Security Risk Management

Introduction

This PowerPoint introduces the essentials of organisational security risk management. It is designed for Managers operating in areas such as: Operations, Facilities, Human Resources, Compliance and Audit who have security/risk and duty of care responsibilities in addition to their core duties.

Disclaimer

The information contained in this document should be used carefully and up-to-date information sought in relation to legislation, rules, regulations and your own in-house policies and procedures.

Security Risk Management

Increasingly, corporations are turning to their facilities managers and other departmental managers, rather than dedicated security directors, to be responsible for the management of security risks affecting their organisations.

However, to be effective in this, especially given the myriad of other responsibilities facing today’s managers operating in the complex arena of the globalised marketplace, a systematic, methodical, process-driven approach that is as simple as possible, and that is based on sound principles, needs to be applied.

Security Risk Management

The material is intended for professionals with little or no security management experience, to provide them with the fundamental knowledge required to meet their security responsibilities.

Content of this learning is based on information from many national and international sources such as:-

https://www.bsigroup.com/en-GB/

https://www.asisonline.org/

https://www.iwfm.org.uk/

https://www.iso.org/home.html

https://www.security-institute.org/

Security Risk Management

Security Risk Management can be simply broken down into two parts:

1. Risk Analysis
2. 2. Risk Mitigation

Failure to conduct effective risk analysis before applying security measures is not dissimilar to a doctor prescribing medicine without first examining the patient.

For many organisations, security risk analysis is a mandatory activity which must be carried out regularly by all organisation’s units.

Risk Security Management

Probably surprising to some, the first step in effective and efficient security risk management isn’t about focusing on security.

Instead, it is to understand the organisation and where it needs to be in the future. To do this, the Manager/s must consider its long-term vision, mission and objectives.

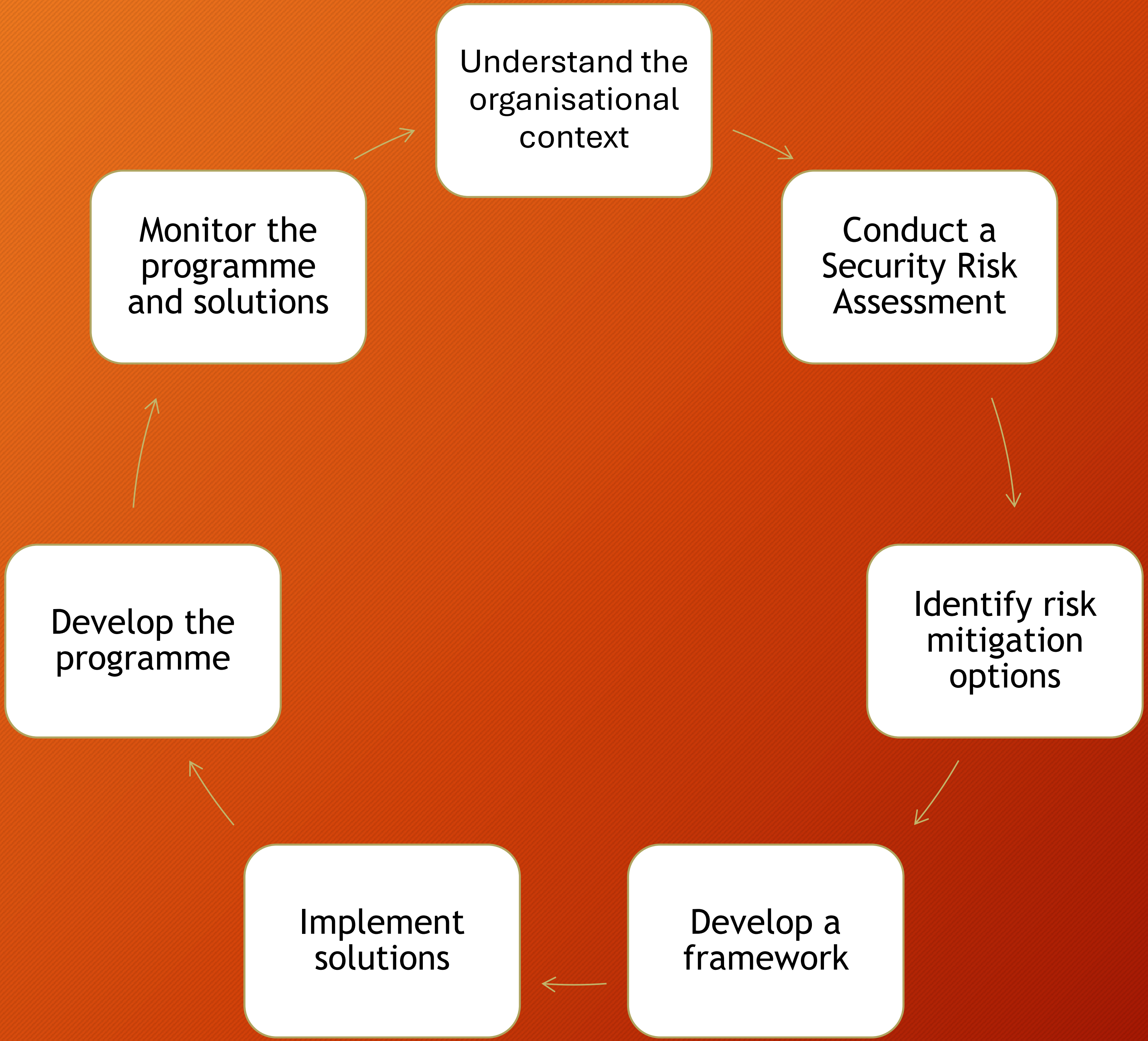
Revenue
Cost

Security Risk Management

Security measures contained within a security programme must fully support the organisations objectives.

A programme must protect company assets in a way that is commensurate with both the internal and external contexts, and risk appetite of the organisation, ensuring they are a contributor, not a cost to the bottom line.

An example of the review cycle is on the next slide.



Understand the organisational context

Conduct a Security Risk Assessment

Identify risk mitigation options

Develop a framework

Implement solutions

Develop the programme

Monitor the programme and solutions

Organisational Security

If the security function is able to demonstrate the value of security as part of the overall enterprise risk management package, rather than merely the cost of having ‘security’, it is likely management will be more supportive.

Such ‘buy-in’ will not only secure funding but will set the tone for how security is perceived by the organisation, its employees, contractors, visitors and customers.

In short, the organisational ‘security culture’ needs to be positive and proactive.

Security Culture

Promoting a positive security culture across the whole of the organisation pays dividends in terms of its overall risk management stance regarding safety, security, and organisational operations.

The bonus for those responsible for security is that the job is easier if the senior manager’s support what you are doing, implementing effective strategies becomes so much simpler.

Security Risk Management

The key to the successful implementation of any security programme is that it is approached in a systematic, methodical manner, and kept as simple as possible.

There are many processes across the world that define how ‘security’ should be implemented and managed.

For example, the ‘The Eight Layers Of Security Preparedness’.

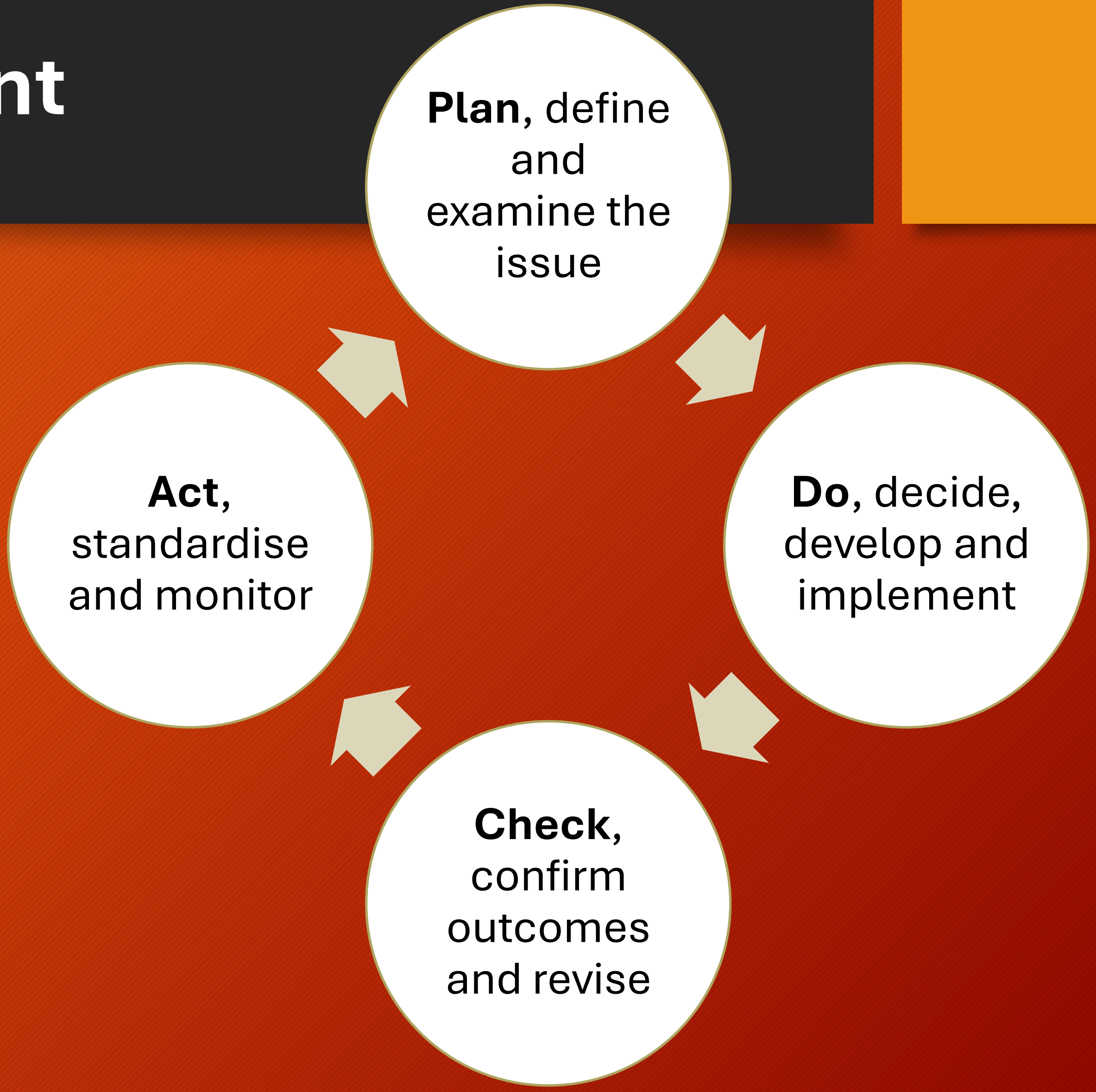
See next slide.

