for intervention,
— To identify intervention teams for each possible incident,
— To establish the communication hierarchy,
— To consolidate the desired approach and ensure the correct response through a set of training and tests.

It is also important to conduct a further risk analysis that identifies the modus operandi of possible intervention methods and their further damage potential (risk) in advance and develop alternative intervention methods to choose the least risky one.

(6) Post-Incidence Operations

After an intervention, the facility must quickly return to normal operations. The minutes, reports, photos, and digital logs required under the judicial, administrative, organisational and insurance requirements following the incident should be fully completed. Production or operations should resume as soon as the facility is fully prepared. Also, note that resuming operations or production before equipment and personnel are fully ready will give the impression that the emergency is causing more damage than it actually is. Therefore, before starting operation or production, checks should first be carried out according to the facility's ramp-up plans.

After the emergency;

— Documents relating to the incident, such as the minutes, reports, photos, digital logs and other official evidence should be retained.
— Camera footage of the incident must be saved/archived.
— The material that serves as evidence of the incident should be retained.
— Depending on the nature and extent of the incident, the scene should be kept as is for further investigations.

Securitas Security Methodology
Step Four:

Implementation

4. Implementation of the Security Solutions

In the event of an agreement with the client and the signing of the contract, the timely, complete, and uninterrupted introduction of the agreed security solutions constitutes the implementation phase.

The Implementation Phase itself is divided into two phases.

— Phase one, the initiation and completion of preparations,
— Phase two, the execution of the service.

After the contract has been signed with the client, the necessary preparations are made by the date promised in the contract and the security service begins. This phase is where the Securitas Service Initiation Procedure comes into play, covering all the start-up activities to make this process as correct and complete as possible.

The service initiation process is the period when the security sensitivity of the facility is at its highest. It is important that this process is carried out according to a plan so that risks are mitigated during this period.

A security service that begins with a plan and checklists minimises potential interruptions. Once the service has start-

ed, the important aspect of the service delivery process is to ensure the continuity of all promised services and to continue to add value to the client. In this context, the development and/or conversion of the existing service should be assessed in line with client needs, current requirements, and developments. In this way, the cost efficiency of the service can be continuously increased. For this reason, it is important to transfer the processes to digital platforms as much as possible.

The careful implementation of the principles for the execution of services within Securitas Security Methodology and the control of the principles through established methods help to ensure business continuity for both the client and Securitas.

Another way to add value is to strengthen the measurable, traceable and reportable aspects of the security service.


Securita
Securitas

Securitas Security Methodology
Step Five:

Quality Control

5. Quality Control

Quality control refers to the methods and tools used to verify that products or services meet established standards and requirements. Organisations that fail to take into account the needs and expectations of their stakeholders when producing products and services are doomed to lose their market share and reputation to others that meet their stakeholders' expectations. Quality control consists of the strict tracking of defined performance indicators and service levels, which includes;

— Compliance with relevant laws and regulations,
— Securitas policies and procedures,
— Client expectations,
— And the correction plans for deficiencies.

To ensure continuity of service standards, various quality control procedures are reviewed to determine whether the service is meeting contractual requirements and/or if there are issues affecting subcontracted operations. All procedures carried out in this framework are quality control activities.

The basic approach to quality control practises includes;

— Controlling periodically,
— Detecting defects,
— Creating warnings,
— Correcting the defects/faults,
— Learning lessons,

— Training,
— Improving,
— Continuing the above listed.

There are various quality control ways to achieve these goals and ensure continuity of quality service delivery. The implementation of quality control is one of the most important indicators for measuring the quality of the security service in relation to client satisfaction. The “quality control” of the security service is carried out with the following activities.

a. On-site Audits

Planned audits by quality auditors within Securitas and certified remote monitoring center operators shall be conducted in accordance with the following principles:

1. Previous audit reports related to the site need to be reviewed prior to the current audit to learn and understand the track record.
2. Site-specific, customised audit checklists must be used.
3. In the selection of subjects to be audited, priority needs to be given to subjects identified as incomplete or low-scoring topics in previous audits.
4. Risks that have been reported recently need to be reassessed and if they persist, they need to be reported again.
5. A method of objectivity needs to be used in audits.
6. In the Yes/No scoring sections of audit checklists, if “no” is selected and the options “medium”, “poor” and “very poor” are selected when scoring multiple-choice questions; the explanation sections must state the reason for selecting these answers and the actions to be taken.
7. With concurrent on-the-job training priority shall be given to the areas of improvement identified in the audit.

