

F S R

TAPA Copyright © Do Not Copy

Facility Security Requirements Guidance Document for users of TAPA Standards

CCTV Systems Guidance V 2

TAPA EMEA
Pastoor Ohllaan 39
3451 CB Vleuten
The Netherlands

www.tapaemea.org
info@tapaemea.org
Tel. +31 619 5734 61

TAPA does not represent nor warrant that the information contained in this document will prevent any loss, damage or injury to a person or property, because of burglary, theft, hold-up, fire or other cause, or that the information will in all cases provide the protection for which it is intended. If the reader chooses to use any information in this document, they assume all risk and liability for doing so.

Contents

1. Introduction 3

2. About TAPA 4

3. Facility Threats and Risk Assessment..... 5

4. CCTV/VSS Systems..... 8

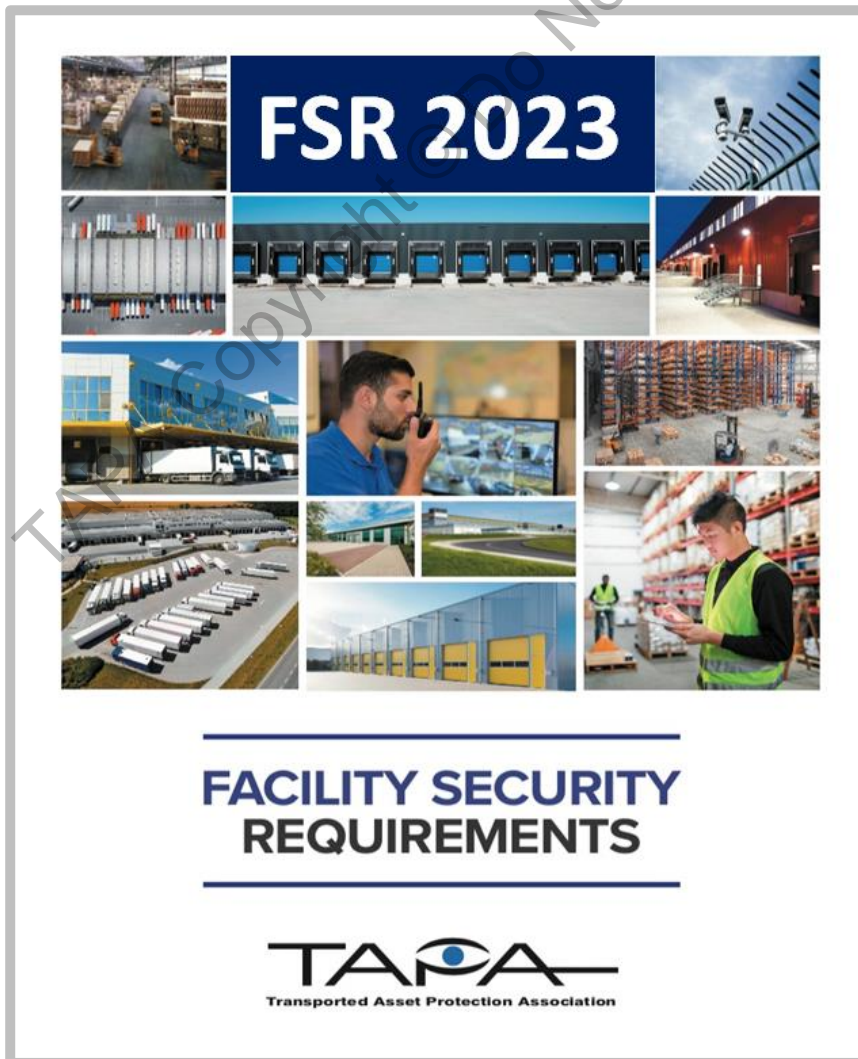
5. FSR Overview 16

6. Frequently Asked Questions..... 31

7. How to find the right CCTV/VSS solution? 39

8. Useful links..... 43

9. Appendix A: CCTV/ VSS Systems Examples 45



1. Introduction

CCTV/VSS is not only a constantly evolving arena with new innovations leading to continued product development and emerging technology, CCTV/VSS is also a recognised component of security systems deployed to protect logistics facilities against criminal activity, and as such CCTV/VSS Systems are an integral part of the TAPA Facility Security Requirements (FSR) Standard.

Closed Circuit Television (CCTV) is a system in which images are monitored and recorded for surveillance and security purposes. Though still in general use, the acronym 'CCTV' is now outdated, as this refers to the hard-wired analogue cabling approach which has generally been replaced by digital Video Surveillance Systems (VSS) that operate over TCP/IP networks (Transmission Control Protocol/Internet Protocol).

TAPA has produced this CCTV/VSS Systems Guidance (CSG) to provide helpful supporting information on CCTV/VSS systems for users of the TAPA Facility Security Requirements (FSR) Standard. To remove any confusion the 2023 FSR Standards revision refers to both CCTV/VSS terminology. In this document, the term “video surveillance” is used to describe the functionality of CCTV/VSS technology.

The purpose of this document is to:

- Provide guidance on how existing and emerging CCTV/VSS systems technology can be used to meet FSR and wider operational requirements
- Provide additional detailed information on CCTV/VSS system solutions not covered in the FSR
- Provide users with CCTV/VSS system categories that will help in the selection and identification of suitable products.
- Provide examples of CCTV/VSS systems and their intended use

TAPA acknowledges CCTV/VSS technology is an area of continued innovation and as such this document will be reviewed and updated as necessary, providing FSR users with up-to-date information on CCTV/VSS systems. The latest version will be available to download from the standards section of the TAPA website.

TAPA has included images and information on products in the CSG. These commercially available products are considered examples of products that help protect workers, facilities, and their cargoes. Other products are available. TAPA does not endorse any of the products included in this document.

TAPA cannot specify which product is appropriate for a TAPA FSR security level, as the suitability of the products relates directly to their functional specifications.

2. About TAPA

Cargo crime is one of the biggest supply chain challenges for manufacturers of valuable and high-risk products and their logistics service suppliers.

The threat is no longer only from opportunist criminals. Today, organized crime rings are operating globally and using increasingly sophisticated attacks on vehicles, premises, and personnel to achieve their aims.

TAPA is a unique forum that unites global manufacturers, logistics suppliers, freight carriers, law enforcement agencies, and other stakeholders with the common aim of reducing losses from international supply chains. TAPA's primary focus is theft prevention using real-time intelligence and the latest preventative measures.

TAPA's Mission

TAPA's mission is to help protect members' assets by minimizing cargo losses from the supply chain. TAPA achieves this through the development and application of global security standards, recognized industry practices, technology, education, benchmarking, regulatory collaboration, and the proactive identification of crime trends and supply chain security threats.



3. Facility Threats and Risk Assessment

Understanding the threat to supply chain facilities is fundamental to designing security systems and countermeasures.

TAPA acknowledges each member will have their own risk assessment process and as such TAPA is not specifying any approach but suggests areas that should be considered for inclusion.

Risk assessment

Most security practitioners will advise the use of a risk assessment process to help/select the countermeasures that can help mitigate the threat of theft to an acceptable level.

A risk assessment process should seek to understand.

- The threat faced – who, how, or what will impact the facility, its employees, and assets.
- The likelihood of an incident occurring.
- Crime Intelligence Data – Review cargo and local crime statistics available from LEAs and other local sources.
- The consequence or impact of an incident occurring.
- Impact on individuals – personal injury or mental health.
- Financial losses. Cargo value; loss of revenue.
- Supply chain disruption.

Risk assessments must be revisited annually. It should also be revisited:

- Following a change in facility usage or assets held at the facility.
- As a result of an incident.

The selection of a suitable CCTV/VSS system should be aided by the risk assessment process.

- What features/protection the CCTV/VSS system must provide.
- The consequences of the CCTV/VSS system being defeated.
- Does the CCTV/VSS system complement the measures that support the protection of the facility and assets?
- Supporting procedures that allow for incident management and emergency response.

In terms of the technical part of CCTV/VSS Systems:

- Camera field of view: Do they reflect changes to the physical/threat environment?
- Data: Does the image quality captured meet the needs and support risk reduction?
- Changes to local laws or data privacy guidelines: Is the system compliant?
- Giving each camera a job description to ensure that each camera specification is in line with the function it is required to fulfil.

Facility Threats

The threat to a facility can come from a person or group who (un-) intentionally causes harm or chooses to act with malice.

This threat can include theft, but also disruption to the facility or supply chain. Action from protesters or activist groups can have a significant impact on a facility but the measures employed to minimise the threat would be similar to that of deterring theft.

The external threats

Just as security professionals complete risk assessments to protect cargo. Criminals are also carrying out their risk assessment and hostile reconnaissance of a planned target.

Is the risk of being caught worth the potential reward?

When it comes to attacking facilities, criminals do not like to be spotted, take too long to access their target cargo, or be interrupted. In most incidents, organized criminals will have the knowledge to:

- Attack the facility when it is at its most vulnerable.
- Access the facility by defeating or avoiding the physical measures in place.
- Have a plan for neutralizing or ignoring any electronic sensors they know will be in place.
- Calculate how much time they need to complete their operation and make their escape with their targeted cargo.

The opportunist threats

Security systems and processes are subject to human error or system faults, where this occurs opportunists can take advantage of the situation and commit crimes.

Security systems and physical security measures must be maintained and tested regularly to minimise the risk .

The internal threats

Often underestimated, the insider is a person from within the Logistic Service Supplier who uses their legitimate access to commit a malicious act or provide the information required by criminals to gain access to the facility or assets.

As the insider is aware of the security measures at the facility, identification of an insider is difficult, and it is an unfortunate fact that employees' collaboration with criminals is still a common risk.

Regular audits of security system data such as access logs are important to identify misuse or trends. Scheduled changing of access pin codes and physical key audits can help deter insider activity. Procedures that control shipping information or access to the cargo are also important factors to consider in protecting the cargo from an internal threat.

Suitable and sufficient management systems

Management commitment to support security policy and procedures that enforce the mitigation options selection should be in place as standard practice.



4. CCTV/VSS Systems

The context of this section is to overview what a CCTV/VSS system is and the principal considerations of what it can do for a logistics asset. CCTV/VSS innovation has greatly advanced in recent times, and it is important to understand what the basic principles are and what they can do.

CCTV/VSS systems - Designing out the risks or: Why do we use CCTV/VSS systems in our facilities?

There are 5 main reasons for using CCTV/VSS as a security risk mitigation measure in a facility:

- To deter criminal activity such as theft
- To monitor suspicious activities (either in real-time or offline)
- To record evidence for post-incident investigations
- To keep a tab on activities and identify potential security risks
- To clarify operational, and logistical issues such as incorrect loading or similar.

CCTV/VSS systems must be designed to assist in supporting the basic security principles of deterring, detecting, delaying, respond and when used in conjunction with additional security measures such as Perimeter Protection; Lighting; Intrusion Detection, and Access Control it can provide a high level of confidence in the security design.

Poorly designed or maintained security systems will attract the attention of criminals. It is through good design and planning that a deterrent can be introduced that helps prevent or minimize the impacts of cargo loss.

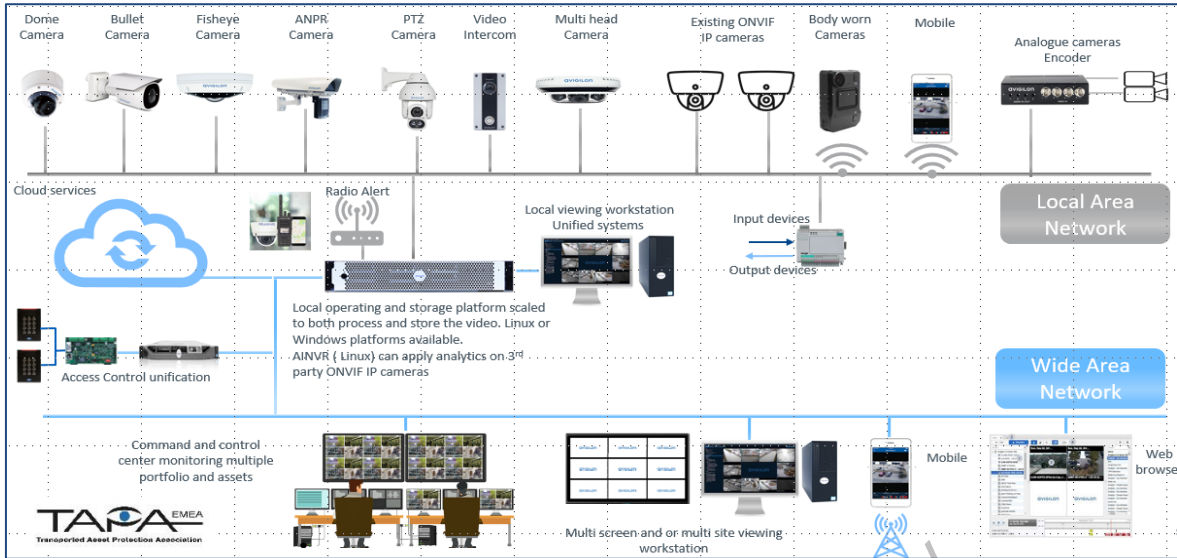
Organized criminal groups adapt and change their approach to counter any security systems they face. Reviewing risk assessments; and the effectiveness of the systems and processes deployed when completing the annual FSR audit helps stay ahead of the criminals.