The Security Toolbox

1. Strategy & security policy.
2. Collect intelligence.
3. Right people to right roles.
4. Technical solutions.
5. Processes & procedures
6. Control & supervision.
7. Test & drill.
8. Internal & external audits.

Security Risk Management

Others approach security in a cyclical way, not unlike the Plan Do Check Act management methodology, which forms the basis of ISO 3100:2018.



Plan, define and examine the issue

Do, decide, develop and implement

Check, confirm outcomes and revise

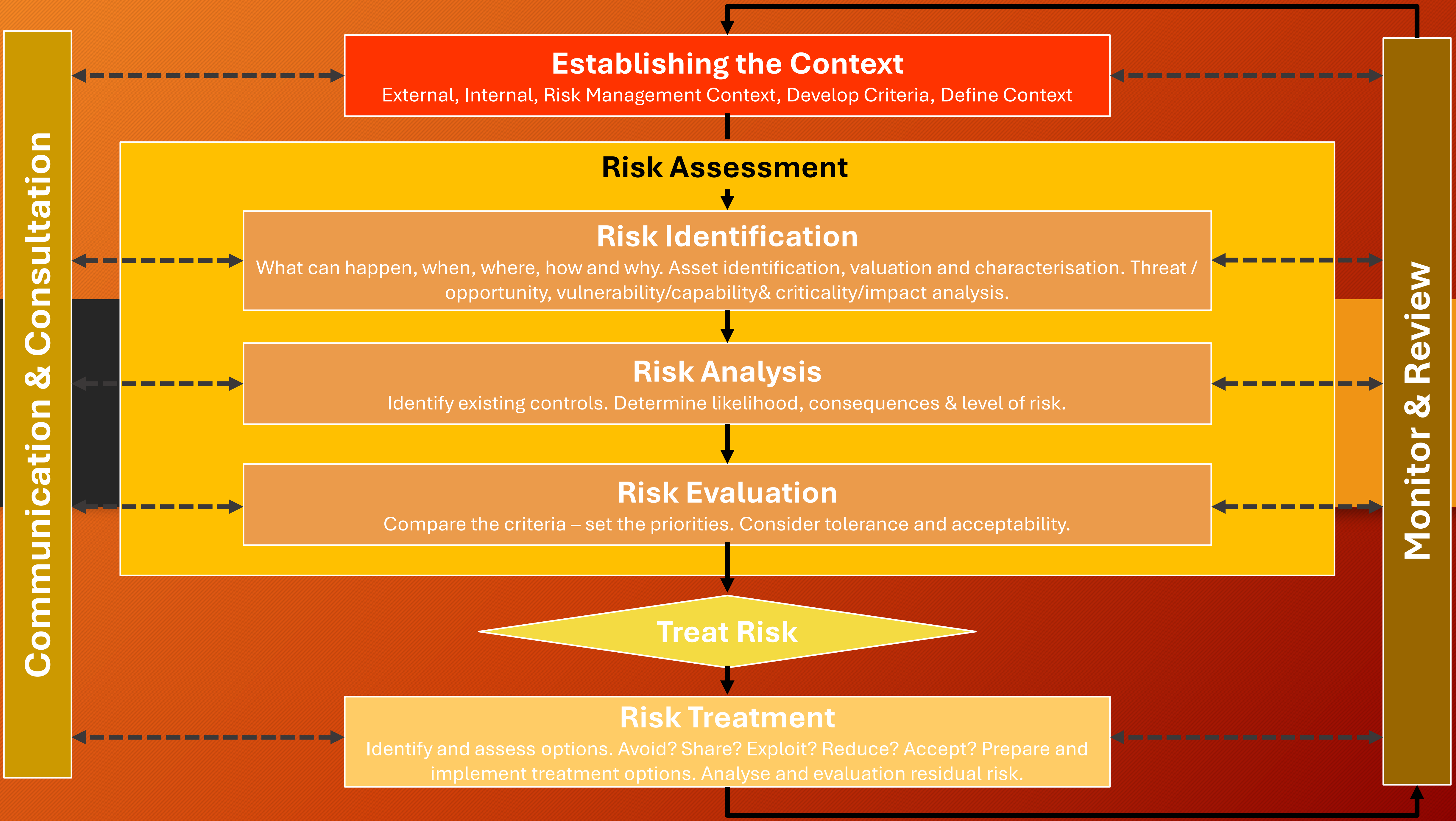
Act, standardise and monitor

Security Risk Management

It is crucial that the organisation’s security risk management policy and strategy supports that of the overall organisational strategy.

However, to contain or manage the risks, it is first necessary to effectively identify these and assess them in the context of the vision and mission of the organisation.

See next slide for process.



Communication & Consultation

Establishing the Context

External, Internal, Risk Management Context, Develop Criteria, Define Context

Risk Assessment

Risk Identification

What can happen, when, where, how and why. Asset identification, valuation and characterisation. Threat / opportunity, vulnerability/capability& criticality/impact analysis.

Risk Analysis

Identify existing controls. Determine likelihood, consequences & level of risk.

Risk Evaluation

Compare the criteria – set the priorities. Consider tolerance and acceptability.

Treat Risk

Risk Treatment

Identify and assess options. Avoid? Share? Exploit? Reduce? Accept? Prepare and implement treatment options. Analyse and evaluation residual risk.

Monitor & Review

Getting Started

We will now look, in a little more detail, at how a security programme can be developed.

- Understand the organisation
- Understand its assets
- Understand who wants to take/harm the assets
- How will they do it – where are *you* vulnerable?
- Decide on your mitigation strategy
- Develop a plan
- Implement the plan and solutions
- Make sure it works and keep checking it

Risk Identification

1. Understand the Organisation

What do they do? How do they do it? Where do they do it?

Organisation’ sector, aims, objectives, regulation, legal and safety considerations; social/political environment.

2. Understand the Assets

What is of value to the organisation? ‘Tangible’ – can it be stolen/broken? ‘Intangible’ – intellectual property, reputation. ‘Mixed’ – people. How critical are the assets to the operation?

3. Understand the Threat

Who are they? What do they want? How many? Why? How are they going to do it?

4. How are you Vulnerable?

Key assets – how are they protected, or even, are they protected at all? Physical protection? Legal protection?

Security Surveys

Before trying to implement security measures, we must understand the organisation, the threats being face, the measures in place and what we would like to have in place.

The security survey will look at the physical, political and operating environment of the organisation.

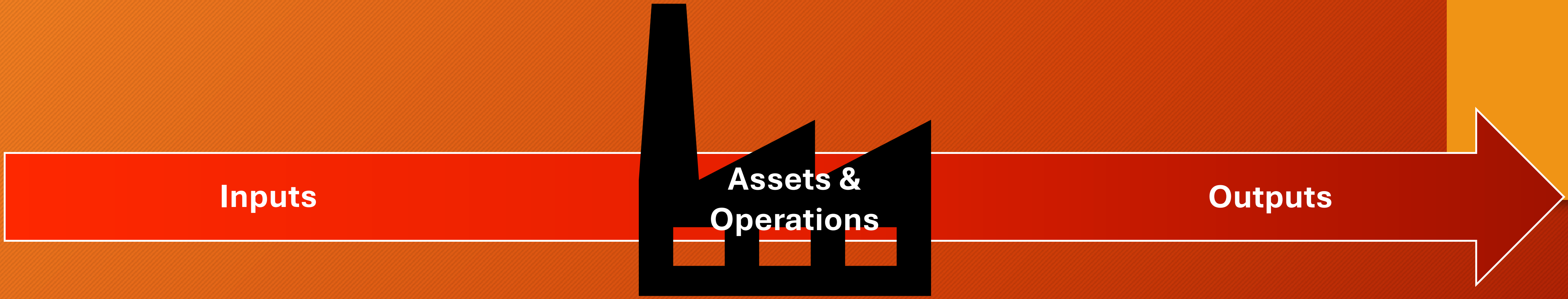
Areas will be examined such as perimeter fences, video surveillance, doors, locks, windows, goods in/out and procedures to assess whether there is adequate protection for identified assets.

Understanding Assets

The key is to understand what our assets are, the threats to them and how vulnerable they are to attack.

Characterise the assets and the context in which they exist.

Determine threats, threat sources, methods, potential targets and their vulnerability. Consider both external and internal (employee and contractor) adversaries.