8. The focus of audits must be balanced between the risk on the ground and the competencies of the officers.
9. Branch managers shall review the Audit Deficiency Reports and plan the necessary actions for continuous risk mitigation.

b. Remote Audits

The Remote Audit Service is conducted through a system consisting of a camera, microphone, and loudspeaker that allows voice communication with the Securitas Operation Centre (SOC). The purpose of these audits is to verify, through authorised and trained SOC operators, that the security officers on duty are performing their duties in accordance with the post instructions.

1. Remote audit systems installed in places where security officers work, such as site monitoring rooms, entrances, gates, and checkpoints, allow two-way communication with the SOC.
2. Remote audits are carried out by SOC operators according to a standardised inspection form.
3. The audit results are automatically sent by the system via email to the relevant branch and the quality department.
4. (The authorised staff of the quality department can access the camera images and the audit results of the remote monitoring centere through the digital platforms.

c. Quality Department Audits

Another instrument of quality control is audits, which are carried out by the specialists of the quality department with the help of digital audit forms. The audits planned by the quality department take into account the SSRA-based security risks

and the corresponding solutions. The responsible branches are informed by the Quality Department coordinators before the audits are carried out.

In line with the above, any sensitivities relating to the site will be reported to the Securitas Quality Manager. Special care will be taken with further audits relating to sensitive client and contractual matters. Further audits and improvement plans will be carried out as part of this coordination.

d. Drills (Awareness Tests)

A drill (awareness test) is a test of the security service provided to the client, using a scenario to verify that the planned solutions are working.

For example, at a gate check point in an airport, the measures against forbidden items in bags and packages are tested with a scenario to see how correctly the measures are implemented.

A drill needs to be carried out with the following principles.

1. The inspection must be covert. As far as possible, the evaluation of the drill must be carried out with camera footage or other evidence.
2. The drill must test a foreseen risk and its modus operandi.
3. Full details of the drill (scenario, time, location, etc.) must be communicated in writing to the client's representative and the relevant area managers.
4. The client's representative must be fully informed in good time before the drill is carried out to avoid panic situations and misunderstandings that may arise.
5. If the drill is carried out by the branch, the planning of the use of materials and methods must be agreed upon with the client in accordance with the modus operandi.


Securitas

6. The whole drill shall be monitored in person and recorded by cameras. If it is to be observed in person, it shall be determined by whom, where, and how it will be observed and documented.
7. The drill needs to test the post-specific instructions in terms of modus operandi and may cover in scope all or any of i) Deterrence, ii) Detection, iii) Verification, iv) Delay, and v) Intervention.

   For example, if the post-specific instruction includes the following wording: "The visitor's legs including ankles, arms including armpits, and the entire front and the back of the body are scanned with an HHMD (handheld metal detector)", a drill control question can be formulated as follows: "Were the visitor's legs including ankles, arms including armpits, and the entire front and the back of the body scanned?

8. The assessment results of the drill are registered in the available digital system for further use.
9. After a failed drill, some time is needed for training and corrective action until another drill with the same scenario can be conducted.
10. Following the drill, a final meeting is held on-site, attended by Securitas staff, Securitas site manager, and the branch manager, if possible also by the client's representative. Here, what happened during the drill, what should have been done, and how it could be done better are being discussed. Based on the evaluation of this meeting, changes can be made to the operating instructions and implementation guidelines, and if there are competence gaps, further training can be planned.

e. KPI (Key Performance Indicators) Tracking

The key performance criteria relate to the issues that need to be assessed and measured.