What is CCTV/VSS?

In general, it's a system that allows you to keep an eye on whatever is ongoing in and around your facility. The cameras, monitors, and recording devices you have installed for such a system, will allow you to view events, live or later via the recorded footage.

Within a CCTV/VSS system, multiple sorts of cameras and other equipment can be used.

The below figure shows a sample of how a professional CCTV/VSS system can be set up. In reality, CCTV/VSS systems for logistic providers can look less complicated but with most of the same sort of elements used as cameras, recording devices, and monitoring



Camera form factors

A logistic centre is a challenging environment for cameras, considerations will include physical protection of devices, space, and access considerations or available lighting. HD Cameras are integrated units with compact profiles with a powerful MP range that doesn't need the physical size to increase to address Logistics sites' range generally.

The form factors of cameras are a variation of the key types below.

Most cameras will come with built-in IR (Infrared) options, and these should be taken in most instances to account for local lighting failure, other elements such as Wide Dynamic Range (WDR) is a consideration to ensure backlighting does not affect the image in areas of wide light change (door openings /shutter areas etc).



Analog cameras:

Have been around for years, but the overall percentage decreased in the meantime on less than 5% of Video Surveillance cameras installed today. They have basic functionality and with connectivity to NVR/DVR, they can store recordings onsite. However, the trend shows only IP cameras are becoming the only option in new installations.

IP (Internet protocol) cameras:

Carry out the same functions as their Analog counterparts, but with vastly greater capabilities. IP cameras boast sharper, higher-resolution images and more flexible features like remote zoom and repositioning. They also give you the option to view footage on a web browser or mobile device.

Cabling:

All CCTV/VSS systems require some amount of cabling, even those with wireless cameras. Cables link different pieces of equipment together, including monitors, recorders, modems, and wired cameras. When using analogue cameras, it is good practice to keep the coax cable running less than 300m and 80m or less in IP installations. The cable run can also affect the power to the camera so cable runs that are too long can cause power losses to the camera.

Video recorders:

CCTV/VSS systems store image data captured on a dedicated recording system, or in some cases hold the images on a storage device embedded within the camera itself.

Cameras can be set up to record all images captured, but this will take up a lot of storage space particularly if you are retaining data for long periods.

Cameras can also be programmed to record only during certain times of the day or when they detect movement. Video recording options include **DVR** and **NVR**.

- **DVRs**, or digital video recorders, are the modern replacement for analogue recorders that use videotapes. DVRs capture footage from analogue cameras in a digital format at the desired resolution and frames per second. When the hard disk gets full, new images will be recorded over the oldest footage first.
- **NVRs**, or network video recorders, work similarly to DVRs, but they're compatible with IP cameras. Your cameras and NVR connect via a network switch or router. You can easily access footage on an NVR through a web browser or mobile app.

Display unit:

CCTV/VSS images can be viewed on single or multiple screens depending on your requirements. If you have IP cameras, you can also view footage remotely from a smartphone or computer.

But installing a CCTV/VSS camera doesn't mean you're automatically safe; Within the FSR requirements, TAPA will explain what the performance should be from such a system to be compliant with TAPA FSR. FSR provides a minimum requirement for CCTV/VSS, so it is important to consider other operational requirements such as safety considerations within your solution design.

Deciding how you'll be monitoring the system:

If you decide to monitor your system using the Internet, getting an IP Address for your Digital Video Recorder (DVR) or NVR will equip it to survey and record easily; an Ethernet cable carries all information via the Ethernet switch.

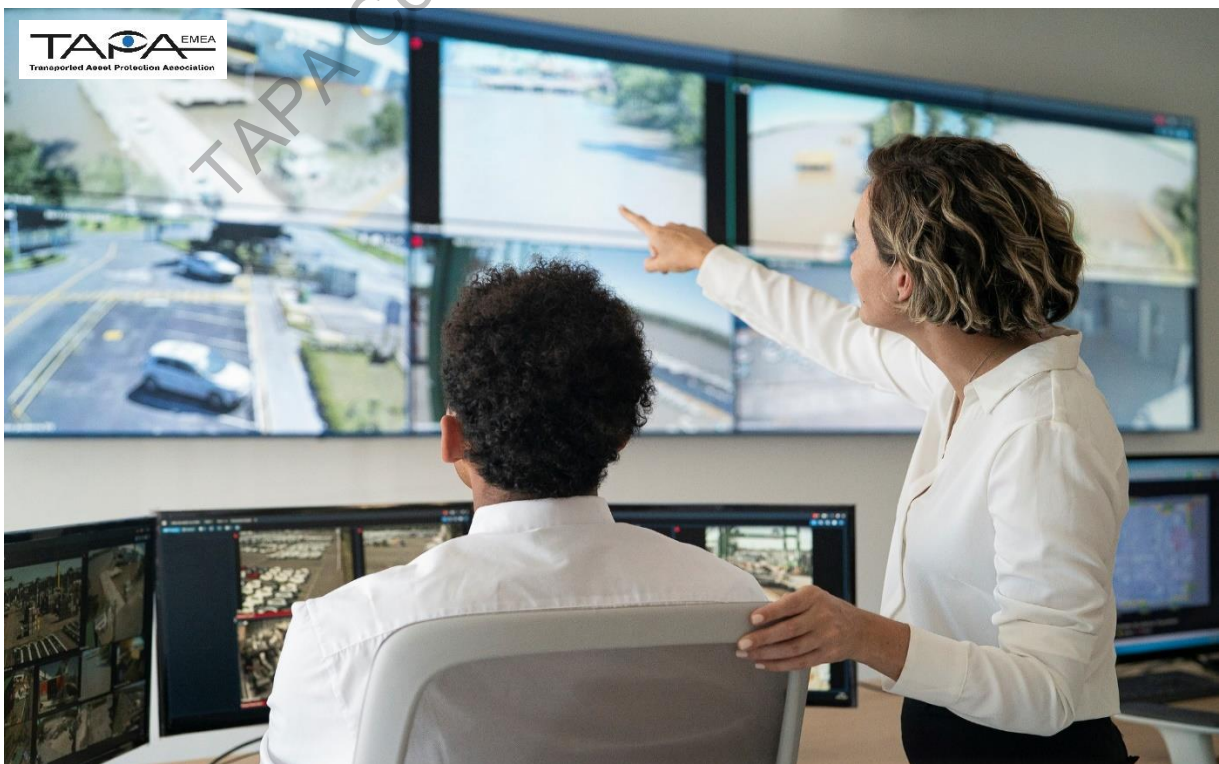
Determining the number of Cameras required:

Depending upon the nature of your requirement and the expanse of the area you want to protect, (in line with the TAPA FSR standards), decide on the number of cameras required to ensure complete security. In the FAQs section, there is an answer that might help you understand how this can be implemented.

Positioning the CCTV/VSS cameras:

TAPA FSR requirements dictate areas CCTV/VSS cameras must be present to comply with the standard however it is important to remember factors that could impact the camera and images being viewed/recorded:

- Exposure to extreme weather conditions such as rain, glare from sunlight etc.
- Glare from lighting
- Landscaping such as trees



CCTV/VSS System Protection:

It is paramount to secure the digital video recorder (DVR) or the network video recorder (NVR) ensuring image data is secured.

Deciding on power backup of CCTV/VSS Camera:

- The CCTV/VSS system requires a constant power supply
- Ensure power cannot be tampered with or switched off unintentionally
- Consider a UPS backup (uninterrupted power supply) for the security system in the event of a localized power failure
- would ensure incessant surveillance. Thus, make sure you have both a constant power supply and a reliable power backup in case of power cuts to ensure security at all times.

Post Installation Testing:

After you're done with the installation process, it is very important to fully test the system.

- Has the installer delivered the brief?
- Are the live and recorded images as expected day and night?
- Are the cameras focused correctly and recording images?
- Do the cameras meet local data protection laws and if not, can they be moved, or images redacted to meet the requirements of the laws?
- Are the cameras and the cables safe from tampering?

Maintaining the CCTV/VSS cameras:

Best practice

- Daily system recording check, documented system's functionality checks
- Regular camera cleaning removing dirt or cobwebs
- Annual (FSR minimum requirement) maintenance inspection of the CCTV/VSS System
- Agree on supplier call-out response time and service schedule

Quality in cameras: how to choose the right security camera?

Although often such advice is given by the installation company used, it's important to understand what makes any camera the best for your facility. Choosing the right camera or cameras is the most complex decision in any video surveillance project.

Different types of cameras can be classified by various technical aspects, such as whether they are motorized or not, or whether they allow night vision or not. On this occasion, we are going to focus on another fundamental aspect that directly refers to the quality of the captured image. By knowing what each camera is supposed to do and giving it a job description will make it easier to ensure the correct camera is selected. The location of the camera can also determine what specification the camera must have for example sunrise and sunset times. Some cameras automatically compensate for the light change (WDR).

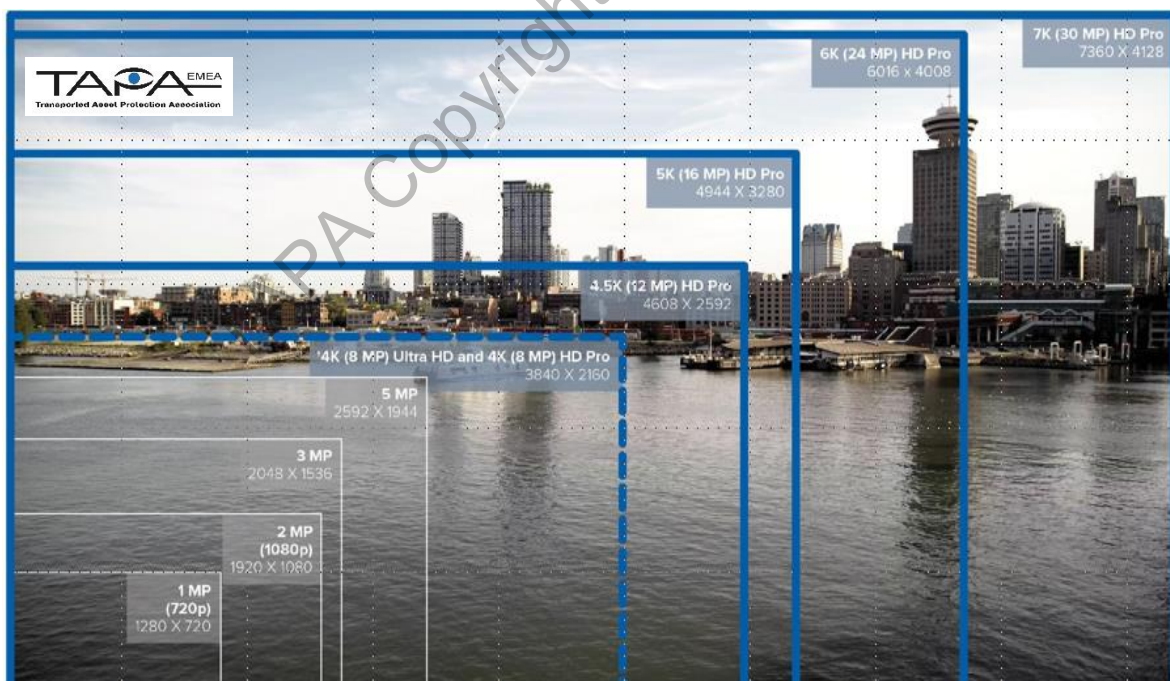
What is image resolution?

The resolution of an image indicates the level of detail that can be observed in it.

Resolution is measured in pixels, specifically in columns of pixels (the width of the image) and rows of pixels (the height of the image). The greater the number of columns and rows of pixels, the higher resolution said image will have, and the greater the level of detail it will be able to offer us.

When we multiply that number of pixel columns by the number of pixel rows, we get the unit of measurement in millions (mega) of pixels. So, for example, suppose we have an image 1500 pixels wide by 1200 pixels high. We would have an image with a total size, a resolution, of 1,800,000 pixels, which if we go to a million, would be 1.80 megapixels.

Megapixel (MP) Comparisons



In the image above, the contrasted viewing coverage can be seen ranging from a small area with a 1Megapixel camera to a vast area with 30MP. The context for logistic sites is that high positions can often be achieved on buildings and lighting columns. This enables greater area coverage (internally and externally) to be achieved with fewer cameras.

IP cameras need little manual servicing as camera setup can be done at the camera, column base, at the operator control position, or remotely (subject to IT security parameters) so optimum and ideal coverage is now achievable with less compromise due to camera access concerns.

Typically, this reduces busy camera count, with camera location intensity now limited to areas with reduced line of site (internal hallways, etc)

IP cameras capture video images, compress them, and transmit them in digital format over the network. The recorder is programmed with IP addresses to receive these video streams and record them to NVR (network video recorder). Typically, HD Cameras range from 2MP, with advanced manufacturers having currently up to 61 MP units. These have revolutionized Video observation with the ability to do more with fewer cameras. Typically, IP cameras are PoE (Power over Ethernet) reducing infrastructure cost versus mains requirement on previous camera types.

Megapixel density now prescribes the camera's relationship to the target, so the distance and definition of target outcomes can now be prescribed, and it would be recommended that any solution offered has a design tool plot to ensure the level of coverage and fixed camera viewing zoom for both live and recorded images.