Inputs

Assets & Operations

Outputs

You should protect:

People

Property / physical assets

Information

Reputation

Operational continuity

Vulnerability examples:

Theft

Violence

Trespass

Criminal damage

Information theft / loss

Counterfeiting

But also consider:

Processes

Supply chain

Organisation know how

Environment

Security Risk Assessment

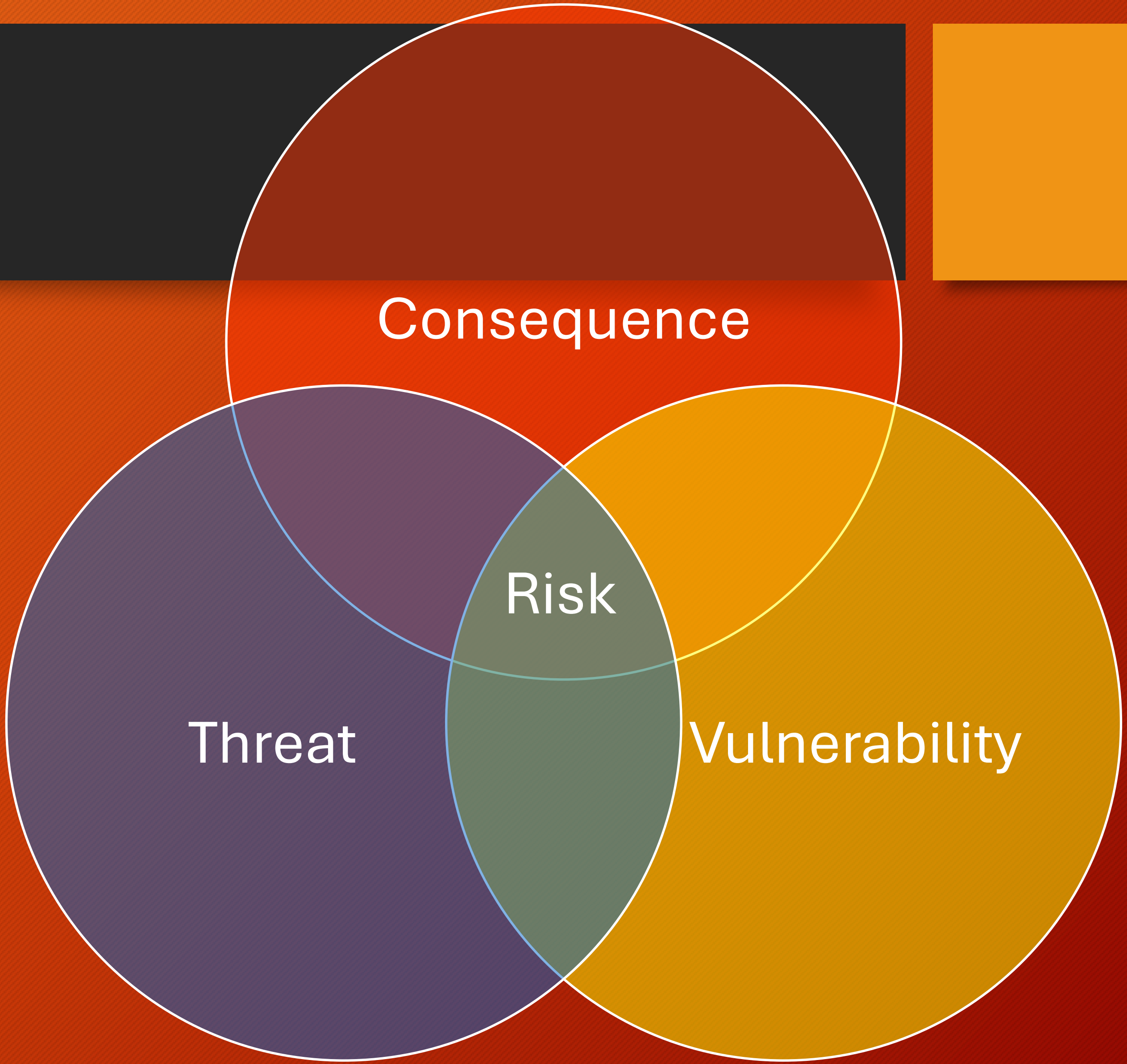
Part of the security survey will consider the relationship between the assets being protected, the threats to them, their vulnerability to the identified threats and the impact of a loss even on the organisation.

This security risk assessment phase (part of the security survey) will analyse the threat / assets pairs and allocate a risk value to them – for which mitigation measures will be designated and implemented.

(Risk – is the potential for loss or harm.)

Security Risk Analysis

Risk is a function of consequence, vulnerability and threat.



Security Risk Assessment

Of course, before any risk prevention or mitigation strategies can be implemented risk to the organisation need to be calculated.

A Security Risk Assessment should provide the necessary information to accurately identify threats, assess the likelihood of an adverse event occurring, evaluate the consequence and then to develop the most appropriate strategy to manage the risk.

The risk assessment process should comprise of three stages.

Security Risk Assessment

1. Risk Identification

- Identify threats to critical assets, weaknesses / strengths in protection, as well as identifying potential security events, and their causes.

2. Risk Analysis

- Likelihood and consequences of a risk event – provides the basis for evaluation and risk treatment during decision making.

3. Risk Evaluation

- Provides the basis for decisions on risk priorities, and risk treatment methods.

Consider your organisation, what are the threats?

Security Risk Analysis

There are three types of risk analysis:

1. **Qualitative**

- Terms used may include Severe, High, Medium and Low. This is a subjective assessment suitable for use on low value sites.

2. **Quantitative**

- The use of numbers to provide an indication of severity. This could be on a scale of 1 to 5, percentage or use mathematical formula

3. **Combined**

- A combination of the above that could be used to describe the situation to various audiences.

Security Risk Analysis

Quantitative risk analysis uses precise values for probability. An example of this could be:

- Once every 10 years or more
- Every 2 to 10 years
- Every 6 to 24 months
- Every 1 to 6 months
- More often than once a month

Conversely, **qualitative** risk analysis uses more abstract terms.

An example might be:

- Rare
- Unlikely
- Possible
- Likely
- Certain

Security Risk Analysis

For **qualitative** risk assessment we can determine likelihood and impact using 5-point scales.

This is simplistic and values can be subjective.

Probability

□ 1 - Rare

□ 2 - Unlikely

□ 3 - Possible

□ 4 - Likely

□ 5 - Certain

Impact

□ 1 - Negligible

□ 2 - Moderate

□ 3 - Serious

□ 4 - Very Serious

□ 5 - Significant

Security Risk Analysis

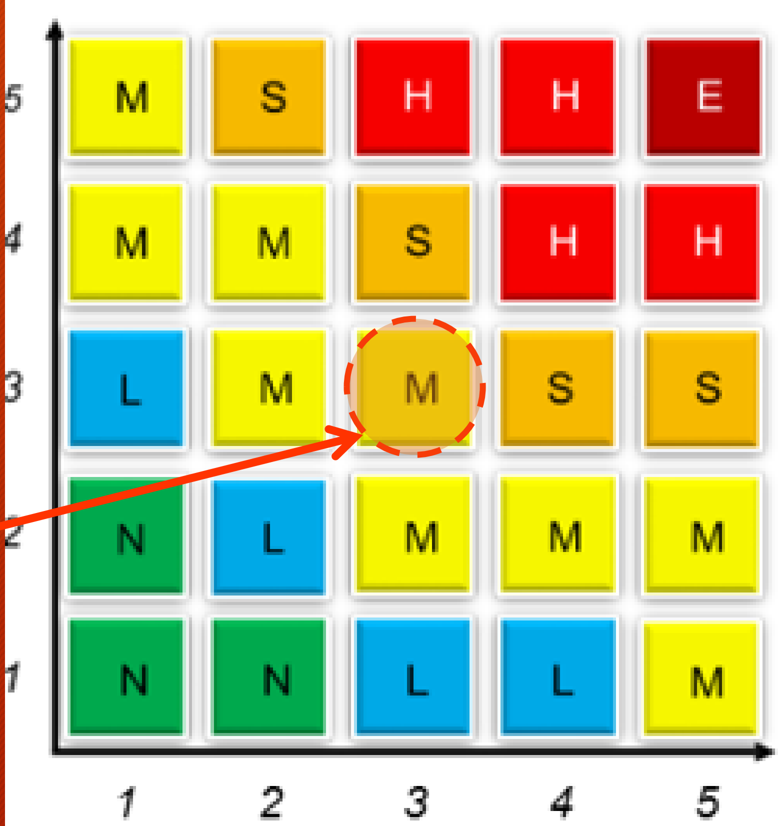
Using this scoring, we can assess a threat. If we consider burglary, the risk value can be demonstrated using **qualitative** values:

Probability of burglary (based o crime statistics, incidents, local knowledge etc) = Possible, a score of 3

Impact of burglary (based on criticality of assets) = Serious, a score of 3

To understand the risk, we need to combine these. 3x3 = Moderate

This is just one of the methods available – the 5x5 matrix. This is then measured against the controls in place, manageability or vulnerability.



Impact

5	M	S	H	H	E
4	M	M	S	H	H
3	L	M	M	S	S
2	N	L	M	M	M
1	N	N	L	L	M
	1	2	3	4	5

Probability

Security Risk Analysis

Vulnerability	
Failsafe	Asset has a very low exposure; multiple layers of security in place and effective management.
Low	Adequate security measures; reduced asset exposure; some areas for improvement based on *ROSI.
Significant	Basic protective measures in place; significant exposure and need for upgrading of security controls.
Extreme	Asset totally exposed; no effective security controls in place.