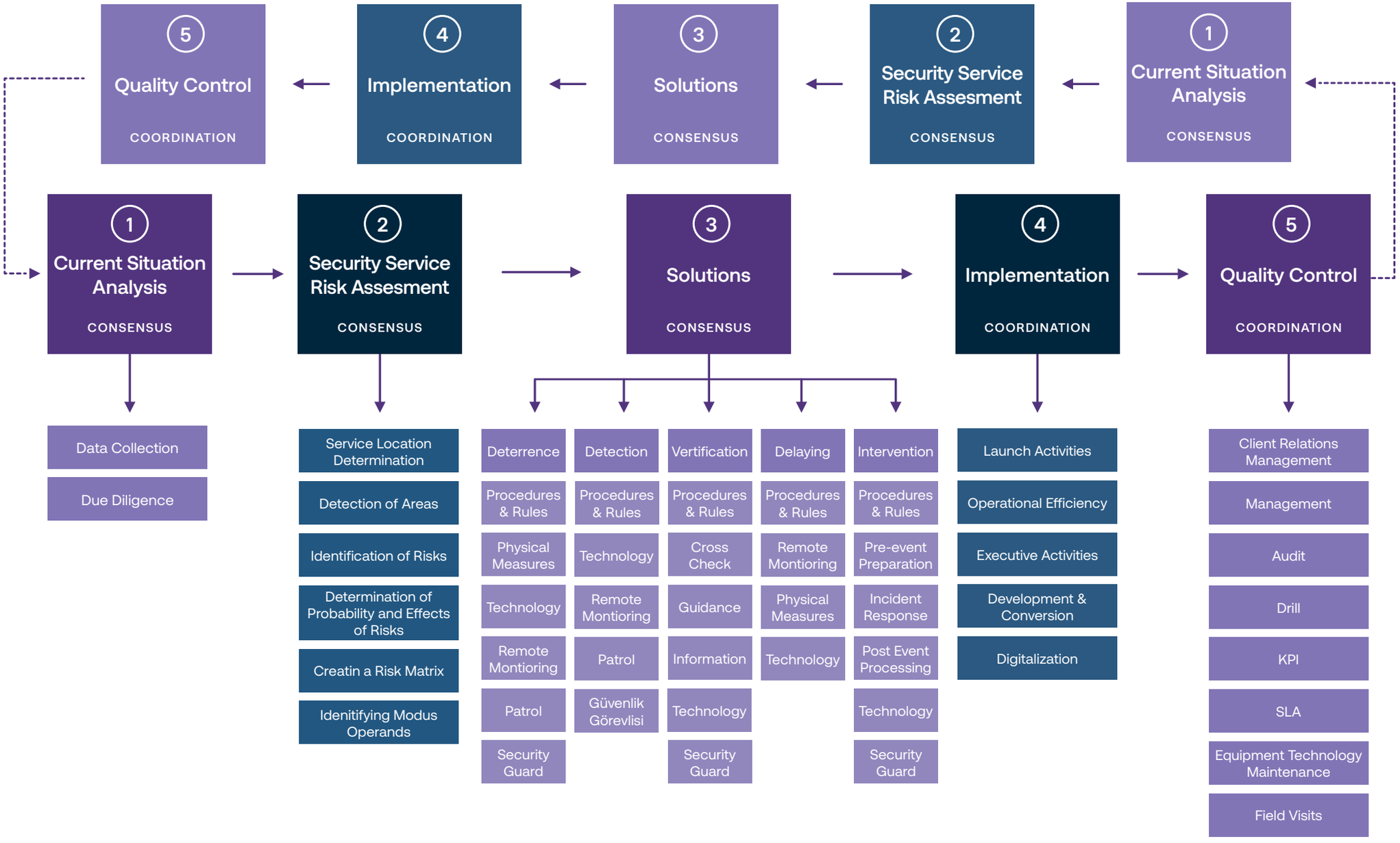
1. Branches will be assessed according to a KPI system, the principles of which determined by the Quality Department.
2. These KPI assessments are done automatically through digital platforms.
3. Branch managers are assessed using a 100-point scale based on the quality audit process. The results of this assessment are regularly communicated at the area and branch level and can be tracked on digital platforms.

Securitas Security Methodology Workflow

The Securitas Security Methodology helps Securitas deliver security services at a level of quality that exceeds client expectations.

This distinctive and holistic approach ensures that Securitas is a leader in the security market.