It is also important to ensure that appropriate ambient area lighting is available in the camera's view. It would be anticipated that with good quality cameras aligned with site lighting as a health and safety requirement for logistics sites general site coverage is enough with ancillary lighting at the edge or shadowed areas.

Consideration should also be given to vegetation management particularly on perimeter lines to ensure cameras are not obscured. Thermal imaging cameras could be a consideration for areas where lighting would be problematic (light pollution adjacent to private housing). Similarly, overshooting into other premises must be avoided when deploying longer-range camera views.

The example below defines the context of megapixel density, however, note, that the relevant density of say could be achieved with a 2-3 megapixel at a short range, raising the camera megapixel spec for longer ranges



Change Management

Internal change controls are an important part of an organization's risk management program, especially where changes to the operating environment, facility layout, usage, asset value, and desirability create additional security risks.

From the outset, supply chain risks, likelihood, and impact are factors that most warehouse, transport, and logistics providers want to assess. In doing so, they seek to minimize the risks associated with supply chain disruptions, security incidents, the unavailability of goods through theft or other malicious acts, and potential damage to an organization's brand or reputation.

The methodology employed, typically referred to as a risk assessment examines both general and specific threats, vulnerabilities, asset criticality, likelihood, frequency, and impact. Ultimately, an organization's assessment program aims to mitigate its known security risks to a level commensurate with its risk appetite.

Facility buildings support many different types of operations and workplaces. The definition of a workspace varies widely according to its function and may range from offices to warehouses, loading bays, and product storage areas. Depending on its use, each area offers different levels of inherent risk, both for the organization and its employees.

Understanding the functionality of a building, and how and where organizational assets are stored, handled, and transported forms an integral part of the facility risk and change control assessments. Facility buildings may also be multi-occupancy, consisting of private and common access areas, which equally need to be managed.

Asset criticality or value is often determined by a range of factors including:

- The cost of purchasing or replacing the asset.
- The commercial impact of an unavailable asset when it is stolen.
- The effects of harm to the asset.
- The length of time required to manufacture and/or replace the asset.
- The impact on an organization's reputation or brand, where the asset can't be delivered to a customer.

Whilst many certified businesses correctly apply TAPA's Facility Security Requirements to their facilities, over time operational changes outlined above may impact its ability to protect its critical assets. One example might be where critical assets monitored by the facility's video surveillance system have been moved to an area without camera coverage. Similarly, a newly constructed internal wall might now block the view of existing video surveillance cameras monitoring a high-value storage area. In both cases, the effectiveness of the security protection has been reduced, thereby increasing the likelihood of a successful targeted attack against the asset.

Most organizations employ some sort of change management process. The facility video surveillance system needs to be an integral part of this process because as we've just seen, new vulnerabilities may be introduced because of systems or environmental change. Wherever possible the security responsible person should identify the organization's change management controls and establish a notification process when a change impacts security. A regular program of security testing will also help to ensure the site's video surveillance camera systems are necessary, relevant, and proportionate to the level of assessed risk.

5. FSR Overview

Video Surveillance systems are an important layer for protecting facilities, the people in and around the facilities, and the cargo being stored or moved through the facilities. However, it should be clear that they are just one of many countermeasures to be considered when selecting deterrents and physical security measures to protect employees, vehicles, facilities, and stored cargo. Therefore, TAPA recommends to its members and the industry to adopt TAPA FSR as the standard for logistic facilities. Achieving TAPA FSR certification means that the facility has been approved by an accredited certification body (IAB) for FSR Level A-C or via a self-audit by authorized auditors (AA) by TAPA LSP/Applicant for FSR Level C.

The FSR requires a layered approach to protecting facilities and includes:

- Scalable security levels to assist the facility owner in the selection of risk mitigation countermeasures.
- FSR Level C provides basic countermeasures and procedures that help to provide deterrents and protection for facilities from criminal interest.
- FSR Levels A and B provide more robust countermeasures and procedures and are more suited to protect high-value and/or vulnerable cargo.
- Where the facility is deemed to be at high risk then FSR can also be used for additional enhancements to cover IT/Cyber threat measures.

TAPA FSR – CCTV/VSS systems and the FSR standard.

TAPA is not a testing and compliance organization and therefore cannot certify, confirm, or reject any security products that are used to help facility owners meet the requirements of TAPA security standards.

Despite claims by some providers of CCTV/VSS systems, no CCTV/VSS systems have been certified by TAPA to meet TAPA standards.

This does not mean that suitable CCTV/VSS systems are not available, it just means TAPA cannot certify or endorse them.

Identifying Video Surveillance systems that meet or exceed TAPA FSR requirements can sometimes be a challenge for auditors and end users. This section will seek to explain the features and capabilities that a CCTV/VSS system is required to meet as part of the FSR certification audit.

TAPA CCTV/VSS FSR Guidance

Why?

Applying the 'defence in depth' principles (deter, detect, delay, mitigate, respond), Video Surveillance cameras when used in conjunction with other security systems form a vital part of the location's overall security protection measures.

Video Surveillance coverage to provide general oversight of open space. This will enhance the site's situational awareness and help detect potential issues before they occur.

- Monitor pedestrian and vehicle movement routes.
- Tracking people, vehicles, and assets around the site.

Deter

The presence of Video Surveillance systems is likely to deter intruders by making the facility perimeter appear too physically/technically difficult to breach, thereby increasing the probability of the attacker's detection, failure and/or capture.

Visual deterrents may include the display of signage on the outer perimeter fence line highlighting the use of Video Surveillance cameras and security lighting.

Detect

Using Video Surveillance cameras to identify suspicious activities within the facility's external cargo handling, shipping, and receiving areas include:

- The early detection of intruders as they cross the outer perimeter boundary.
- Visual verification of perimeter intrusion alarms and alerts.
- To raise the alarm and to initiate further investigations and/or escalation.
- Initiation of an appropriate response to the perceived threat.
- Most systems now can detect movement and/or in specific directions and alert controllers remotely.

Delay

The presence of Video Surveillance camera systems in conjunction with other physical barriers, including secure access, loading bay, and driver reception doors maximize the time taken for an attacker to breach the building's security once detection has occurred.

Where intruders have already breached the outer perimeter and gained access to the facility's cargo handling, shipping, and receiving areas, Video Surveillance cameras provide visual verification of the attack force, including information about their numbers, the use of a getaway vehicle, possession of any weapons, prohibited articles or tools.

Mitigate

The use of perimeter protection measures, including Video Surveillance to minimize the impact of an attack.

Maximize the protection provided to access points at the perimeter.

Facility warehouse external cargo handling, shipping, and receiving yard areas are generally located in a zone between the outer and inner (building) perimeter boundaries. Operational activities typically include the loading and unloading of products, shunting, and vehicle marshalling. For this reason, they are busy workspace areas.

Threats may include the presence of onsite intruders, illegal migrants (from a trailer incursion), insider threats (rogue employees), or other unauthorized personnel in the area.

Response

Use of Video Surveillance and other perimeter detection systems to determine where/if an attack is taking place.

- Allocation of resources to deal with the threat.
- Law enforcement response.
- It is important that the response time is less than the time of detection and the time of breach.

In this section, we shall review the CCTV/VSS-related requirements included in the FSR 2023 standard and try to analyse why these requirements are in place and what would have been the risk if they were not included in the standard. Some lighting-related requirements are reviewed in this section since lighting is an integral part of effective Video Surveillance.

7.1 Warehouse External Cargo Handling, Shipping & Receiving Yard (General)

Warehouse External Cargo Handling, Shipping and Receiving Yard (General)	
7.1.1	CCTV (Closed-Circuit Television) / VSS (Video Surveillance System) able to view all traffic at external cargo handling, shipping and receiving yard (including entry and exit point(s)) ensuring all vehicles and individuals are recognizable at all times unless temporary obstruction due to operational needs (i.e., truck loading and unloading in real time).

Why?

Even though not all TAPA FSR Certification levels mandate a physical perimeter, a facility operator needs to be able to view via CCTV/VSS the area surrounding the warehouse building and the handling areas, as well as to recognize approaching and leaving vehicles and individuals.

Risk

A lack of CCTV/VSS compliance in this key risk area may result in

- The undetected presence of a site intruder
- Unavailability of evidence to support claims or investigations.

External Dock Areas

External Dock Doors	
7.1.11	External Dock areas covered via color or “day/night” exterior CCTV/ VSS cameras.
7.1.12	CCTV/ VSS Cameras mounted to be able to view all operations and movement around external dock area at all times unless temporary obstruction due to operational needs (i.e. truck loading and unloading in real time).
7.1.13	All vehicles and individuals around external dock areas must be covered by CCTV / VSS cameras which can clearly show the vehicle identification information and able to discern facial features of personnel. <i>Note: TAPA will allow existing certification holders without the capability to upgrade to camera resolution, to continue with their current resolution until the 2026 revision. New certificate holders or new sites must meet the new requirement.</i>
7.1.14	Vehicles and individuals around external dock areas must be covered and visible by CCTV/ VSS cameras in most cases.
7.1.15	All external areas around dock doors fully illuminated.

Why?

External dock doors are used to facilitate the delivery/collection of finished goods, product packaging, and raw materials. For some facilities, the presence of external dock doors allows direct access into the warehouse, production, or storage areas, thereby increasing the likelihood of a successful targeted attack against its protected assets.

Video Surveillance Cameras deployed in external dock areas shall be of sufficient quality to provide recognizable day/night images of vulnerable areas outlined within the TAPA FSR Standard.

The term “facial features” means recognition and differentiation, such as skin and hair color, structure, and individual peculiarities, which would possibly support the identification of an employee or a well-known person.

An image is recognizable if the user can identify an individual by their demeanour, mannerisms, clothing or a vehicle by its registration plate number, model, color, and branding.

Video Surveillance images are important in the recognition of site intruders, the identification of suspicious or criminal behaviour, and to prevention of the loss of company property. Real-time images allow the security team to make dynamic risk decisions based on the events being viewed.

Gaps in video surveillance coverage mean security incidents may be missed. Camera quality concerns also introduce question marks over evidential quality and image integrity.

Risk

Where video surveillance cameras are not deployed within these critical areas to meet the required TAPA’s Facility Security Requirements level, the following risks could materialize:

- Risk of an undetected intrusion event, resulting in serious injury or harm to a company employee.
- Unauthorised access to a restricted area or asset
- Theft
- Product interference
- Safety violation
- Unavailability of images for post-incident investigation

7.2 Outside Walls, Roof and Doors

Exterior sides of the facility: CCTV	
7.2.1	Color or “day/night” exterior CCTV/ VSS camera in place covering all exterior sides of the facility.
7.2.2	Color or “day/night” exterior CCTV/ VSS camera system in place covering exterior sides of facility with doors, windows or other openings.
7.2.3	All views of exterior CCTV/ VSS camera system clear at all times unless temporary obstruction due to operational needs (i.e. truck loading and unloading in real time).
7.2.4	All vehicles and individuals around exterior sides of the facilities be covered by CCTV/ VSS cameras, which can clearly show the vehicle identification information and able to discern facial features of personnel.
7.2.5	Vehicles and individuals visible in most cases by the exterior CCTV/ VSS cameras.
7.2.9	External access to roof (ladder or stairs) must be: Physically locked and covered by CCTV/ VSS (Color or “day/night” cameras). or Physically locked and alarmed.

Why?

Applying the defense-in-depth principles, the exterior facility sides typically represent the inner perimeter boundary line. Within this inner perimeter are often located the businesses' protected assets. Risk areas include facility windows (ground & lower floor), walls, roof, and doors. Attackers will target these vulnerable areas, as they often represent the path of least resistance to achieving their goal.

The presence of Video Surveillance cameras in these key areas allows for the:

- Early detection of intruders as they cross the inner perimeter boundary.
- Visual verification of perimeter intrusion alerts.
- To raise the alarm and to initiate further investigations and/or escalation.
- Initiation of an appropriate response to the perceived threat.

Video Surveillance cameras deployed within these critical areas will both capture these events and mitigate the security risk down to acceptable levels.

Gaps in camera coverage mean security incidents may be missed.

Camera quality concerns also introduce question marks over CCTV/VSS evidential value and image integrity.

Risk

Where TAPA’s Facility Security Requirements are not met at the required level, there is a risk of:

- Undetected intrusion event
- Unauthorised access to information or other protected assets
- Theft
- Safety violation
- Unavailability of images for post-incident investigation.

7.3 Office and Warehouse Entry and Exit points

Office area Visitor Entry Points (s)	
7.3.2	Office area visitor entry point(s) covered by CCTV; (Color or “day/night” cameras) individuals clearly recognizable at all times.

Why?

Office and warehouse entry/exit points are typically the main entry points through which company employees gain access to the site’s protected assets. The deployment of Video Surveillance cameras in conjunction with other security systems ensures building access is both controlled and monitored, thereby mitigating the risk of a successful targeted attack.

Additionally, the setup of a CCTV/VSS system according to the above requirement facilitates the recognition of visitors in real-time or at a later date.

Video Surveillance cameras deployed within these critical areas will both capture these events and mitigate the security risk down to acceptable levels.

Gaps in camera coverage mean security incidents may be missed.

Camera quality concerns also introduce question marks over CCTV/VSS evidential value and image integrity.