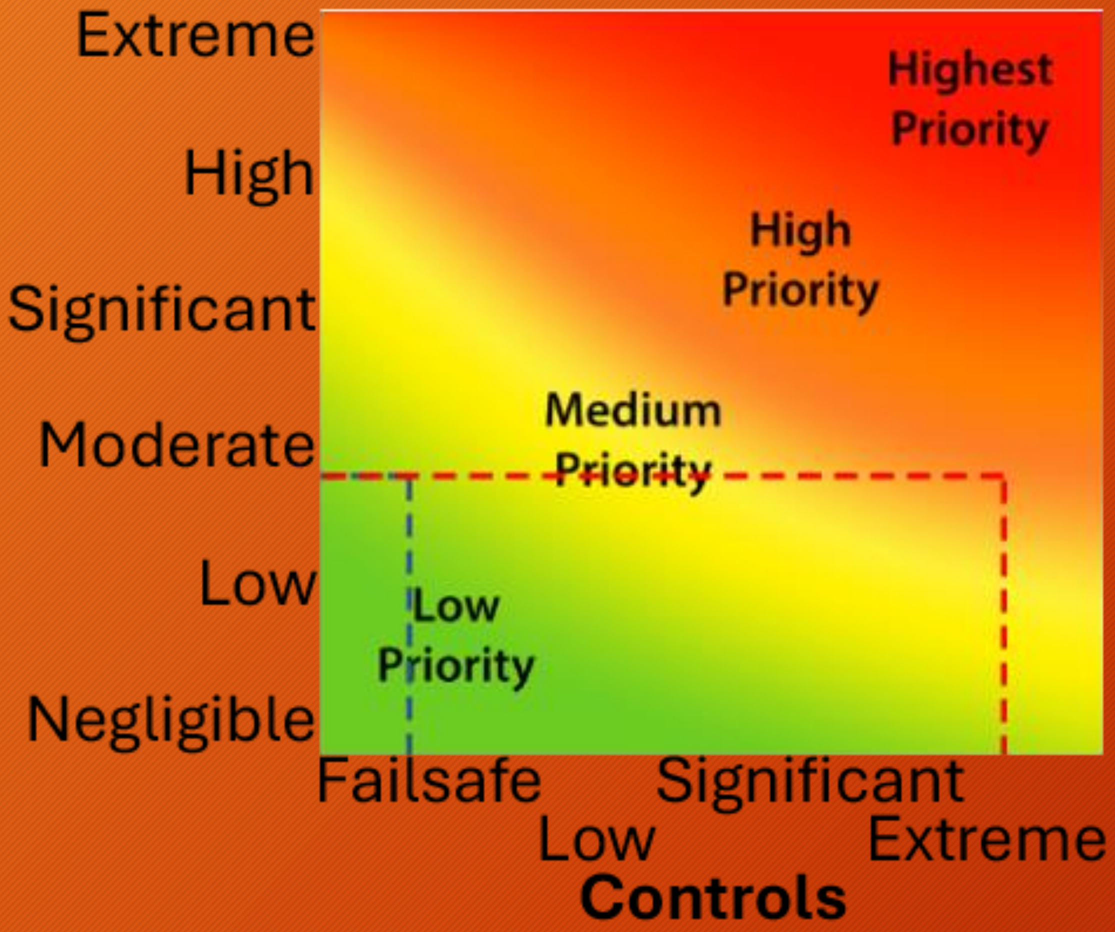
Now that we have looked at the likelihood and impact of an adverse event to give an indication risk, we have to consider how vulnerable the asset is to that risk.

Risk may be affected by factors such as how attractive an asset is to an adversary, but also how effective security controls are, or not.

Vulnerability can be assessed qualitatively using matrices such as this.

**Return on Security Investment – a calculation that justifies security spend and evaluates security programme effectiveness.*

Security Risk Analysis



Use other graphs to measure risk against existing protection etc. to determine risk priorities.

We can see that moderate risk with ‘failsafe’ security creates a low priority whereas an ‘extreme’ vulnerability creates higher priority for risk treatment.

Risk Registers

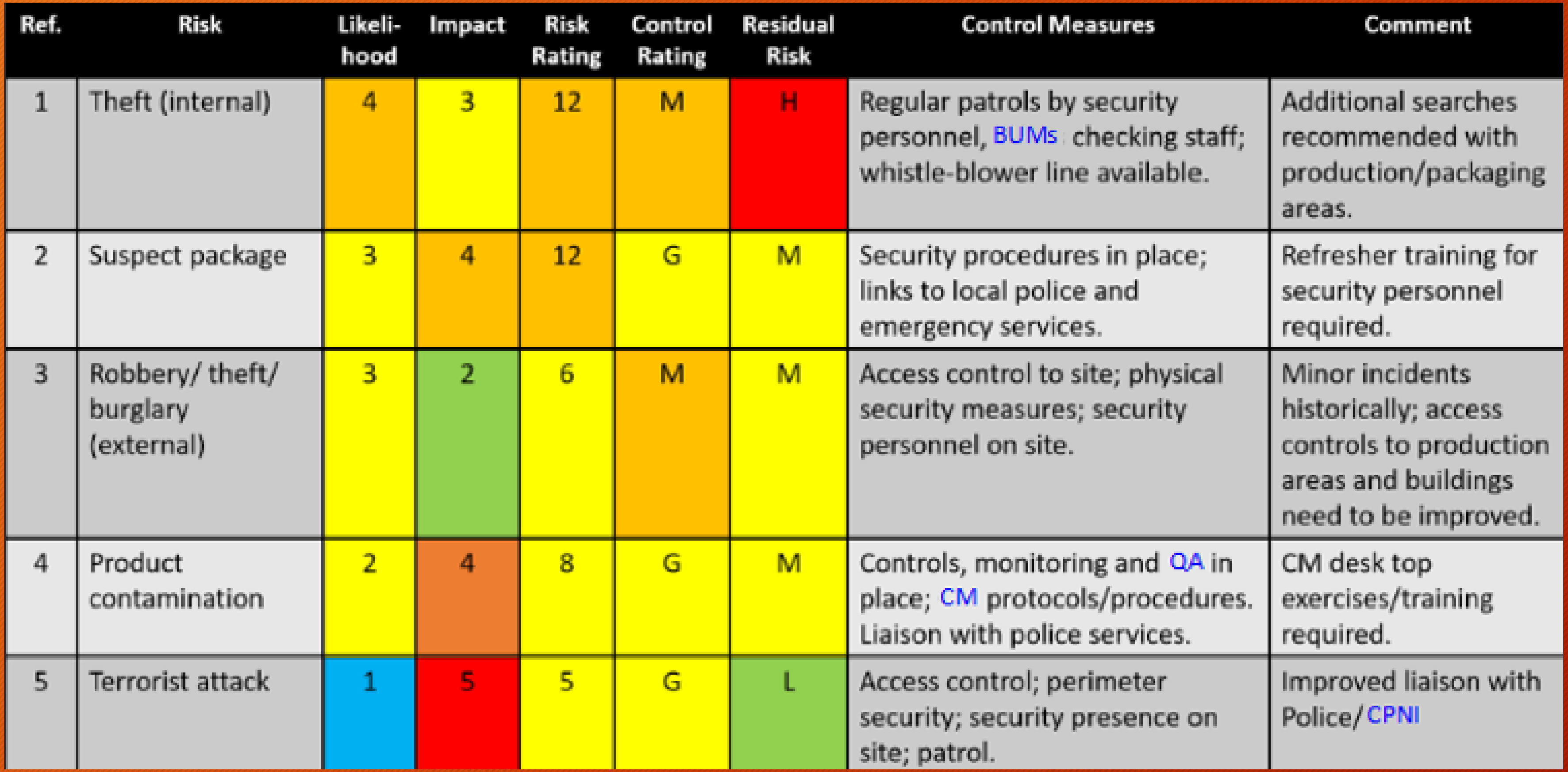
It is quite common practice to document your risk analysis in a Risk Register.

A Risk Register may list:

- Assets under threat
- A description of the threat
- The likelihood/probability of the threat taking place
- The impact/consequence of the threat taking place
- Current controls
- Additional controls required

Although the term ‘threat’ may be applied to unintentional, and natural events, this package focuses on a threat being an intentional malevolent act by an adversary.

Risk Registers



Ref.	Risk	Likeli-hood	Impact	Risk Rating	Control Rating	Residual Risk	Control Measures	Comment
1	Theft (internal)	4	3	12	M	H	Regular patrols by security personnel, BUMs checking staff; whistle-blower line available.	Additional searches recommended with production/packaging areas.
2	Suspect package	3	4	12	G	M	Security procedures in place; links to local police and emergency services.	Refresher training for security personnel required.
3	Robbery/ theft/ burglary (external)	3	2	6	M	M	Access control to site; physical security measures; security personnel on site.	Minor incidents historically; access controls to production areas and buildings need to be improved.
4	Product contamination	2	4	8	G	M	Controls, monitoring and QA in place; CM protocols/procedures. Liaison with police services.	CM desk top exercises/training required.
5	Terrorist attack	1	5	5	G	L	Access control; perimeter security; security presence on site; patrol.	Improved liaison with Police/CPNI

*BUMs = Business Unit Managers

*QA = Quality Assurance

*CM = Crisis Management

*CPNI = Centre for the Protection of National Infrastructure

Risk Evaluation

Security Risk Analysis Results

The results around a particular risk are determined, based on the associated consequence (impact), vulnerability, and threat (likelihood).

+

Risk Criteria

These are the terms of reference used to measure and evaluate the significance and effects of the identified risk. They are a function of the organisation's objectives, values, and policies, as well as the internal and external environment. They can be derived from jurisdictional laws, obligations, and other requirements.

=

Risk Priorities

Once the risk analysis results have been determined in the context of the risk criteria, risk priorities may be identified, which then inform decisions around appropriate risk treatment measures.

Risk Treatment (Mitigation)

Once we’ve assessed the threats to our assets and understood the we must ‘treat’ the risk.

Risk treatment in a security management context, usually focusses on physical security measures (including security personnel) and policy procedures.

From a more strategic standpoint we look at 5 avenues to risk treatment.

Risk Treatment (Mitigation)

Accept – depending on the risk appetite and security culture of the organisation, together with the potential cost of preventing or mitigating particular risks, some will be accepted in the course of doing business.

Spread – it may be beneficial to spread the risk to another geographic location / department / building / partner etc.

Transfer – this includes transferring the risk to an insurance company or outsourcing.

Reduce – this includes measures to reduce the likelihood of it occurring, reduce vulnerabilities, and/or reduce impact (consequence) should the risk actually occur. Agreed working practices, simple procedures and proportionate physical and technical security measures are examples of risk reduction.

Avoid – risk may be totally avoided by removing a highly vulnerable asset or ceasing a particular operation. Although highly unlikely in practice, it can also be achieved if the threat is totally removed.

Policy & Strategy

As with all things, the steps taken to reduce risk need to be formalised and recorded.

