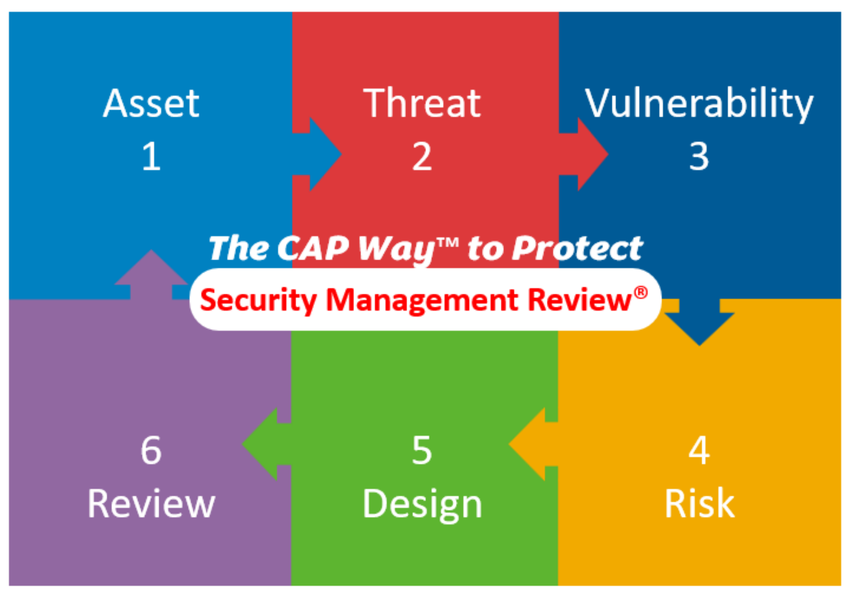
A collaborative approach to create proportionate security arrangements



Asset 1

Threat 2

Vulnerability 3

The CAP Way™ to Protect

Security Management Review®

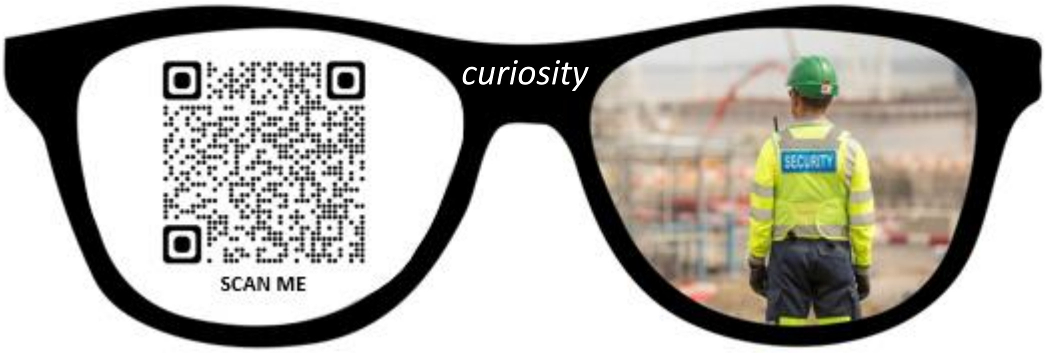
4 Risk

5 Design

6 Review

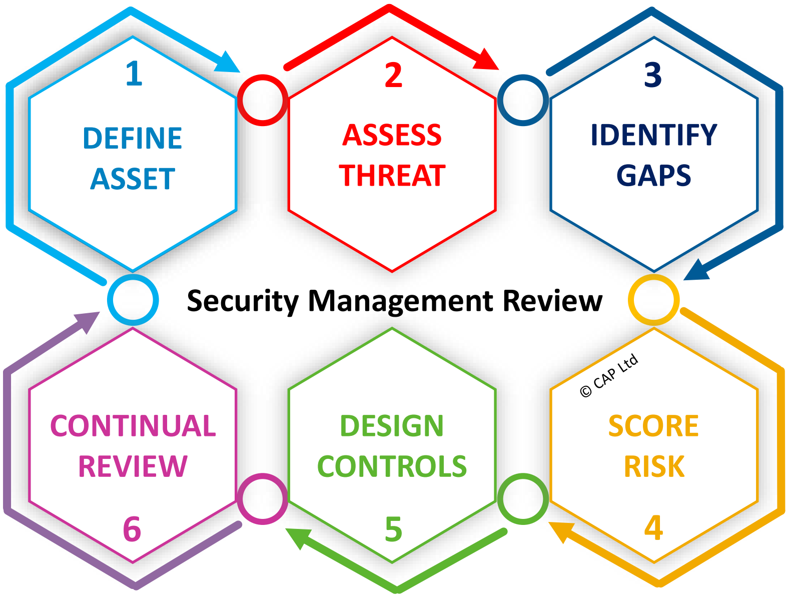
Security Management Review
Process Guide

The CAP Way™ ***To Protect***



Viewing the world through a security lens

a logical, repeatable, and defensible process



grounded in scientific research

Benefits of *The CAP Way*™ SMR Process:

- ➢ Demonstrates cognitive process and builds confidence with stakeholders.
- ➢ Helps justify financial expenditure.
- ➢ Helps to withstand external scrutiny.
- ➢ Meets the '*Reasonable Person Standard*' at a post incident investigation or enquiry.

Additional Information available on ***The CAP Way***™ website: https://thecapway.com/
Prepared by: Frank Cannon. frank@cannonassetprotection.uk
This is a Cannon Asset Protection Limited Publication. January 2024. Guide Number: 001

What is the **Security Management Review** Process?