Risk

Where TAPA’s Facility Security Requirements are not met at the required level, there is a risk of:

- Undetected intrusion event
- Unauthorised access to information or other protected assets
- Theft
- Safety violation,
- Unavailability of images for post-incident investigation.

Workforce Entry Points	
7.3.10	Workforce entry point (s) covered by CCTV/VSS; (color or "day/night" cameras).

Why?

Video Surveillance cameras deployed at workforce entry points shall be of sufficient quality to provide recognizable day/night images. An image is recognizable if the user can identify an individual by their demeanour, mannerisms, and clothing.

Video Surveillance images are important in the recognition of site intruders, the identification of suspicious or criminal behaviour, insider threat, and theft. Real-time images allow the security team to make dynamic risk decisions.

Recorded images assist with the investigation and detection of crime.

Additionally, the setup of a Video Surveillance system according to the above requirement facilitates the recognition of drivers and employees in real-time or at a later date, to trace the entry and exit points.

Video Surveillance cameras deployed within these critical areas will both capture these events and mitigate the security risk down to acceptable levels.

Gaps in camera coverage mean security incidents may be missed.

Camera quality concerns also introduce question marks over CCTV/VSS evidential value and image integrity.

Risk

Where TAPA’s Facility Security Requirements are not met at the required level, there is a risk of:

- Undetected intrusion event
- Unauthorised access to information or other protected assets
- Theft
- Safety violation
- Unavailability of images for post-incident investigation.

Driver and Vehicle Identification	
7.3.17	Vehicle identifiers are logged manually (i.e. written) or with cameras. Include at a minimum license plate and vehicle type.

Why?

The presence of Video Surveillance cameras at vulnerable vehicle entry points ensures truck identifiers, such as the vehicle model, color, branding, and registration numbers are viewed both in real and recorded time. When combined with other security systems, such as barrier and access control, Video Surveillance cameras provide a vital element of the facility's overall security protection systems.

Facilities are at risk from both petty (opportunistic) and organised crime activities, where attackers use a variety of fraud techniques including the use of false company, truck, and driver identities to steal from businesses.

The presence of effective entry controls combined with effective Video Surveillance cameras and identity verification systems ensures the risks associated with a fraudulent collection are mitigated to acceptable levels.

Risk

The absence of Video Surveillance cameras in this area means vital evidence may be lost and/or missed. The resultant losses may be both financial (in terms of the value of the goods stolen) and reputational in respect of the impact on the company brand. Once stolen goods may also be sold on the 'black market' with consequential quality and consumer risks.

Internal Dock Doors and Dock Areas	
7.4.4	All internal dock doors and dock areas covered by CCTV. (Color or "day/night" cameras).
7.4.5	Views of freight being loaded/unloaded at all internal dock doors and dock areas, clear at all times unless temporary obstruction due to operational needs (i.e. truck loading and unloading in real time).
7.4.6	Buyer assets under 100% CCTV surveillance in cargo movement or staging areas (i.e. pallet breakdown/ build up areas, routes to and from storage racks, dock, transit corridors).

Why?

There are several reasons for this requirement, addressing both malintended activities as well as identification of misplaced goods that might not reach their destinations and claims that might be initiated by customers.

If we take out the real-time or post-incident identification of intruders (i.e. with Video Content Analysis alarming functionality or with real-time CCTV/VSS monitoring), this requirement, if in place, might be proven very helpful:

- In case your customer raises a claim, you need to be able to prove that the sealing process has been applied correctly (you need to be very careful when you install your internal dock-doors cameras and also ensure that dock doors are closed after the sealing process is completed if you want to be able to take advantage of this functionality),
- Or that a specific pallet or package missing at the destination was actually loaded at the origin. Of course, you need to adapt the resolution of your Video Surveillance system recordings if you want to take advantage of this capability, as well.

Risk

Where TAPA's Facility Security Requirements are not met at the required level, there is a risk of:

- Undetected intrusion event,
- Unauthorised access to information or other protected assets,
- Theft
- Safety violation
- Unavailability of images to investigate
 - Undetected intrusion event
 - Vehicle loading/unloading & sealing processes
 - Customer claims

7.4 Inside Warehouse and Office

High Value Cage (HVC) /Area	
7.4.15	Complete CCTV/VSS (Color or "day/night" cameras) coverage on HVC entrance and internal area. <i>Note: If the HVC is too small to locate a camera inside, camera coverage of the entrance is sufficient.</i>
7.4.16	CCTV (Color or "day/night" cameras) coverage on HVC entrance.
7.4.18	HVC doors/gates are alarmed to detect forced entry. Alarms can be generated by door contacts and/or use of CCTV/ VSS motion detection to detect unauthorized access.

Why?

As the High Value cage is the area where definition the most theft-targeted products are stored, it goes without saying that the entrances and the interior of the High Value cage need to be protected as best as possible.

In some cases, Video Surveillance is also used with motion detection functionality to alarm these cages.

Risk

Where TAPA’s Facility Security Requirements are not met at the required level, there is a risk of:

- Undetected intrusion event to the HVC
- Unauthorised access to the HVC
- Theft
- Unavailability of images for post-incident investigation.

Trash Inspection from Warehouse	
7.4.21	Internal and/or external warehouse main trash collecting bins/ compacting areas are monitored by CCTV/VSS.

Why?

One common way to carry small-sized goods from the warehouse, out of it, is by using the trash bins, usually, by employees. Having effective CCTV/VSS coverage of these bins can assist in preventing or identifying losses executed with this modus operandi.

Risk

Where TAPA’s Facility Security Requirements are not met at the required level, there is a risk of:

- Theft,
- Safety violation
- Unavailability of images for post-incident investigation

Internal fraud and pilferage incidents can be prevented if this requirement is applied effectively, otherwise, losses associated with this modus operandi might appear.

Cargo Integrity; Loading/Unloading Validation Process	
7.4.32	<p>Robust procedures are in place ensuring that all Buyer assets shipped and received are validated at the point of handover by conducting a manual and/or electronic piece count. The process must ensure abnormalities are consistently recognized, documented, and reported to the LSP/Applicant and/or Buyer.</p> <p>Manual and/or electronic records must be of evidential quality. If drivers are not present to witness this activity, Buyer/LSP/Applicant must ensure alternative count verification such as scans and/or CCTV/VSS images, collected and retained specifically for this purpose.</p> <p><i>Note: In addition to missing pieces, abnormalities may include damage, missing straps or tape, cuts, or other obvious openings, indicating a possible theft or pilfering.</i></p>

Why?

In this case Video Surveillance supports cargo counting during loading or unloading as an alternative method. The records by CCTV/VSS should be kept for as long as your customers have the right to claim for missing goods, so even if the standard requirement is 30 days min, you might consider expanding this duration if your customers can claim missing goods for more than 30 days, provided of course that there are no operational or legal restrictions.

Risk

Where TAPA’s Facility Security Requirements are not met at the required level, there is a risk of:

- Not being able to collect post-incident evidence for losses and customers’ claims.
- Not being able to collect evidence of missing items during cycling or wall-to-wall inventory counts.

7.5 Security Systems; Design, Monitoring, and Responses

CCTV	
7.5.18	Digital recording of CCTV/VSS in place.
7.5.19	Recording speed for CCTV/VSS is set as a minimum for 8 frames per second (fps) per camera.
7.5.20	Digital recording functionality checked daily on operational days via procedure. Records available.
7.5.21	CCTV/VSS recordings stored for a minimum of 30 days, where allowed by local law. LSP/Applicant must provide evidence of any local laws that prohibit the use of CCTV and/or limit the video data storage to less than 30 days.

CCTV	
7.5.22	Access tightly controlled to CCTV/VSS system, including hardware, software, and data/video storage. This room must be locked if the CCTV/VSS storage system is on premises with access controls in place.
7.5.23	CCTV/VSS images, for security purposes, are only viewed by authorized personnel.
7.5.24	Procedures in place detailing CCTV/VSS data protection policy regarding use of real-time and archive images in accordance with local law.

Why?

Manufacturers of Video Surveillance equipment no longer support analogue recording systems, therefore the recommended recording platform for FSR compliance is digital.

The digital recording provides:

- Superior image quality which meets data protection legislation
- Higher capacity for data storage of images.

Frames per Second (FPS) set at a higher frame rate results in smoother image playback of recorded images.

Eight (8) fps does not only enhance the quality of the video but also gives the capability of the Video Surveillance system to capture more frames during an incident. For example, if there is a suspicion about an employee carrying a small smart-phone box out of the facility, and the employee is captured in the CCTV/VSS for 15 seconds running from the warehouse exit door to his parked car (50 or 60m away from the door), then with 8 fps the system shall record $8 \times 15 = 120$ frames, whereas with 3fps the system shall record $3 \times 15 = 45$ frames. As usually, the employee tries to hide the box, it is more likely to have a frame recorded the box when you have 120 frames compared to 45 frames.

A daily check of recording is necessary to ensure the effectiveness of the system. It is very disappointing and frustrating to realize that recordings are not available after an incident has taken place and an investigation has been initiated.

Thirty (30) days of Video Surveillance records storage is a requirement addressing the need for evidence availability in case of claims or losses that are either identified not in real-time (i.e. cyclic inventory counts, or destination claims of missing goods). You might consider expanding this duration if your customers can claim missing goods for more than 30 days, provided of course that there are no operational or legal restrictions.

As destruction or alteration of evidence is a common way for criminals to escape from identification, it is very important to protect the access of the CCTV/VSS system, including hardware, software, and data/video storage.

This protection is both physical and electronic i.e., both the data rooms need to be physically protected and alarmed, as well as the software access either locally or in the cloud should be adequately and effectively protected. Management of access rights and passwords should be in place to ensure the proper application of this requirement.

Finally, personal data protection requirements, both legal and ethical) should be considered to ensure Video Surveillance images, for security purposes, are only viewed by authorized personnel and that documented procedures are in place detailing Video Surveillance data protection policy regarding the use of real-time and archive images in accordance with local law.

Local legislation should always be analyzed to ensure understanding is identical to the legal requirements and that we do not interpret the law according to our intentions.

Risk

Where TAPA’s Facility Security Requirements are not met at the required level, there is a risk of:

- Lack of adequate CCTV/VSS records to support investigations
- Lack of evidential quality CCTV/VSS recordings
- Intentional or unintentional deletion or alteration of CCTV/VSS records
- Legal implications.

Exterior and Interior Lighting	
7.5.25	Exterior and interior lighting levels are sufficient to support CCTV/VSS images that allow investigation and evidential quality image recording.
7.5.26	Exterior and interior lighting levels are sufficient to clearly recognize all vehicles and individuals.

Why?

Even though current technology supports video recording in the dark, it is always desirable to enhance the video recording capability with ambient lighting. As day-night cameras switch from color to black and white recording when the lighting conditions are not sufficient, CCTV/VSS is able to record even in the dark.

A rule of thumb related to the quality of recording and lighting conditions is that lighting for CCTV/VSS should be based on the inverse square rule: **if you double the distance to the subject being lit, you will need FOUR times the original light**. Additional lighting can be used to create an evenly lit scene in the camera's field of view, as this will ensure captured images are not too dark or washed out.

Experts recommend (not required):

- External light levels at the sides of the building need a minimum of 5 Lux
- Loading/unloading area needs a minimum of 50 - 100 Lux
- Parking /handling area close to the dock area needs a minimum of 20 Lux
- Gatehouse/vehicle entrance area needs a minimum of 100 Lux

- In the warehouse min 150 Lux.

A good reference for this topic is included in the link below:

<https://www.anixter.com/content/dam/Suppliers/Raytec/Complete%20Guide%20to%20CCTV%20Lighting.pdf>

Risk

Where TAPA’s Facility Security Requirements are not met at the required level, there is a risk of CCTV/VSS images not of evidential quality hindering both real-time and post-investigation situations.

7.6 Training and Procedures

Maintenance Programs	
7.6.11	Maintenance programs in place for all technical (physical) security installations/ systems to ensure functionality at all times (e.g. CCTV/ VSS, Access Controls, Intruder Detection, and Lighting).

Why?

To ensure proper functionality all technical systems need to undergo a planned maintenance program.

Risk

The major risk when no regular and scheduled preventive or corrective maintenance is in place is that the systems might not be fully operational when required.

8.6 CCTV and alarm layout of sites

CCTV and alarm layout of all the sites	
8.6.1	The central function shall have procedures in place that ensures that all sites review and maintain documents on all physical security systems like CCTV and alarm layout.

Why?

A documented procedure ensures consistency in keeping updated documents and installation plans for technical systems.

Risk

In case there is no updated documentation related to the installed technical systems including CCTV, issues might appear in case of operation, troubleshooting, maintenance, and rectification of systems.

Requirements vs. Associated Risk Matrix

Req/Security Risk	Internal Fraud and Pilferage	Not real-time intrusion detection and alarming	Unavailability of CCTV/VSS to support claims or investigations	Legal implications	Deletion or alteration of CCTV/VSS records	Non evidential quality records
7.1.1		X	X			X
7.1.11 7.1.12 7.1.13 7.1.14 7.1.15	X	X				X
7.2.1 7.2.2 7.2.3 7.2.4 7.2.5 7.2.9	X	X	X			X
7.3.2		X				
7.3.10	X	X	X			
7.3.17		X	X			
7.4.4 7.4.5 7.4.6	X	X	X	X		X
7.4.21	X					
7.4.32	X		X			X
7.4.15 7.4.16 7.4.18 7.4.21 7.4.32	X	X	X	X		
7.5.18 7.5.19 7.5.20 7.5.21 7.5.22 7.5.23 7.5.24			X	X	X	X
7.5.25 7.5.26			X			
7.6.11		X	X		X	X
8.6.1	X		X		X	

6. Frequently Asked Questions

What is an IP camera?