A security policy is required that outlines the approach to security risk management.

Too often these documents are lengthy and never read.

- A policy statement is required that summarises the general approach to security, specific aims and objectives: a statement of intent.
- Allocation of security responsibilities.
- Linkage to standard security procedures/standard operating procedures.
- Consideration of compliance criteria.

This policy must be communicated throughout the organisation, for all stakeholders (whether internal or external).

Security Planning

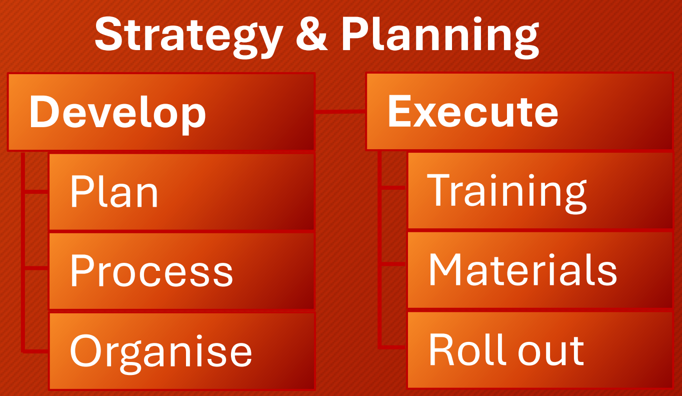
Evidently, part of security planning is the security risk assessment.

Security planning documents will provide the detail of the measures required to mitigate risks to a level as low as reasonably practicable.

These can only be developed after the security risk assessment / security survey has taken place.

A key purpose is to show how proposed mitigation measures will provide on a return on security investment.

It is therefore crucial that the manager has the commercial ability to demonstrate how selected measures will add value to the organisation.



Security Planning

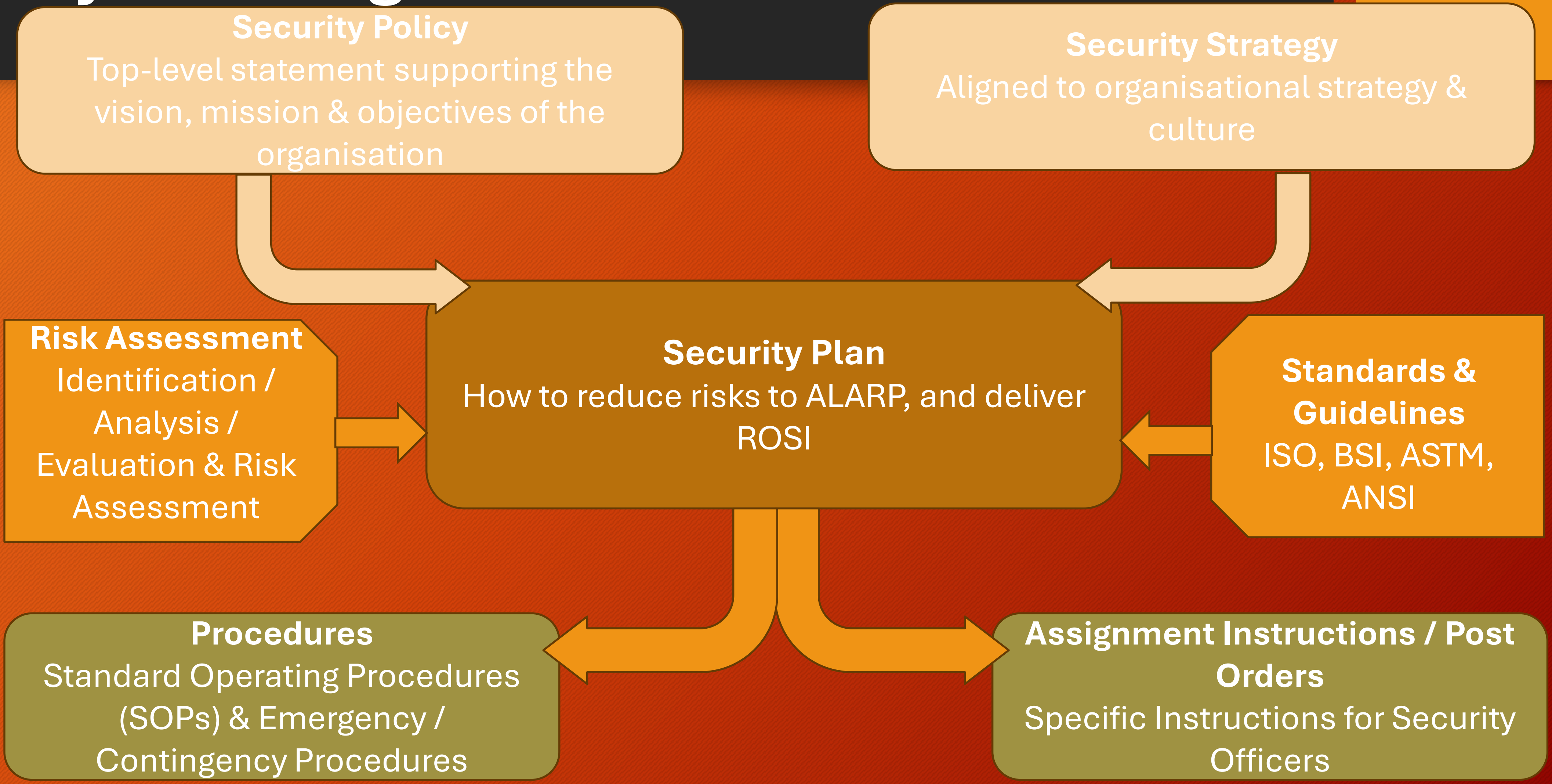
Companies need a Security Plan – detailing how the security function will achieve the aims and objectives in the Security Policy.

The Security Plan will detail how security measures will be implemented and will be supported by standard operating procedures (the how to for security personnel).

The areas covered will include physical security (including security personnel), procedures and technical measures, as well as roles and responsibilities, management and operation of security technologies, incident and crisis management, and training.

Security Standards and Guidelines are used to communicate security requirements to the organisation as a whole.

Security Planning



Security Policy
Top-level statement supporting the vision, mission & objectives of the organisation

Security Strategy
Aligned to organisational strategy & culture

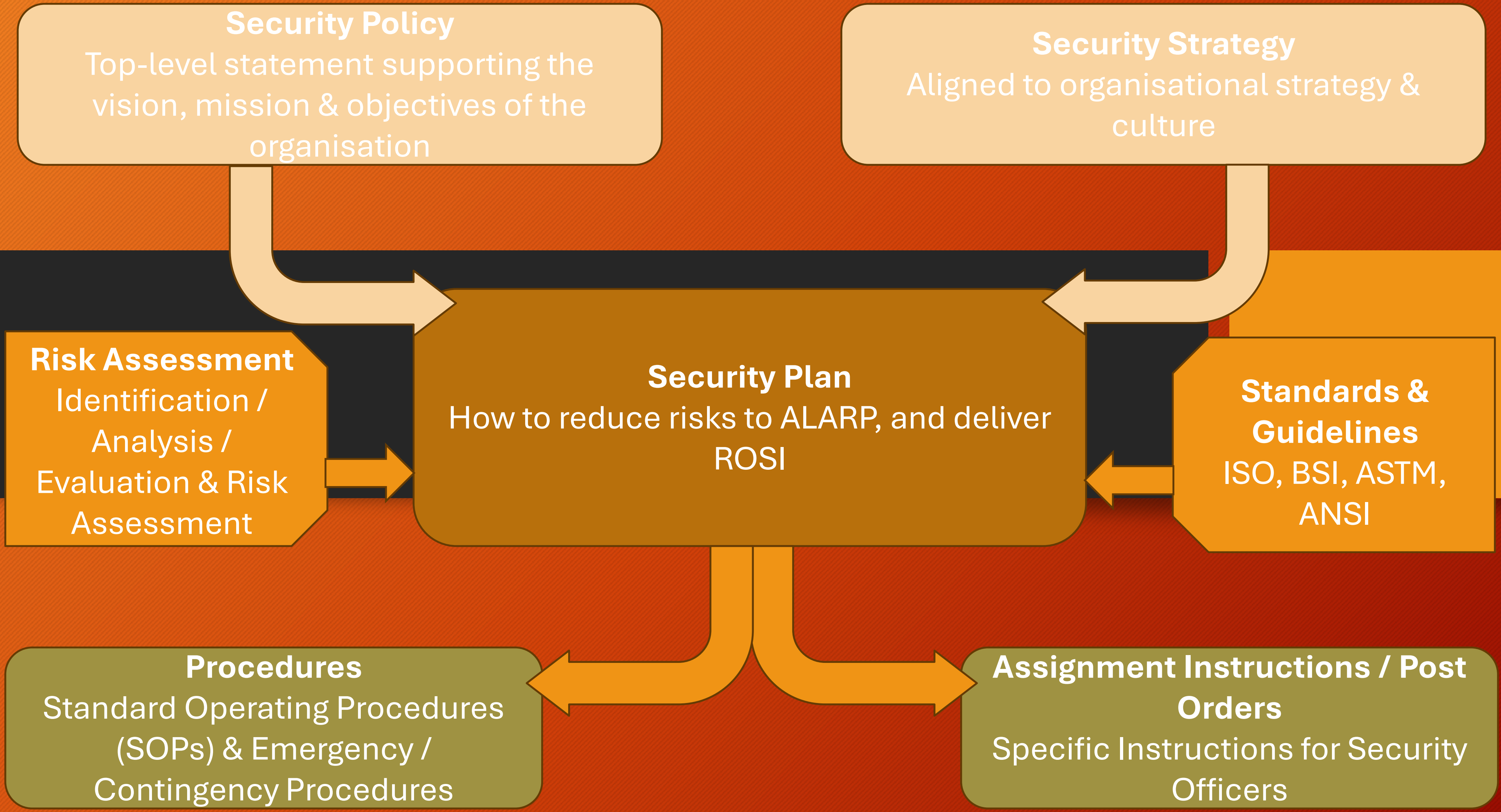
Risk Assessment
Identification / Analysis / Evaluation & Risk Assessment

Security Plan
How to reduce risks to ALARP, and deliver ROSI

Standards & Guidelines
ISO, BSI, ASTM, ANSI

Procedures
Standard Operating Procedures (SOPs) & Emergency / Contingency Procedures

Assignment Instructions / Post Orders
Specific Instructions for Security Officers



Security Policy
Top-level statement supporting the vision, mission & objectives of the organisation

Security Strategy
Aligned to organisational strategy & culture

Risk Assessment
Identification / Analysis / Evaluation & Risk Assessment

Security Plan
How to reduce risks to ALARP, and deliver ROSI

Standards & Guidelines
ISO, BSI, ASTM, ANSI

Procedures
Standard Operating Procedures (SOPs) & Emergency / Contingency Procedures

Assignment Instructions / Post Orders
Specific Instructions for Security Officers

Security Planning

The Security Plan may also cover the timescales for effective implementation of the security solutions (think SMART – Specific, Measurable, Achievable, Relevant, Time-bound).