Securitas Security Methodology Workflow



References

- Altun, B. (2017). Kurumsal Stres Kaynakları ve Stresle Başa Çıkma: Beylikdüzü Belediyesinde Bir Uygulama (Yüksek Lisans Tezi). Göller Bölgesi Aylık Hakemli Ekonomi ve Kültür Dergisi Ayrıntı Sayı 49, 58-65.
- ARPAT, R. S. (2016). Acil Durum ve Kriz Yönetimi. Gece Kitaplığı.
- Coşkun, S. (Haziran 2018). Sosyal Bilimlerde Metodloji Problemi. Dört Öge, 13, 59-72.
- Çalışkan, F. (2021, Eylül 21). Güvenlik Uygulamaları Kapsamında “Risk İştahı” Kavramı. Linkedin: https://www.linkedin.com/in/feramuzcaliskan/ adresinden alındı
- Görmen, M. (2018). ÖRGÜT KÜLTÜRÜ İLE RİSK KÜLTÜRÜ ARASINDAKİ İLİŞKİNİN İNCELENMESİ. Balkan Sosyal Bilimler Dergisi, 121-135.
- Hopkin, P. (2017). Fundamentals of Risk Management, Understanding, Evalluating and Implementing Effective Risk Management. Newyork: Kogan Page Ltd.
- International, A. (2005). Business Continuity Guideline, A Practical Approach for Emergency Preparedness, Crisis Management and Disaster Recovery. ASIS International.
- İŞTAR, A. G. (2012). Stres ve Verimlilik İlişkisi. Akademik Bakış Dergisi.
- Kanat, E. B. (2020, Ocak 20). Metodoloji Nedir? Enstitü: https://www.iienstitu.com/blog/metodoloji-nedir adresinden alındı
- LAM, J. (2015). Implementing an Effective Risk Appetite. Montvale, NJ: The Association of Accountants and Financial Professionals in Business.
- ÖZALP, H. (2016). Özel Güvenlik Risk Yönetim Sistemi. İzmir.
- Prof Dr Handan Türkoğlu, Y. D. (2001). Acil Durum Planlaması. İstanbul: İTÜ Afet Yönetim Merkezi .
- Prof. Dr. Deniz Taşçı, Y. D. (2013). Kalite Yönetim Sistemleri. Eskişehir: Anadolu Üniversitesi.
- Ruziye COP, A. Y. (2016). DEĞER TEMELLİ PAZARLAMADA MÜŞTERİ DEĞERİNE, FİRMA VE MÜŞTERİ BAKIŞ AÇISINDAN BOLU İLİNDE BİR UYGULAMA. Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 49-80.
- Sinek, S. (2020). Neden İle Başla. İstanbul: Arıtan.
- Toker, K. (2018). Endüstri 4.0 ve Sürdürülebilirliğe Etkileri. İstanbul Management Journal, 51-64.
- ÜNVER, O. (tarih yok). Risk ve Risk Değerlendirmesi. İstanbul: GÜSOD.
- Wikipedia Metodoloji Nedir? (tarih yok). Wikipedia: https://tr.wikipedia.org/wiki/Metodoloji adresinden alındı
- Winberg, H. (2019). Yaklaşık Olarak Doğru. Ankara: Bilgi Yayınevi.
- Yrd. Doç DrFerit KÜÇÜK, Y. D. (Aralık 2007). Kurum İçi Stres Kaynaklarının Kurumsal Bağlılığa Etkisi: Şanlıurfa Belediye Örneği. Çağ Üniversitesi Sosyal Bilimler Dergisi, 66-89.

SECURITAS SECURITY METHODOLOGY

If security processes are not methodised, damage caused by overlooked risks cannot be prevented. The Securitas Security Methodology is therefore, under the guidance of ISO 31000, our risk-based, measurable way of working with a focus on business continuity.

Berti Bora
Head of Business Development & Sales

Business continuity, one of the main goals of any business, is possible by anticipating any threat that could pose a risk in the execution of their activities and taking measures to minimise the potential.

Securitas Security Methodology, created with the aim of communicating the ways and methods to be followed is an extremely useful guide for the security market.

Hüseyin Erim
Head of Security Processes and Quality

A perfect guide explaining how risk management, which is the foundation of security operations, should be handled from start to finish, detailing the steps to be taken from setting up the ideal security structure to running the security service in a sustainable manner and with defined quality standards.

Gökhan Usta
Security Processes and Quality Manager

Securitas

Securitas Türkiye publication, not sold.