IP stands for Internet Protocol. An IP camera is a digital video system that can be connected and transmit data over a network. These cameras work can be viewed both locally and remotely so that you can view your security feed from anywhere with an Internet connection. IP cameras can also be referred to as network cameras or webcams.

What is the difference between a DVR and NVR?

There are several differences between DVR and NVR, the most important are:

- NVR can be part of a computer network along with the IP cameras, therefore there is no need to run dedicated wires to support your CCTV/VSS system; you can use the existing network infrastructure.
- The NVR supports high-resolution megapixel cameras
- The DVR uses coaxial connections to each of the analogue cameras.
- The DVR supports only cameras with VGA resolution

Does lighting need to be on permanently?

Lighting only needs to be on only if it acts as a deterrent in itself; criminals prefer to work in dark environments. Energy-efficient LED lighting significantly reduces the cost of permanently illuminating dark areas. As an alternative to permanent lighting in a CCTV/VSS monitored area, lights can be controlled by motion sensors, provided they respond immediately to catch fast action.

How many hours of video can the DVR/NVR store?

Several parameters may affect this answer. Some of them are:

- Number of cameras
- Resolution and Frames per second recorded
- Size/capacity of storage devices (hard drives)

How much does a CCTV/VSS system cost?

Price is always a relative figure. What is most important here is to find the best relationship between price and quality. Absolute prices of CCTV/VSS systems may vary significantly based on the components. For example, CCTV/VSS cameras range in price from about €100 to around €500.¹

The most important thing is to understand what you want to achieve with the system and then get one that brings together the right components that make it fit for the purpose you intend. Always describe your operational needs rather than technical specs.

¹ <https://www.security.org/security-cameras/cost/>
CSG Version 2.0 – 01st March 2024

The supplier needs to “translate” your operational needs to the technical specifications of the system that he has to design, install, and commission.

Value rather than the lowest cost is the foremost objective of many buyers. Maintenance and support, as well as hardware, software, and installation costs, should all be factored in when trying to determine the supplier that offers the best value.

IP CCTV/VSS supports a Lower Total Cost of Ownership (TCO) through remote monitoring of camera operation and reduced maintenance. HD cameras with up to 30-megapixel resolution, and remote control of zoom and direction of view, enable system consolidation by reducing the number of cameras required.

What are the basic components of a modern CCTV/VSS system?

For an IP surveillance system, you’ll need:

- The actual IP cameras
- An NVR or other type of storage system
- Accessories such as microphones and speakers generally will come built into the cameras (if necessary) so additional parts will not be required.

How does recording on motion detection work?

You can program your CCTV/VSS system to record motion detection. Usually, the programming supports also recording some seconds before motion detection (i.e. you can program your system to record 15 seconds before someone enters a room.)

But how does the system know that in 15 seconds someone will enter the room, so it can start recording 15 mins ahead?

The answer is simple: the system records continuously and if there is no entrance, it deletes the recorded video and over-writes the new one. In case motion is detected, the system records until the motion is stopped and the recorded video is stored and not deleted.

What is Lux?

Lux is the unit for measuring the quantity of lighting. One lux (Latin for “light”) is the amount of illumination provided when one lumen is evenly distributed over an area of one square meter.

What is lumen? Unfortunately, you need to go deep into your school physics books to find this out.

Note: Just for reference and not for information: a lumen is equal to the amount of light emitted per second in a unit solid angle of one steradian from a uniform source of one candela. Many unknown words, there is no need to go deeper!

What happens if there is a power outage?

Like any electrical component, DVRs and NVRs might be damaged by power surges and spikes (fluctuations of voltage), so they must be properly protected. DVR/NVRs will come back on as soon as power is restored. However, an uninterruptable power supply (UPS) that provides a short period of backup power and serves as a surge protection device is strongly recommended. This ensures your video surveillance will still be online in the event someone cuts the power to break in unnoticed.

If you decide to use a UPS for a short period of time, please note that CCTV/VSS records will not be available in case of longer power outages; a backup power connection to an existing diesel generator might be a good solution to ensure the continuity of CCTV/VSS operation.

Can I use a CCTV/VSS system to identify and report an alarm?

Yes, even older DVRs can transmit an alarm based on specific conditions (i.e., motion detection). Modern CCTV/VSS systems are equipped with alarm-triggering conditions based on VCA (video content analysis) that can raise an alarm.

What is Video Content Analysis?

Video content analysis or video content analytics (VCA), also referred to as video analysis or video analytics, is the capability of analyzing video automatically to detect and determine temporal and spatial events. This analysis can be executed by software or hardware applications/components installed at both the cameras and the CCTV/VSS components/devices.

Motion detection is the simplest video analytics application where a camera can identify a motion event and execute some specific tasks (i.e. start recording video footage or trigger an alarm).

Some other Video Contents Analysis applications are:

- Object detection, where the presence of a type of object, for example, a person or car, can be identified.
- Shape recognition, where specific shapes in the input video, for example, circles or squares, can be identified.
- Tamper detection, which is used to determine whether the camera or the output signal is tampered with.
- Recognition, that is used for face recognition or number plate recognition applications.
- Missing Object detection, where the disappearance of an existing object from the camera view can be identified.
- Flame and smoke detection, where modern IP cameras with intelligent video surveillance technology can be used to detect flame and smoke in 15–20 seconds or even less due to internal built-in special hardware.

- Dynamic masking, where a part of the video signal is automatically blocked, for example, because of privacy issues.

How much storage space do I need to be compliant with the FSR 2023 standard's requirements?

Several factors need to be taken into account when it comes to the calculation of CCTV storage capacity. Below you can find some of them and also see a rule of thumb to have an initial calculation of the required storage capacity for your CCTV/VSS system:

- **Resolution:** The higher the resolution of the cameras, the more storage space will be required to store the video footage. Higher resolutions will result in larger video files.
- **Frame rate:** The frame rate of the cameras determines how many frames per second the cameras capture. Higher frame rates will result in more storage space being required. In your training material, there are some links where you can take a look at different fps rates and see the resulting footage. These links are also included at the end of this document.
- **Compression:** Compression algorithms can help reduce the size of video files but at the cost of some loss of quality. The amount of compression used can impact the amount of storage space required.
- **Retention period:** The length of time that the video footage needs to be stored will affect the amount of storage space required. Longer retention periods will require more storage space.

There are several methods to calculate the required storage capacity. One of them is to use the following formula:

$$\text{Storage Capacity per camera (GB)} = \text{Bitrate (Kbps)} * 1000 / 8 * 3600 * 24 * \text{Days} / 1\,000\,000\,000$$

Where:

- Bitrate is the amount of data that is generated per second by the cameras (in kilobits per second or kbps). Generally, bitrate is the amount of data processed per second when recording footage. More bits per second equals more video information. More information implies more details, which means better screen quality.
- 3600 is the number of seconds in an hour.
- 24 is the number of hours in a day.
- Number of Days is the retention period.
- 8 is the number of bits in a byte.

For example, if you have 1 camera with a bit rate of 1024 kbps, and you want to keep the footage for 30 days, the required storage capacity is:

Storage Capacity = $(1024 \times 1000 / 8 \times 3600 \times 24 \times 30) / 1\,000\,000\,000 = 332 \text{ GB or } 0.32 \text{ TB}$.

In case you have 30 cameras installed, it is easy to calculate by multiplying the above figure with the number of cameras, i.e. $30 \times 0.32 \text{ TB} = 9.72 \text{ TB}$

This is only an estimate; the actual storage capacity required may vary depending on the specific cameras and system settings (continuous or motion-activated recording and others) used and needs to be calculated by the designer/installer of your CCTV/VSS system.

How can I review and confirm adequate coverage before the actual installation of the CCTV /VSS system?

This is one of the most often asked questions by members who do not have the technical expertise to evaluate the proposals received by the CCTV installers. It is very common for CCTV suppliers to ask for technical characteristics before they prepare and submit a financial proposal, this is the reason why they shall ask you about resolution, pixels, color or day-night cameras, continuous or event-driven recording, storage space, etc. Some of us might be aware of what these terms mean, but this is completely different from using these terms to define the components of the CCTV system that you want to purchase, install, and operate.

In most cases, suppliers try to commit you to technical specifications to avoid any liability in case the delivered system does not perform according to your expectations. This is why it is strongly advisable to avoid detailing technical specifications; instead, you can use functional requirements to describe your expectations.

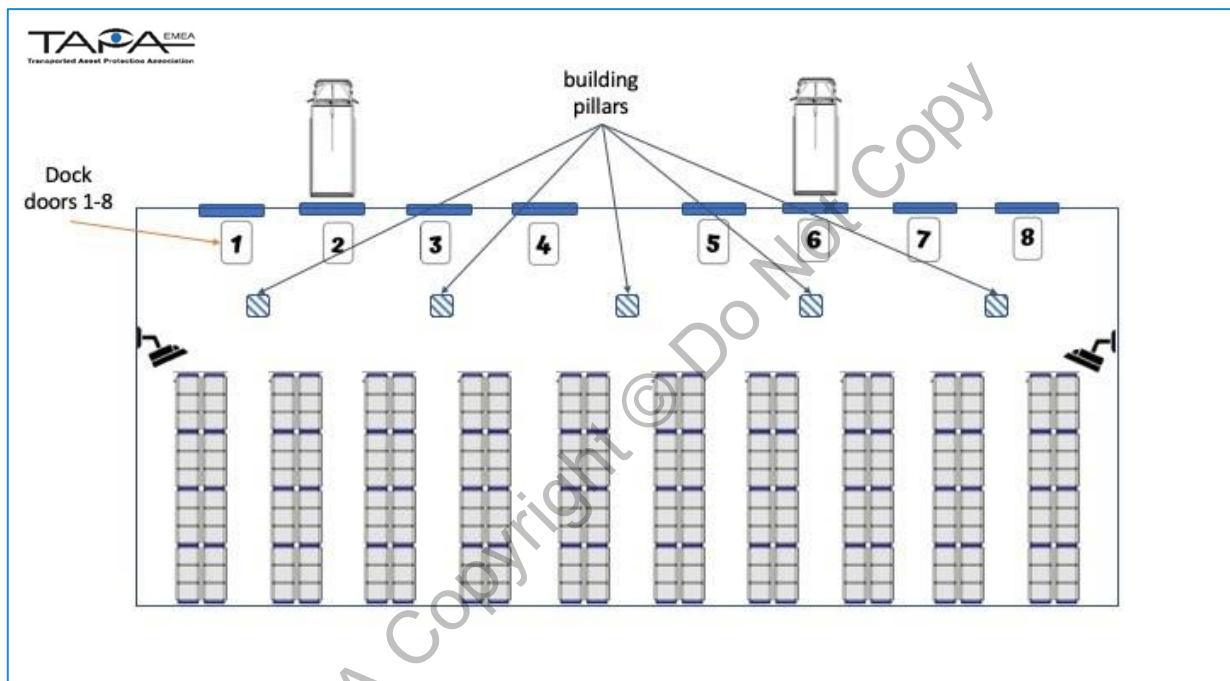
As a simple example, instead of stating that you want a resolution of 1280 x 720 pixels, you can state that you want to be able to read vehicles' license plates at a specific entry/exit point of your facility. Another functional requirements statement might be that you want to view all activities inside the shipping and receiving yard of your warehouse, which is quite large) but unfortunately, you cannot install cameras close to the fence as there are no poles that the cameras can be installed at. This will probably require the cameras to be installed on the warehouse walls and be able to view at a significant distance. By stating these functional requirements, your supplier needs to:

- Visit the location to identify what area needs to be covered (field of view – FOV)
- Decide how many cameras shall be installed and where they shall be installed to avoid any blind spots
- Decide what type of cameras shall be installed (dome, bullet, PTZ, IP, Thermal, Covert, etc.)
- Decide the required resolution and image quality (e.g. analogue, 720P, 1.3MP, 1080/2MP, 4MP, 8MP/4K)

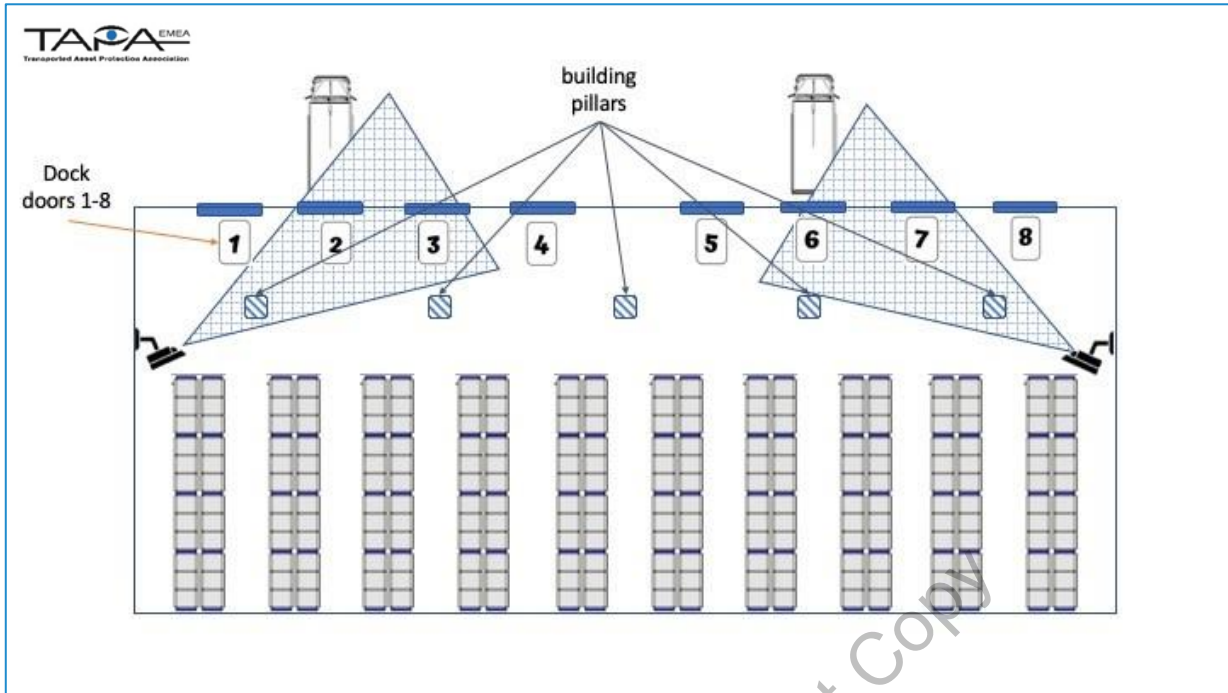
- Select the proper lens (e.g. narrow angle, 22mm, 16mm, 12mm, 6mm, or wide angle)
- Select whether the system should have night vision and/or low-light performance
- Design the connectivity and storage setup

It is very important to ensure that the Field of View (FOV) is accurately depicted on your CCTV installation drawings and that any blind spots are clearly identified when it comes to coverage evaluation.