People & Human Resources

Modern security programmes comprise three core elements: people, procedures and technology.

The success of the security function will come from working, as any other organisational unit, with other stakeholders, e.g. Human Resources, Compliance, Audit and Legal Departments.

Working collaboratively with these departments ensures appropriate policies are published, and procedures followed, in areas such as personnel security, pre-employment vetting, due diligence, workplace violence and lone working.

People & Human Resources

For any security programme to be effective, it is essential that those on site understand the rationale for security and, like senior management, buy into the concept.

Security awareness and a positive security culture will ensure the success of the programme.

This can be achieved through internal awareness campaigns and at employee induction.

Organisations should ensure there is a reporting system for use by all staff and other stakeholders to report security related incidents.

Effective reporting is fundamental to the effectiveness of a security programme and is part of the organisation’s security culture.

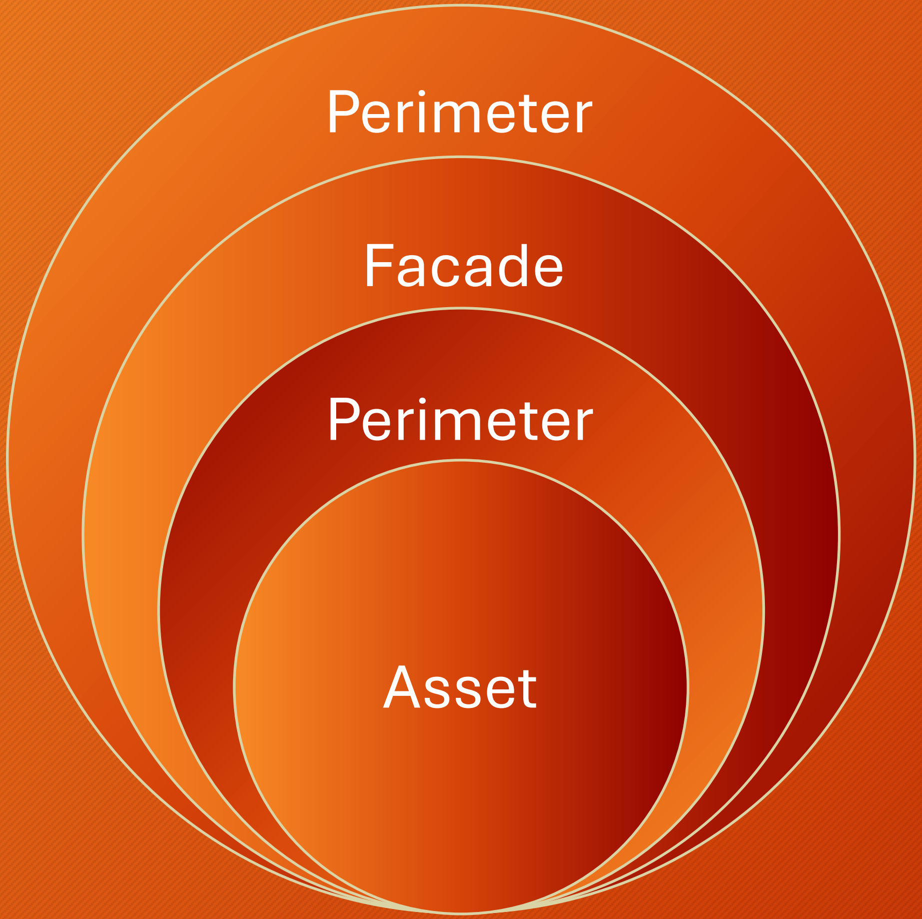
https://www.youtube.com/watch?v=2sh4BIaF6gg

Security Technology

Over reliance on security technology can create vulnerabilities and a fortress mentality. Selection of systems and hardware must be proportionate to the identified risks. They also need to be sensitive to constraints such as budgets, but also the organisational ethos. For example, would you put 3m high fences, barbed wire, floodlights and guard dogs around a local primary school?

Technology must support the human and procedural elements to make a layered system that provides protection in depth and reliability.

Security Technology



Protection in depth means multiple layers of complementary security components that require each one to be overcome for the asset to be compromised.
Detection as far from the asset as possible to assist responders.
The closer to the asset, the stronger the protection.

No system will be able to operate without there being some failure or technical issue. Redundancy/back up systems and procedures are essential.
When choosing security system components tried and tested is perhaps better than new and innovative.

Building Structure – Basic Considerations

Protection or Defence in Depth – is often referred to as the onion skin approach, multiple layers of security that become increasingly hard to overcome, the nearer you get to an asset.

Layers of security are provided physically and operationally. Therefore, security officers, fences, doors, walls, CCTV, intruder alarms etc. all combine to complicate the adversary path to the asset, slowing the attacker down and providing better opportunities for them to be stopped and caught.

Balanced security – essentially all your components (doors, windows, locks etc.) need to provide the same delay time and protection.

Defence in Depth/Layered Security

Remember to balance your security provision across people, procedures and hardware/technology; don’t just rely on your security team.

Utilise fencing, vegetation, traffic flow, parking areas, parking gates, access controls (manual and electronic), lighting, signage, access points, CCTV cameras, control room, security guards, senior executives and assets to guide where and what you need to mitigate risks.

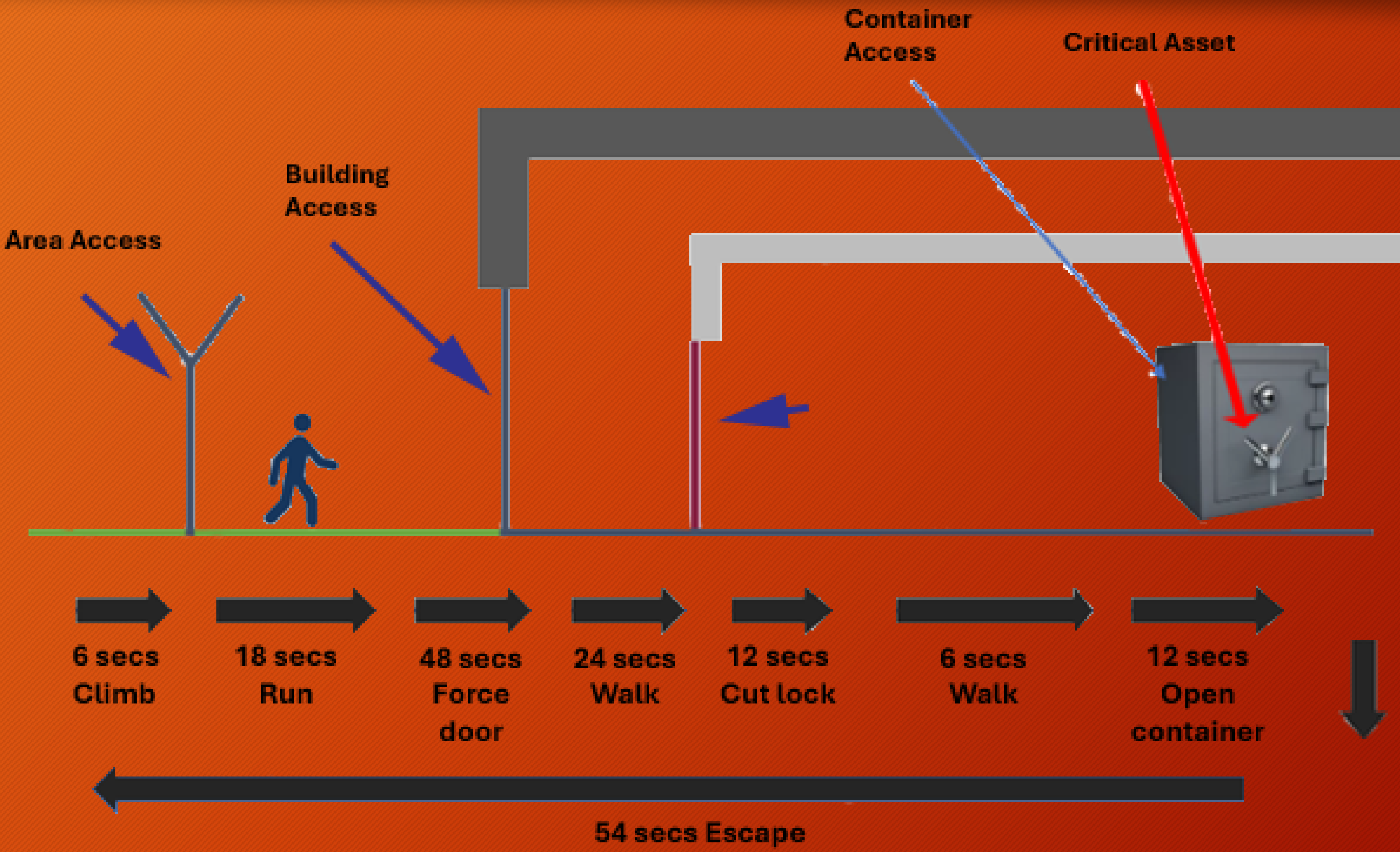
Time of Penetration

Each layer of security e.g. fences, doors and walls will cause an adversary to slow down, as they negotiate each obstacle.