In the picture below, you can see a typical part of a warehouse's dock doors area that needs to be covered internally by CCTV. In our example, consider that we need to cover the internal dock area in front of the docks numbered 2, 3, 6, and 7.



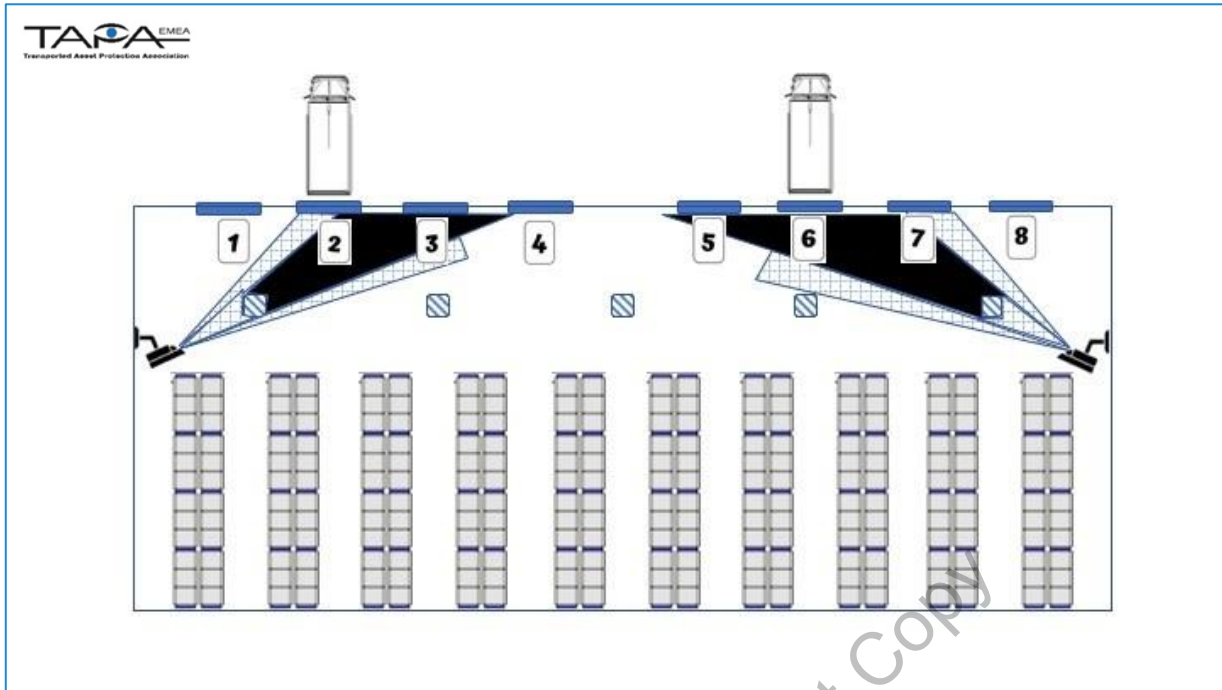
Your installer prepares for you a proposal that includes the installation of two cameras at the locations shown in the picture below and shows also the coverage diagram, that initially looks like it satisfies your requirement.



But if you look deeper, you can realize that three factors affect the Field of View of the above installation setup:

- a. The building pillars that are very common in warehouse constructions constitute physical obstacles that prevent the coverage of the cameras behind the pillars.
- b. The Field of view of the selected cameras is not enough to cover effectively the distance between the cameras and the dock doors.
- c. Finally, it is evident that the cameras cannot view the area externally of the warehouse behind the warehouse's external wall.

You can see the actual Field of View (FOV) as well as the blind spots from this installation setup in the picture below. You can realize that the Field of View is significantly smaller than the one considered initially.



Therefore, it is strongly recommended when evaluating the Field of View of cameras to investigate whether there are blind spots related bot to the window coverage as well as the distance range where you want these cameras to cover.

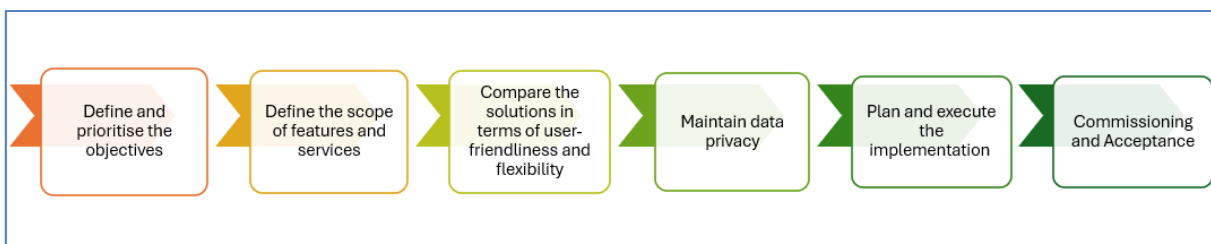
7. How to find the right CCTV/VSS solution?

The demands on modern logistics processes are constantly increasing. In addition to greater safety on the premises, process optimization is at the top of the list of priorities in many places. For example, service quality and thus customer satisfaction must be increased, costs must be controlled effectively, and the criteria for industry certifications must be met. One of the key factors is the type of video system that companies use for their facilities. The market offers very different solutions here - from pure video surveillance to multifunctional video management systems. The following five steps help companies streamline the selection process and find the right solution for their needs.

Modern software combined with high-quality optical hardware offers a wide range of possible applications. Classic video surveillance systems focus on the issue of security. In contrast, some solutions go beyond theft prevention and enable comprehensive image-controlled process management in the hall. Selecting the right video system from the wide range of available solutions with very different specifications is not a trivial task.



With the following six steps, companies can speed up the selection process and take into account all relevant aspects:



Below you can find some additional information for each step presented above.

Step 1: Define and prioritize the objectives

First, define the overall business goals you want to achieve with the help of the video system:

- Do you want to permanently increase the level of security on the premises?
- Are you aiming at greater customer satisfaction and thus remaining competitive in the long term?
- Or is the focus set on increasing the quality of services and improving your company's reputation?

The operational goals result from the strategic goals. The latter are actual process optimizations that contribute to the achievement of a strategic goal. Record your operational goals in detail and prioritize them. It makes sense to initially tackle two to three goals. The subsequent goals should also be considered according to their priority when comparing the systems. It is important to ask in which areas the software is to be used and what improvements should result from it:

- Is your goal to find missing shipments faster?
- Do you strive for clearly documented transfer of liability?
- Are you looking to sustainably reduce the loss ratio?

Step 2: Define the scope of features and services

The corresponding must-have and can-have features of the video solution are derived from the objectives defined in the first step. A central criterion here is also the degree of digitization:

- Which interfaces need to be in place to integrate the video system with all relevant data sources - such as shipping software, merchandise management system, and databases?
- Is the video solution capable of processing large amounts of data securely and delivering it fast for retrieval?

In addition to looking at the features, it is important to compare the providers in terms of support and experience:

- To what extent should the company's own IT department take over software administration and where is support from the service provider required?
- Do the providers in question have references that demonstrate their experience in similar use cases?

Step 3: Compare the solutions in terms of user-friendliness and flexibility

Logistics is a fast-paced industry. To keep operations running smoothly, employees must grow familiar with the new solution quickly. The effort required for familiarisation should be as low as possible. The following questions will give you an impression of usability:

- Is the video management software designed to be user-friendly and can the various modules and functions be accessed intuitively? For example, is it easy to find the image recordings of a particular shipment - even without knowing the individual camera positions?
- How extensive and practical are the display and processing options for the image material (e.g. full screen and zoom, 360-degree view, data export)?
- Can repeating work steps, such as the search for missing shipments, be seamlessly integrated into existing workflows?

The expandability of the functional scope cannot be underestimated as a criterion. Modular systems offer sufficient room for adjustments in response to changing conditions. The system should be ready for flexible expansion with additional features, such as scanner location, data analyses for process optimization, etc. In this way, companies can quickly adapt their solution to new requirements.

Step 4: Maintain data privacy

Compliance with data protection regulations in the facility has been a topic not only since the GDPR (Basic Data Protection Regulation). The requirements for a video solution range from legally mandatory storage periods to safeguarding employee rights when recording and processing the video material. If logistics companies also want to have their services certified according to national and international security standards such as TAPA & AEO the video system must also meet the corresponding criteria. To be GDPR-compliant, providers should be able to answer the following questions, among others, with yes:

- Is the system protected from tampering and interference at all times?
- Is the user administration password-based? Are there individual authorization levels to control access to certain data?
- Can the image data be hosted on the company's server?
- If it is a cloud solution: Does the provider take comprehensive measures to ensure that the information is protected from unauthorized access?

In the event of an evidentiary situation, the video system should also be able to provide recordings of the facility that can be used in court.

Step 5: Plan and execute the implementation

The budget and the implementation period play a central role in the cost-benefit assessment. To ensure that the switch to the new solution runs smoothly, it is important to coordinate closely with the provider and plan precisely together. To avoid downtime, the installation should be able to take place during ongoing operations. Even with the most thorough preparation, however, unforeseen hurdles sometimes arise. That's why the provider should continue to guarantee fast support in the first few weeks after going live. Ask targeted questions already during the selection phase:

- Is it possible to implement the video system during operation?
- What temporary limitations on operational processes can be expected during this time?
- Do you have an assigned contact person throughout the planning and implementation?
- Is the support easy to reach and which response times are guaranteed?
- Which options are available for support, consulting, and supervision after implementation?

Once these points have been clarified, you will already have a concrete idea of how the introduction of the video solution will take place - and have sufficient planning certainty for the project.

Step 6: Commissioning and Acceptance

The commissioning of the installed CCTV/|VSS system is the full responsibility of the installer/supplier. During this process, the following activities should be covered in general:

- Installation of the CCTV software and ensure communication among all components
- Configuration and parameterization of the CCTV components
- Ensure all alarms are properly generated with suitable sensitivity
- Setup the users at all levels

For acceptance it is strongly recommended to focus on both technical and functional requirements. The best practice is to have a pre-agreed list of acceptance criteria (the FSR requirements can be used for this purpose) as far as the functional tests are concerned and be supported by a properly qualified in-house technician (either electrician or network technician) to check and confirm proper installation of the cables and the equipment.

Warranty and maintenance issues should also be addressed before completing the acceptance process.

8. Useful links

TAPA Members - Security Service Providers (CCTV/VSS systems)

- <https://www.bettinivideo.com/EN/>
- <https://en.g4stelematix.com/secure-supply-chain>
- <https://www.genetec.com>
- <https://shop.geutebrueck.com/>
- <https://info.geutebrueck.com/en/supply-chain-security-tapa>
- <http://www.multiprotexion.com>
- <https://www.axis.com/products/>
- <https://www.divis.eu/en/>
- <https://e-dentic.fr/>

Information on CCTV/VSS

- Video Security & Access Control Systems – Motorola:
https://www.motorolasolutions.com/en_xu/video-security-access-control.html
- Understanding CCTV Components: The Parts Every System Requires:
<https://www.gensecurity.com/blog/understanding-CCTV/VSS-components-the-4-parts-every-system-requires>
- CCTV (closed circuit television):
[https://www.techtarget.com/whatis/definition/CCTV/VSS-closed-circuit-television#:~:text=CCTV/VSS%20\(closed%2Dcircuit%20television\),for%20surveillance%20and%20security%20purposes.](https://www.techtarget.com/whatis/definition/CCTV/VSS-closed-circuit-television#:~:text=CCTV/VSS%20(closed%2Dcircuit%20television),for%20surveillance%20and%20security%20purposes.)
- CCTV Glossary of Terms: <https://ellipsesecurity.com/2019/05/CCTV/VSS-glossary-of-terms/>
- CCTV Glossary:
http://www.pfn.ir/editor/uploadfiles/tabshow/pic/solutions/CCTV/VSS_glossary.pdf
- HD COMPARISON VIDEOS: <https://www.CCTV/VSSsecuritypros.com/hd-comparison-videos/>
- What Are the Different Types of CCTV Camera?:
<https://www.caughtoncamera.net/news/different-types-of-CCTV/VSS/>
- A comparison of CCTV technologies: <https://www.its.com.au/comparison-CCTV/VSS-technologies>
- CCTV Camera 2, 5 and 8 Megapixel (4K) comparison:
<https://www.youtube.com/watch?v=kjUa0UjZBYQ>
- IP CAMERA COMPARISON CHART:
<https://www.anixter.com/content/dam/Suppliers/Hikvision/IPC-Comparison-Chart-Jan-2019.pdf>

- Understanding CCTV Storage Requirements: <https://www.securitysolutionsmedia.com/2019/02/26/understanding-CCTV/VSS-storage-requirements/>
- Surveillance Storage Capacity Estimator Tool: <https://www.westerndigital.com/tools/surveillance-capacity-calculator>
- CCTV Storage Calculation: Formula & Storage Saving Tips: <https://reolink.com/blog/CCTV/VSS-storage-calculation-formula/>
- NPSA - CCTV: <https://www.cpni.gov.uk/CCTV/VSS>
- CCTV within the workplace: [20200203 CCTV/VSS in the Workplace.pdf \(cpni.gov.uk\)](#)
- CCTV within the perimeter of a site: <https://www.cpni.gov.uk/system/files/documents/a9/3b/20200203%20CCTV/VSS%20within%20the%20Perimeter%20of%20a%20Site.pdf>
- CCTV for Perimeter Security guidance: <https://www.cpni.gov.uk/resources/CCTV/VSS-cni-perimeter>
- Frames per second visual app: <https://frames-per-second.appspot.com/>
- Frame Rate: A Beginner's Guide: <https://www.techsmith.com/blog/frame-rate-beginners-guide/>









The following products, solutions, and mentioned Security Service Providers are only suggestions to assist in compliance with our TAPA FSR standards. It is important to note that TAPA assumes no responsibility for the incorrect selection, faulty installation, non-conformity, or non-fulfillment of the chosen CCTV/ VSS solution concerning the FSR levels. Additionally, TAPA does not guide which CCTV/ VSS solution would be preferable for each FSR security level. The following data and information are based on descriptions and visual material provided by TAPA Security Service Providers. The appropriate CCTV/ VSS solution and associated installation are to be agreed upon between the user and the supplier. TAPA acts solely as a supporter and facilitator in the selection of the designated CCTV/ VSS solution.

9. Appendix A: CCTV/ VSS Systems Examples

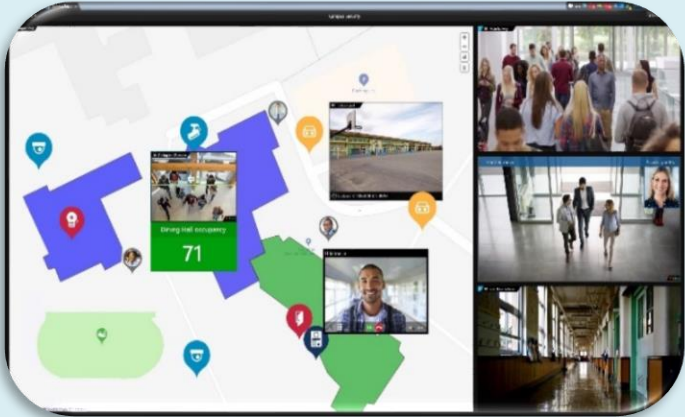


Ref	Product	Description
CSG-01.1	GAMS by BETTINI - Video Surveillance Made in Italy	GAMS – 360° solutions for video surveillance designed and manufactured in Italy by Bettini.
		 https://www.bettinivideo.com/EN/
CSG-01.2	Artificial Intelligence Video Analytics	Gams provides a wide selection of NVRs, DVRs, Workstations, and Servers for video professional Surveillance systems with complex and wide infrastructures. Privacy Compliance and Cyber Security are guaranteed.
		 https://www.bettinivideo.com/EN/
CSG-01.3	DETECTA-MADE IN ITALY - AI	Gams Neura is the new Video Analytics solution powered by Artificial Intelligence. NEURA is an innovative solution which allows any video surveillance device to perform AI powered video analysis. Using Neura, both new and existing video systems can automatically recognize events (aggressive behavior, man down...) and specific objects categories (people, types of vehicles, animals, potentially dangerous objects...). This classification feature improves real-time event management operations and minimizes false alarms.
		 https://www.bettinivideo.com/EN/






<p>CSG-01.4</p>	<p>LOGISTICS - BVI</p>	<p>Business Video Intelligence systems are solutions that use video data from cameras to manage business processes (for example in Logistics, Finance, Retail, etc.). They can generate a new database by extracting and combining the event data from the images of a video system and information contained in management and ERP software.</p>	  <p>https://www.bettinivideo.com/EN</p>
<p>CSG-01.5</p>	<p>Video Cameras</p>	<p>Gams offers a wide range of IP cameras of many different types and resolutions. Bullet, minidome, speed dome, panoramic, fisheye, multisensor, and thermal cameras are useful for any application.</p>	  <p>https://www.bettinivideo.com/EN/</p>
<p>CSG-01.6</p>	<p>Bettini Services</p>	<p>CONSULTING, DESIGN AND SALES ENGINEERING, PRIVACY CONSULTANCY, TESTING AND CONFIGURATION OF SYSTEMS, ON-SITE SUPPORT AND SYSTEM, START-UP, AFTER-SALES TECHNICAL ASSISTANCE, REPAIR SERVICE, GSP: GAMS SERVICE PACK – EXTENDED WARRANTY AND OTHER ADVANTAGES</p>	  <p>https://www.bettinivideo.com/EN</p>
<p>CSG-02.1</p>	<p>CCTV & SOFTWARE</p>	<p>Video Surveillance is at the heart of any integrated security programme. G4S has many years of experience in specifying, installing, and supporting commercial CCTV for high security applications.</p>	  <p>https://en.g4stelematix.com/secure-supply-chain</p>





<p>CSG-02.2</p>	<p>IP CAMERAS</p>	<p>IP cameras are the backbone of any modern video system. Using digital technology, they allow you to adopt a smarter approach to security by using analytics to evaluate video in real-time and alert to suspicious activity.</p>	  <p>https://en.g4stelematix.com/secure-supply-chain</p>
<p>CSG-02.3</p>	<p>REMOTE CCTV MONITORING</p>	<p>Real-time video surveillance provides a permanent “eyes on your premises”. Ensuring the surveillance facility delivers an appropriate service and avoids wasted expenditure can be a real challenge.</p>	  <p>https://en.g4stelematix.com/secure-supply-chain</p>
<p>CSG-02.4</p>	<p>VIDEO ALARM VERIFICATION</p>	<p>False alarms are a real nuisance. They disrupt neighbouring properties and leave staff following up false alarms. A fast, efficient process for handling video surveillance alerts is critical to minimise disruption and identify real emergencies.</p>	  <p>https://en.g4stelematix.com/secure-supply-chain</p>
<p>CSG-02.5</p>	<p>VIDEO ANALYTICS</p>	<p>Monitoring CCTV systems can be very time-intensive and costly to ensure that alarms and escalating situations are not missed at any time. In addition, it can be very staff intensive due to the regular rotation of operators required on any shift.</p>	  <p>https://en.g4stelematix.com/secure-supply-chain</p>

<p>CSG-02.6</p>	<p>RAPID & TEMPORARY SURVEILLANCE</p>	<p>Securing sites left vacant at short notice and monitoring outdoor spaces around the clock are real challenges. Our range of rapid deployment CCTV Towers are available temporarily at short notice and provides the platform for 24*7 surveillance.</p>	  <p>https://en.g4stelematix.com/secure-supply-chain</p>
<p>CSG-02.7</p>	<p>SURVEILLANCE</p>	<p>Automation and technology enhancements have made drone technology a reality. Whether it is perimeter or external inspections, a visible criminal deterrent or replacing physical patrols, drones have a role to play.</p>	  <p>https://en.g4stelematix.com/secure-supply-chain</p>
<p>CSG-02.8</p>	<p>ANPR SOLUTIONS</p>	<p>Automatic Number Plate Recognition can be an integral part of an integrated security system.</p>	  <p>https://en.g4stelematix.com/secure-supply-chain</p>
<p>CSG-02.9</p>	<p>ADVANCED DRIVER ASSISTANCE SYSTEMS</p>	<p>Improve driver safety in real-time through optional in-cab coaching in high-risk situations such as yawning, smoking, distraction, phone call, no seatbelt, and more, helping drivers practice safe driving habits.</p>	  <p>https://en.g4stelematix.com/secure-supply-chain</p>









<p>CSG-02.10</p>	<p>VEHICLE CAMERAS</p>	<p>From vandal-proof cameras to anti-explosion cameras, from indoor cameras to outdoor cameras which are tested with up to IP68 protection level, they all provide the best image quality for choices of different requirements.</p>	  <p>https://en.g4stelematix.com/secure-supply-chain</p>
<p>CSG-02.11</p>	<p>CCTV MAINTENANCE</p>	<p>Our systems are only as good as we maintain them. Here is a case study on how we maintain 230 IP & legacy analogue CCTV cameras across 5 sites.</p>	  <p>https://en.g4stelematix.com/secure-supply-chain</p>
<p>CSG-02.12</p>	<p>TRANSITION FROM ANALOG TO IP CAMERAS</p>	<p>Migrating to an intelligent IP based platform whilst securing zero downtime is challenging. Here is a case study on how we migrated to new tech within the constraints of a demanding environment.</p>	  <p>https://en.g4stelematix.com/secure-supply-chain</p>
<p>CSG-02.13</p>	<p>CYBERSECURITY SERVICES</p>	<p>Physical security & cybersecurity come together in one service.</p>	  <p>https://en.g4stelematix.com/secure-supply-chain</p>

<p>CSG-03.01</p>	<p>Security Center Omnicast™</p>	<p>Security Center Omnicast™ is an IP-based video management solution. It provides a clear overview of events, empowering you to respond quicker and make informed decisions. The solution scales easily with your needs and its flexible architecture allows you to benefit from a constantly evolving ecosystem of hardware and analytics technologies. Omnicast is part of our Genetec™ Security Center platform, making it easy to unify video with access control, intrusion, comms, and more. With a smarter approach to video, Omnicast helps you protect the everyday.</p>  <p>Genetec™</p> <p>https://www.genetec.com</p>
<p>CSG-04.1</p>	<p>CCTV cameras and accessories</p>	<p>Complete camera range of CCTV cameras for all types of applications, form factors, resolutions and mounting variants from indoor or outdoor to thermal imaging</p>  <p>GEUTEBRÜCK</p> <p>https://info.geutebrueck.com/en/supply-chain-security-tapa</p>
<p>CSG-04.2</p>	<p>CCTV servers and appliances</p>	<p>Complete range of servers and workstations for CCTV application with configurable HDD capacity and RAID level protection.</p>  <p>GEUTEBRÜCK</p> <p>https://info.geutebrueck.com/en/supply-chain-security-tapa</p>

<p>CSG-04.3</p>	<p>Video Management Software</p>	<p>Video Management Software for professional CCTV applications with a wide range of video analytics, third-party interfaces and logistics specific options. Court acceptance and GDPR compliance through specific integrity features.</p>
		<p>GEUTEBRÜCK</p>
<p>https://info.geutebrueck.com/en/supply-chain-security-tapa</p>		
<p>CSG-04.4</p>	<p>Video Analytics Options</p>	<p>Classical and AI-based video analytics for perimeter security Rule-based video analytics for loitering, occupancy, tailgating, and other detections OCR-based video analytics to detect vehicle license plates, container numbers, etc.</p>
		<p>GEUTEBRÜCK</p>
<p>https://info.geutebrueck.com/en/supply-chain-security-tapa</p>		
<p>CSG-04.5</p>	<p>Integrated Solutions</p>	<p>Readily available interfaces for various scanner types and systems. Mobile Scanner Integration together with Android application and indoor positioning system. Advanced experience in customizing interfaces.</p>
		<p>GEUTEBRÜCK</p>
<p>https://info.geutebrueck.com/en/supply-chain-security-tapa</p>		
<p>CSG-05.1</p>	<p>CCTV Cameras Axis, Avigilon, Arecont, American Dynamics, Bosch, Dahua, Dallmeier, HikVision, Honeywell Etc</p>	<p>Video compression with H.264, H.265 and MJPE/MPEG, 30 FpS and more, multiple lens options, able to work with Ultra-Low-Light or Ultra-Backlight, HDTV 1080p or 4K, WDR Forensic Capture, up to 20 Privacy Masking Zones, from IP67, I68Ex to IP69, ONVIF Compliant, adaptive IR Beams, Audio Capabilities, Varios Layouts: 360 Deg, PTZ, Thermal, Domes, Box, Bullet,</p>
		