The ideal is to detect the intruder as far from the asset as possible.

The combined time to negotiate each layer/obstacle must be greater than the time it takes for security to apprehend the intruder before they get to the asset – see next slide for illustration.

Time of Penetration



Balanced Security

Balanced security means that all security components, doors, windows, glazing, locks and the walls into which they are fitted proved the same protective capability – it takes the same time to break through them.

Balanced also means there is no over reliance on a particular aspect of the programme – people, procedures or technology. If one aspect fails, then other components can cover the vulnerability. For example, if the access control system fails, security personnel take over.

Balanced Security

All components of a security programme must have an effect that reduces risk in one form or another.

For example, a fence may deter unauthorised entry to a site – but will not prevent determined intruders. It only serves to delay their progress and complicate their plans.

By adding a perimeter detection system to the fence, this does not prevent the intrusion but detects the intrusion and allows for a response.

Time of Penetration

The security practitioner can create the necessary delay time by choosing security components that have been tested and rated due to their ability to withstand attack.

Various schemes exist and products are tested using a variety of tools and attack methods.

This is why you need to understand who your adversaries are, their capabilities and motivations.

Time of Penetration

Deter –

Physical components – fences, lighting, doors, windows

Detect –

Surveillance camera technologies; may deter the adversary, detect wrongdoing and alert the response

Delay –

Interior locking doors or other physical barriers e.g safes

Deny –

Barriers and technologies e.g. access control, slow down and complicate intrusion, providing opportunity to apprehend

Destroy/Defend –

Security/law enforcement personnel respond and attempt to apprehend the intruder

Crime Prevention Through Environmental Design

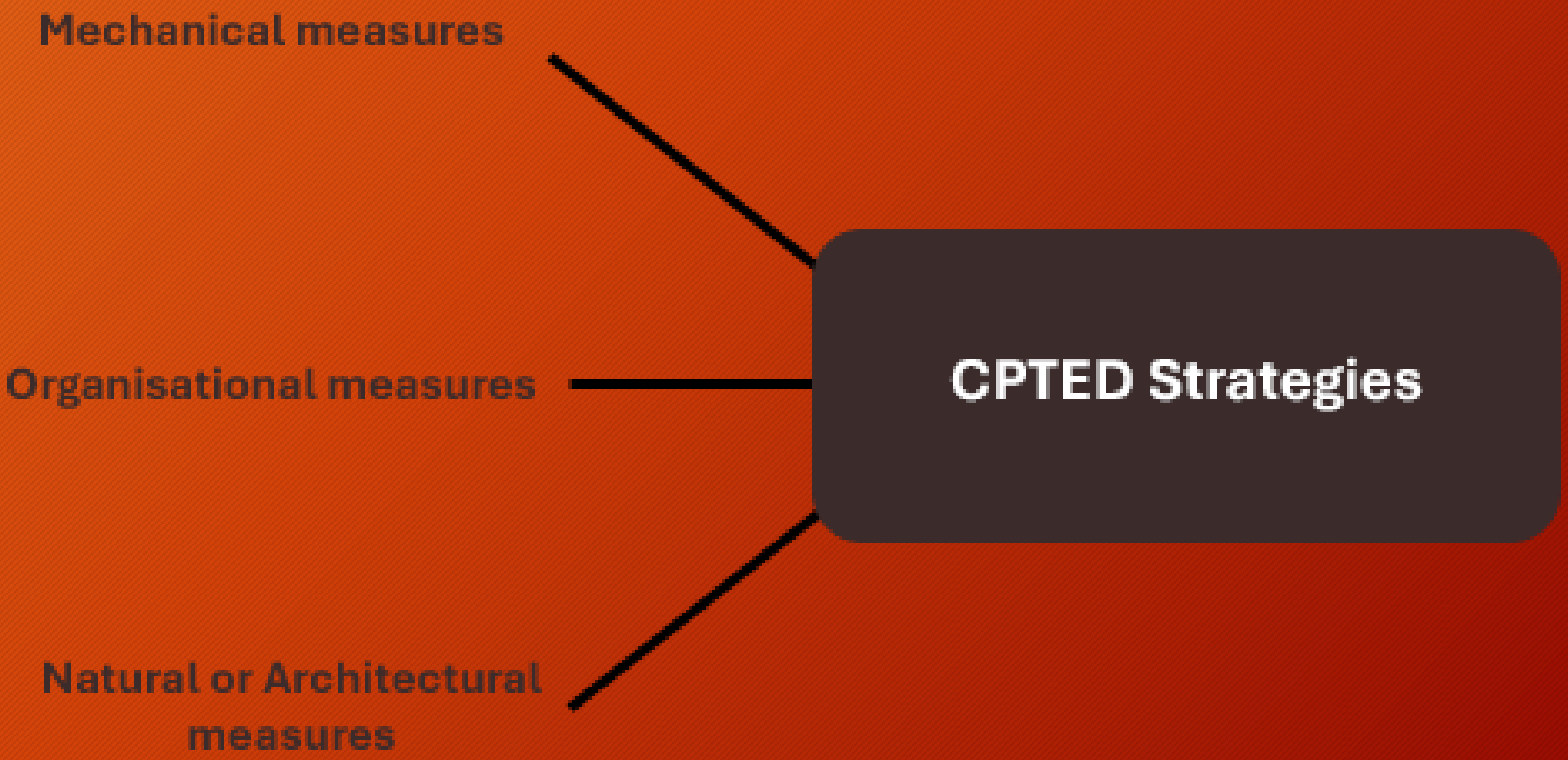
Part of our mitigation strategy for crime prevention must include Crime Prevention Through Environmental Design.

CPTED refers to the design, upkeep and management of the built environment to reduce opportunities for crime.

CPTED strategies include mechanical, organisational and natural or architectural measures to discourage those who may be contemplating criminal acts, and to encourage activity and witness potential by legitimate users.

CPTED concepts and applications can be applied to existing facilities, as well as new buildings and renovations.

Building Security



Mechanical measures

Organisational measures

Natural or Architectural measures

CPTED Strategies

Crime Prevention Through Environmental Design

When considering building security at your site, always try to apply the four principles of CPTED.

1. **Natural surveillance:**

Can be supported by the placements of windows in a building and designing open plan spaces to allow for surveillance/observation by legitimate uses.

Crime Prevention Through Environmental Design

2. Natural access control:

The use of physical (fences, doors, shrubs, hedges, waterways, signs) and psychological barriers (changes of floor surface in transitional zones, position of counters and tills) to channel people to/from buildings and through the surrounding environment.

This measure also involves guiding visitors past ‘capable guardians’ – those who have responsibility for an area e.g. security personnel, receptionists, which again creates a psychological barrier.

Crime Prevention Through Environmental Design

3. Territorial reinforcement:

These are design features that demarcate public areas (e.g. the street) to semi-private and private areas (e.g. the foyer). Demarcation, through the use of physical and psychological barriers, so that employees feel responsible for an area and take ‘ownership’ of the space. This assists in keeping potential intruders out and allows for early and effective detection of an adversary.

Crime Prevention Through Environmental Design

4. Maintenance and management:

Maintaining buildings and ensuring the area within and around a site in a good state of repair, reduces the risk of criminality whilst creating an environment in which your staff and visitors feel safe.

The Broken Windows Theory (Wilson & Kelling, 1982) states that disorder – or broken windows – promotes more serious crime.

Crime Prevention Through Environmental Design

5. Target hardening:

Involves strengthening a site, facility or building and complicating the task of the adversary to gain access. Hardening may have a deterrent effect but, will also contribute to other aspects of the 4 Ds.

This may comprise perimeter and internal fences, hostile vehicle mitigation, locks on doors and windows, upgraded window glazing, deployment of security teams, access control systems, turnstiles, CCTV, intruder alarms etc.

https://www.npsa.gov.uk/

Operational Requirements

When planning a security programme, to ensure the Ds of Security are proportionate to the threats and risks, a formal process known as Operational Requirements are used.

The OR process brings together all stakeholders to discuss their security requirements and potential impacts on organisational activities (Level 1).

With agreed strategy in place, then specific security components are assessed and included (or not) in the security programme and specific requirements agreed (Level 2).

Operational Requirements – Level 1

A Level 1 Operational Requirement assesses, evaluates and provides the rationale for mitigation measures (whether physical or procedural) to mitigate risks from identified threats.

1. Outlines and assesses threats and associated risks
2. Identifies risk mitigation options e.g ASTRA
3. Creates a strategic statement of how security needs will be addressed (i.e. Security Plan)
4. Presents a rationale (and costed) business case for security expenditure

Operational Requirements – Level 1

Stakeholder inputs and decisions are formalised and recorded, covering areas such as:

- Site or building to be protected
- Stakeholders involved
- Critical asset(s)
- Threats, vulnerabilities, impact
- Security plan
- Organisational constraints
- Implementation and integration
- Critical dependencies
- Costs and benefits
- Organisational readiness

Operational Requirements – Level 2

The purpose of the Level 2 Operational Requirement process is to provide the detail required to develop a performance specification covering a range of possible solutions.

Having a detailed specification, agreed by all affected parties, will facilitate an accurate procurement process and installation of proportionate mitigation measures.

Operational Requirements – Level 2

- Obtain a copy of the Level 1 OR
- Agree with appropriate stakeholders which Level 2 Ors should be pursued
- Discuss Level 2 checklists with the appropriate stakeholders together with a copy of the Level 1 OR for reference. Use a security consultant if necessary.
- Complete Level 2 checklists with the appropriate stakeholders and collate. Ensure that different Ors integrate. Discuss any anomalies.
- Ensure the Level 2 OR statement integrates and relates to the Level 1 OR. Obtain senior management approval to proceed.
- Produce a performance specification using someone with technical knowledge.
- Once agreed, commence procurement.