<p>http://www.johnsoncontrols.com</p>		







<p>CSG-05.2</p>	<p>Servers Dell, HP, Fujitsu, Lenovo</p>	<p>up to 4 Sockets per Server Memory: (96 DIMMS): 8GB/16GB/32GB/64GB/128GB RDIMM, LRDIMM up to 2400 MT/s Storage: 2.5" SATA/SAS SSD, SAS HDD (15K, 10K), nearline SAS HDD (7.2K) 2.5" Dell PowerEdge NVMe Express Flash PCIe SSD</p>	 <p>Johnson Controls</p> <p>http://www.johnsoncontrols.com</p>
<p>CSG-05.3</p>	<p>Switches Cisco, Netgear, HP, Zyxel, Ubiquiti</p>	<p>32 x 100G QSFP28 ports Wire-speed, ultra-low latency switching Supports Open Network Install Environment (ONIE) for zero-touch installation of network OS SDN-enabled with OpenFlow 1.3 support Dual AC/DC hot-swappable power supply modules for 1+1 redundancy and load sharing</p>	 <p>Johnson Controls</p> <p>http://www.johnsoncontrols.com</p>
<p>CSG-05.4</p>	<p>UPS APC, Bluewalker</p>	<p>Output Power Capacity: 1.0k Watts / 1.5 kVA Output Connections: (2) IEC Jumpers (Battery Backup) (8) IEC 320 C13 (Battery Backup) Nominal Output Voltage: 230 Volt Nominal Input Voltage: 230 Volt Cold-Start-Capability, Green Mode, Intelligent Card Slot, LCD Interface, Predictive replace battery date, Temperature-compensated battery charging.</p>	 <p>Johnson Controls</p> <p>http://www.johnsoncontrols.com</p>
<p>CSG-05.5</p>	<p>Software Axis, Avigilon, Bosch, Briefcam, Cisco Meraki, ExacqVision, Genetec, Heitel, Honeywell, Milestone etc.. ,</p>	<p>Parcel-Tracking, DWS-Integration (Dimensioning, Weighing, Scanning), Deep Barcode Scanner Integration, Conveyor-Belt-Connectivity, X-Ray Integration, RFID- Integration and Integration with Picking-Systems, Cloud- based solution available, Cyber-proof, AI-ready</p>	 <p>Johnson Controls</p> <p>http://www.johnsoncontrols.com</p>

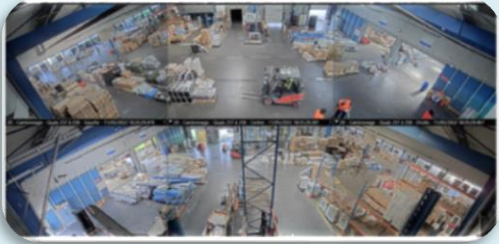





<p>CSG-06.1</p>	<p>ET01 SOLAR TOWER</p>	<p>ET01 is a mobile station of active video surveillance completely autonomous, equipped with 4 thermal cameras with A.I. and a VOIP kit. Equipped with 3 integrated solar panels and an ingenious folding system, which allows the optimal absorption of solar energy, the system is combined with high-efficiency batteries that guarantee a long autonomy.</p>
		  <p>http://www.multiprotection.co</p>
<p>CSG-07.1</p>	<p>AXIS P56 PTZ Camera Series</p>	<p>AXIS P5655-E PTZ Network Camera is a cost-effective high performance PTZ camera for versatile surveillance. Thanks to the newest generation of Axis chip, it offers excellent video quality, even in the most challenging light conditions, and a high level of defense to protect your system. It's ideal for deterrent surveillance of large outdoor and indoor areas and provides great details when zooming in</p>
		 <p>https://www.axis.com/products/axis-p56-series</p>
<p>CSG-07.2</p>	<p>AXIS M55 PTZ Camera Series</p>	<p>AXIS M5525-E is a versatile camera for indoor or outdoor use, compatible with all Axis PTZ mounts. It offers two-way audio and four digital I/O ports for integration with other</p>
		 <p>https://www.axis.com/products/axis-m55-series</p>
<p>CSG-07.3</p>	<p>AXIS Q1951-E Thermal Camera</p>	<p>AXIS Q1951-E delivers a high-quality thermal video stream 24/7, in all weather, and any light conditions. Ideal for perimeter security and long-range detection, it captures events taking place at great distances. With four lens alternatives (7 mm, 13mm, 19 mm and 35 mm), the network camera can optimize detection performance to meet most application requirements. Thanks to electronic image stabilization</p>
		 <p>https://www.axis.com/products/axis-q19-series</p>

<p>CSG-07.4</p>	<p>AXIS Q2101-TE Thermal Camera</p>	<p>AXIS Q2101-TE lets you remotely monitor temperatures over large areas— automatically or manually with just one camera. It can monitor temperatures from -40 °C to 350 °C (-40 °F to 660 °F) with several trigger types such as lowest and highest temperature or temperature gradient. When mounted on a positioning unit (sold separately), this robust camera provides a 360° unobstructed field of view. This also enables a thermometric guard tour with support for up to 256 presets with 10 polygonal detection areas each. Spot temperature reading acts as a visual aid and lets you see the exact temperature in a specific area</p>
		 <p>https://www.axis.com/products/axis-q2101-te</p>
<p>CSG-07.5</p>	<p>AXIS P13 Box Camera Series</p>	<p>AXIS P1375-E is designed to be reliable under rough conditions and in harsh climates. It can withstand extreme temperatures ranging from -40 °C to 60 °C (-40 °F to 140 °F). Its IP66-, IP67-, IK10- and NEMA 4X-rated casing protects it against water, corrosion and dust. Furthermore, AXIS P13 Weathershield Extension A is available for extreme protection against snow or rain and to prevent reflections. The innovative design of the AXIS P1375-E makes it easy to access connectors and cables, so installation is quick and efficient. The built-in camera rails allow you to easily adjust or change the lens to a larger tele lens (up to 12 cm) or i-CS lens.</p>
		 <p>https://www.axis.com/products/axis-p13-series</p>
<p>CSG-07.6</p>	<p>AXIS M20 Bullet Camera Series</p>	<p>Ideal for tough environments, this outdoor-ready bullet-style camera offers affordable Axis excellence. Lightweight and compact in design, it's easy to install and supports analytics with deep learning. Available in two lens alternatives.</p>
		 <p>https://www.axis.com/products/axis-m20-series</p>
<p>CSG-07.7</p>	<p>AXIS P14 Bullet Camera Series</p>	<p>This robust, outdoor-ready camera is ideal for a variety of surveillance scenarios. Available with a wide or tele lens, it offers excellent image quality, advanced analytics based on deep learning on the edge, and built-in cybersecurity features.</p>
		 <p>https://www.axis.com/de-de/products/axis-p14-series</p>

CSG-07.8	<p>AXIS M32 Dome Camera Series</p>	<p>AXIS M3215-LVE offers excellent 2 MP resolution and ensures high-quality images around the clock and in any light conditions. It features Axis Lightfinder for sharp color images in low light and with Axis Forensic WDR you get clarity even when there are both dark and light areas in the scene. Plus, Axis OptimizedIR enables surveillance in total darkness up to 30 m (98 ft) or more depending on the scene. Furthermore, Axis Zipstream with support for H.264 and H.265</p>
		 <p>https://www.axis.com/products/axis-m32-series</p>
CSG-07.9	<p>AXIS M32 Dome Camera Series</p>	<p>AXIS P3265-LV delivers outstanding image quality and forensic details in 2 MP. Including a varifocal 9 mm lens for wide-area surveillance, it offers a field of view of 100-36 degrees and up to 60 fps at full frame rate. Thanks to Lightfinder 2.0 and Forensic WDR, it delivers true colors and great detail in challenging light or near darkness. And, with OptimizedIR, you'll enjoy sharp and clear footage in complete darkness up to 40 m (130 ft) without the need for extra lighting.</p>
		 <p>https://www.axis.com/products/axis-p32-series</p>
CSG-07.10	<p>AXIS M43 Panoramic Camera Series</p>	<p>AXIS M4328-P offers a complete overview with outstanding sharpness, great detail, and no blind spots. This 12 MP camera delivers 360° or 180° panoramic overviews. It includes Axis Lightfinder and Axis Forensic WDR for true colors and great details in challenging light or near darkness. With its stereoscopic lens and digital PTZ, this panoramic camera enables improved image processing and great image quality.</p>
		 <p>https://www.axis.com/de-de/products/axis-m43-series</p>
CSG-07.11	<p>AXIS P37 Panoramic Camera Series</p>	<p>AXIS P3735-PLE offers four channels with 2 MP per channel at 30 fps letting you capture both wide-angle and zoomed-in, detailed views. It includes day/night functionality and 360° IR illumination with individually controllable LEDs and a removable IR cut filter. So, you'll enjoy clear, reflection-free footage and excellent image quality even in low light or complete darkness</p>
		 <p>https://www.axis.com/products/axis-p3737-ple</p>

<p>CSG-07.12</p>	<p>AXIS M5000-G PTZ Camera</p>	<p>AXIS M5000-G offers total situational awareness of indoor areas up to 400 m2 (4300 ft2). Featuring three 5 MP sensors and one PTZ camera with 10x optical zoom and HDTV 1080p, it lets you benefit from sweeping overviews and you can zoom in to get the details. With everything displayed on one monitor, you can move from overview to detailed views in a single click. And, with autofocus capabilities, you can quickly zoom in on areas of interest. Furthermore, it features indication lights to help deter antisocial and criminal behavior, ideal for retail stores and large indoor areas.</p>
		 <p>https://www.axis.com/products/axis-m5000-g</p>
<p>CSG-07.13</p>	<p>AXIS Perimeter Defender</p>	<p>AXIS Perimeter Defender reinforces physical access controls to give you an edge where security starts – at the perimeter of your site. Together with Axis cameras, it provides an effective edge-based system that automatically detects and responds to people and vehicles intruding on your property. When combined with thermal and PTZ cameras, it's suitable even for high-security locations</p>
		 <p>https://www.axis.com/products/axis-perimeter-defender</p>
<p>CSG-07.14</p>	<p>Network speakers</p>	<p>AXIS C1004-E Network Cabinet Speaker makes audio announcements smart and easy. Use it to proactively warn off intruders or provide instructions with voice messages. AXIS C1004-E can be mounted horizontally or vertically and it's possible to install it on the exterior of buildings, for instance under the eaves, where it's not directly exposed to the elements. It's ideal for installation in warehouses</p>
		 <p>https://www.axis.com/products/</p>
<p>CSG-07.15</p>	<p>AXIS C1310-E Network Horn Speaker</p>	<p>Deter unwanted activity and warn off bad actors detected by your cameras with smart, easy-to-integrate AXIS C1310-E Network Horn Speaker. Or use it to provide voice instructions. This rugged horn speaker is perfect for most outdoor environments in most climates.</p>
		 <p>https://www.axis.com/products/axis-network-intercoms</p>

<p>CSG-07.16</p>	<p>Axis network intercoms</p>	<p>AXIS A8207-VE MkII is three top-of-the-line security solutions in one, which eliminates the need for additional equipment around your entrances. For clear two-way communication between personnel and all visitors, it offers echo cancellation, noise reduction, and an induction loop for hearing aids. It also has an integrated access control reader (RFID) for integration with your access control system, managing employee access that allows for remote entrance control using your computer, desk phone or mobile device.</p>
		 <p>https://www.axis.com/products/axis-network-intercoms</p>
<p>CSG-07.17</p>	<p>AXIS W110 Body Worn Camera</p>	<p>Wearable cameras deter bad behavior and positively influence the public and camera wearers alike. Axis W110 Body Worn Camera brings these benefits to the workplace for sectors like logistics</p>
		 <p>https://www.axis.com/products/axis-w110-body-worn-camera</p>
<p>CSG-08.1</p>	<p>The DIVIS ecosystem includes video management software solutions for the investigation of palletized shipments in cross docks (CargoVIS) or for package tracking in CEP warehouses (ParcelVIS) as well as plus features to create a customised software solution.</p>	<p>The CargoVIS software links video data with scanning and shipment data, creating a scanning motion path enabling seamless tracking of goods, and thus replacing the conventional - often time-consuming - search for misplaced or incorrectly loaded shipments.</p> <p>The ParcelVIS software links video data, scanning, and sorting information. Once the parcel has been identified by the parcel label number, the path of a shipment can be tracked until the transfer of liability.</p> <p>Various Plus+ features enable different camera-based functions to be mapped. This unique platform fully incorporates the Plus+ features into the software solutions, eliminating the need for a multitude of stand-alone solutions.</p>
		 <p>https://www.divis.eu/en/</p>

CSG-09.1	Epyo Pallet	Video tracking pallet   https://e-dentic.fr/
CSG-09.2	Epyo Parcel	Video tracking parcel   https://e-dentic.fr/
CSG-09.3	Epyo Scan	Scan camera for Parcel and pallet   https://e-dentic.fr/

Publishing and copyright information

The TAPA EMEA copyright notice displayed in this document indicates when the document was last issued.

© TAPA EMEA 2024

No copying without TAPA EMEA permission except as permitted by copyright law.

Publication history

First published in April 2022.

The first (present) edition was published in March 2024.