Control & Monitoring

Effective control and supervision is of extreme importance in the implementation of security programme procedures.

The security practitioner must lead by example, ensuring that clear procedures, based on sound policy are followed by all stakeholders.

The security supervisor, has a key role in ensuring the effectiveness of the security function as they managed their respective teams on the ground and are often the face of security to the organisation.

Too often, security personnel are merely seen as gatekeepers or the hi-vis brigade. Engaging the security team with the organisation can be achieved through security awareness sessions and briefings.

Senior Security Practitioner Competence

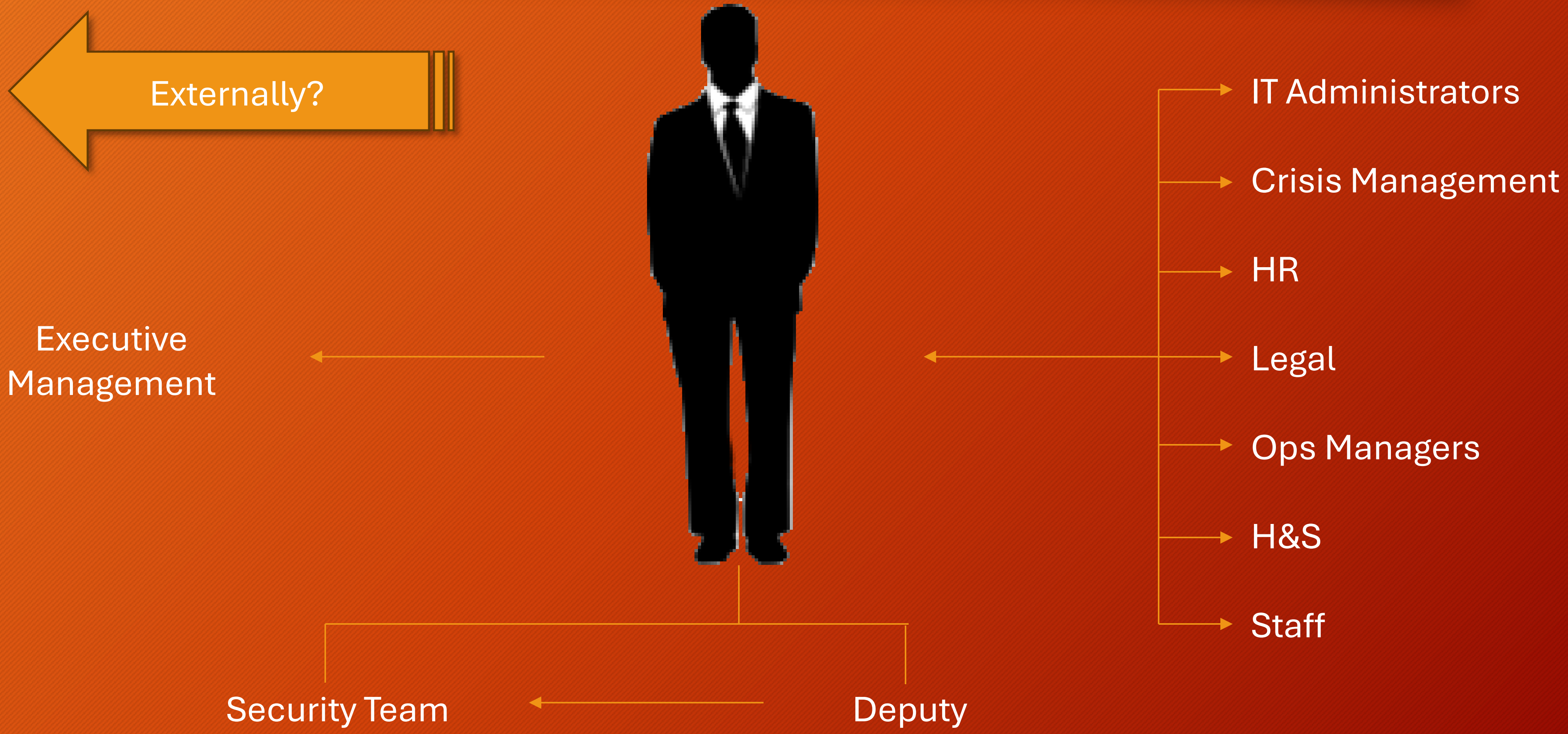
Things you should be able to do

- People manage
- Programme/project manage
- Financial projections and ROI projections
- Security risk analysis forecasts
- Recommend appropriate mitigation
- Crime prevention

Things you should get **trained** to do

- Security survey
- Investigate
- Specify technical solutions
- Fraud risk management
- Special management skills (project management, time management etc.)
- Crisis and organisational continuity management

Stakeholders



Externally?

Executive Management

IT Administrators

Crisis Management

HR

Legal

Ops Managers

H&S

Staff

Security Team

Deputy

Control & Monitoring

An essential part of the OR process is ensuring that specifications contain the necessary criteria to monitor and evaluate system success.

These may cover performance requirements for technical systems e.g. false alarm rates for an intruder detection system or false acceptance rates for an access control system.

However, they also extend to personnel e.g. how many patrols/searches conducted; customers assisted; training sessions delivered etc.

Security metrics can be used to calculate the cost of security provision against reduced losses, to produce a positive return on security investment (ROSI).

Control & Monitoring

Security audits assess the performance elements of security programme – how well they integrate to effectively prevent or mitigate current security risks.

Audits are a security management tool to identify vulnerabilities caused by technological / equipment deficiencies, the contribution made by persons (e.g. staffing levels/employee compliance), and procedural irregularities (e.g. response to security events).

Although the terms security audits and security surveys are often used interchangeably, they are in fact different.

A security audit may be defined as an assessment of the performance of the security programme, not just technology, but also personnel, procedures, and employee compliance.

An onsite examination and evaluation of existing measures to reduce security risks, identification of areas of vulnerability and recommendations to rectify issues.

Control & Monitoring

Security metrics can be extended across the organisation. For example, clear desk policies for part of the security/risk grouping and compliance needs to be measured.

Just as with Health & Safety, all employees have a responsibility for security – not just the security officer who is expected to deal effectively with both slow time and spontaneous security related incidents.

Those managing the security function need to develop clear and workable standard operating procedures.

Control & Monitoring

Care must be taken on how SOPs are communicated to the workforce.

In the same way that the fortress approach to security may well be detrimental to staff willingness to adhere and contribute to the security programme, the same could apply if staff believe or perceive procedures under the programme are too regimented, rigid or unnecessary.

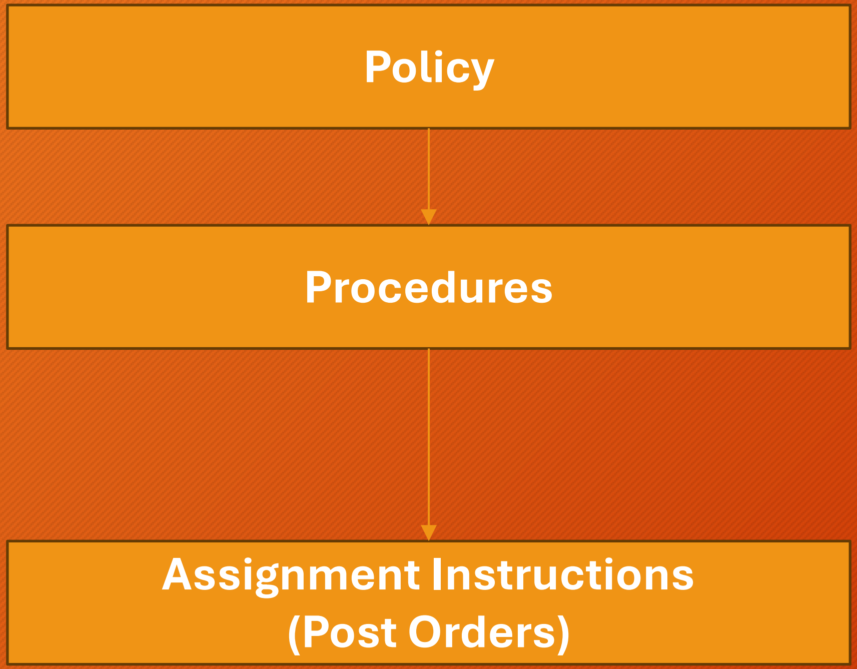
It is important therefore, that required procedures are communicated to the workforce in a facilitative, transformational way, as part of an ongoing security awareness programme.

Control & Monitoring

Assignment instructions (sometimes referred to as Post Orders) are specific instructions for Security Officers / Guards. These need to be written clearly and concisely to ensure full understanding by those officers needed to consult them.

Assignment Instructions / Post Orders need to be written for each task a guard is required to perform, and each particular security post that requires staffing by an officer.

Policy, Procedures & Assignment Instructions



Policy

Procedures

Assignment Instructions (Post Orders)

Organisation’s management position, purpose or direction.

- What management want to achieve.

- Detailed instructions that need to be followed to achieve specific outcomes required under the policy.
- Explain how and to what standard.

- A specific type of procedure for security officers.
- Often step-by-step
- Routine and emergency actions.

Test & Drills

Although daily operations may be routinely monitored with a view to ensuring performance, this is not possible in respect of spontaneous events, such as security breaches, hardware/software failure, and unexpected absence of key personnel.

To ensure procedures around responding to such events are adhered to, and are appropriate for the task, tests, exercises and drills are essential. These may take various forms: - peer reviews, tabletop exercises, scenarios, Red Teaming, penetration testing.

Frequency will vary greatly depending on the nature of the organisation, its size, structure and operations.

Reviews of crisis management, and organisational continuity plans following security incidents are essential and should never be disregarded.