The SMR process is a stakeholder and client collaboration that provides a common methodology to design and implement a layered defence to deter, detect, or delay an adversarial attack. The protective security solution shall include a proportionate blend of physical, technical, and behavioural controls to reduce theft, sabotage, malicious damage, or anti-social behaviour across the workforce.

The SMR is strategic in nature and provides a chronological approach that negotiates pre-determined steps to standardise an outcome. The process provides the Senior Risk Owner sufficient information to make quality decisions regarding the required levels of protective security controls.

1. **Asset Characterisation**. Understand what needs to be protected, who owns it, who accepts the risk, who pays for the defences?

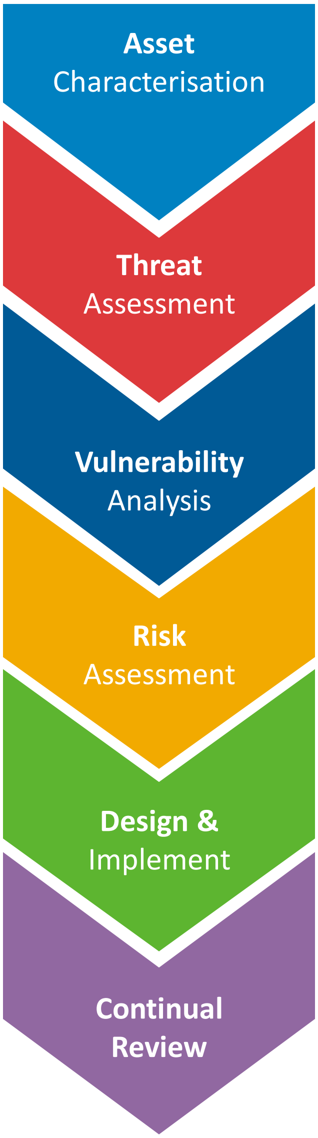
2. **Adversarial Threat Assessment**. Who is likely to attack the assets, what are their motivations and capabilities, what are their strength?

3. **Vulnerability Analysis**. What is already in place to protect the assets from an adversarial attack, are there any gaps in the defence?

4. **Adversarial Risk Assessment**. What is the likelihood and impact of an adversary exploiting a gap to mount a successful attack?

5. **Design Protective Defence**. Create affordable and proportionate defensive measures that still allows business operations to continue.

6. **Review**. Continuous assessment of the defensive efficacy.



Asset Characterisation

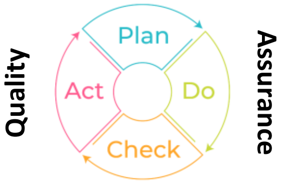
Threat Assessment

Vulnerability Analysis

Risk Assessment

Design & Implement

Continual Review

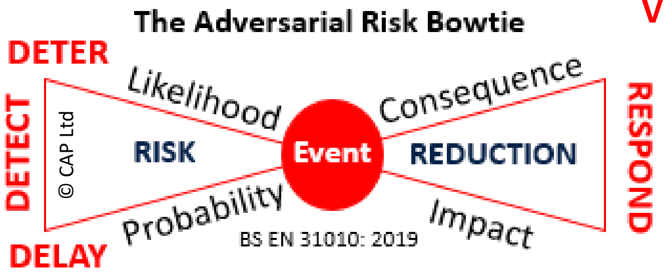


ISO 9001

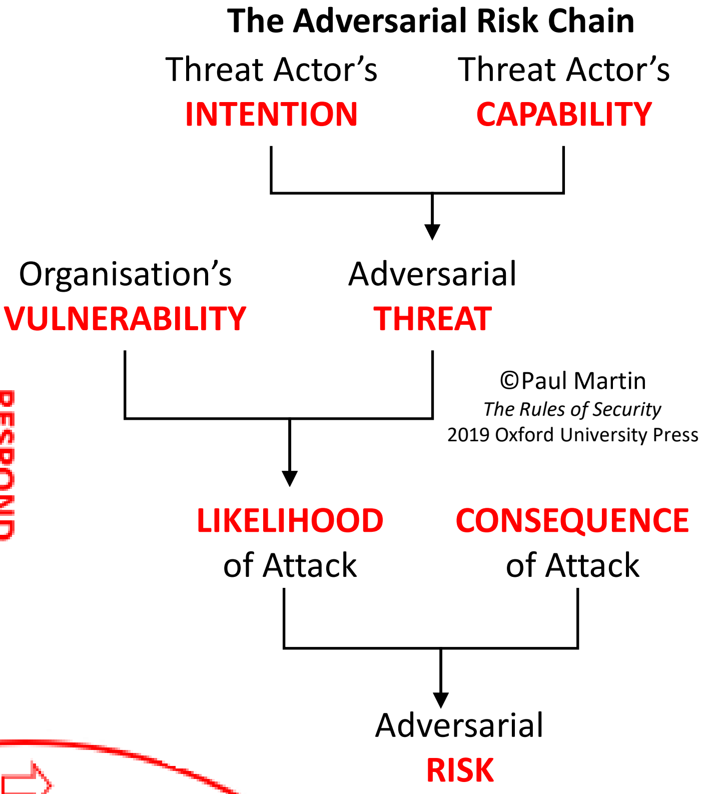
This guide should be read in conjunction with the subordinate *StoryBoards®* within *The CAP Way*™

Influencing References – Shaping *The CAP Way*™ to Protect

A logical, repeatable, and defensible process grounded in scientific research


The Adversarial Risk Bowtie

BS EN 31010: 2019

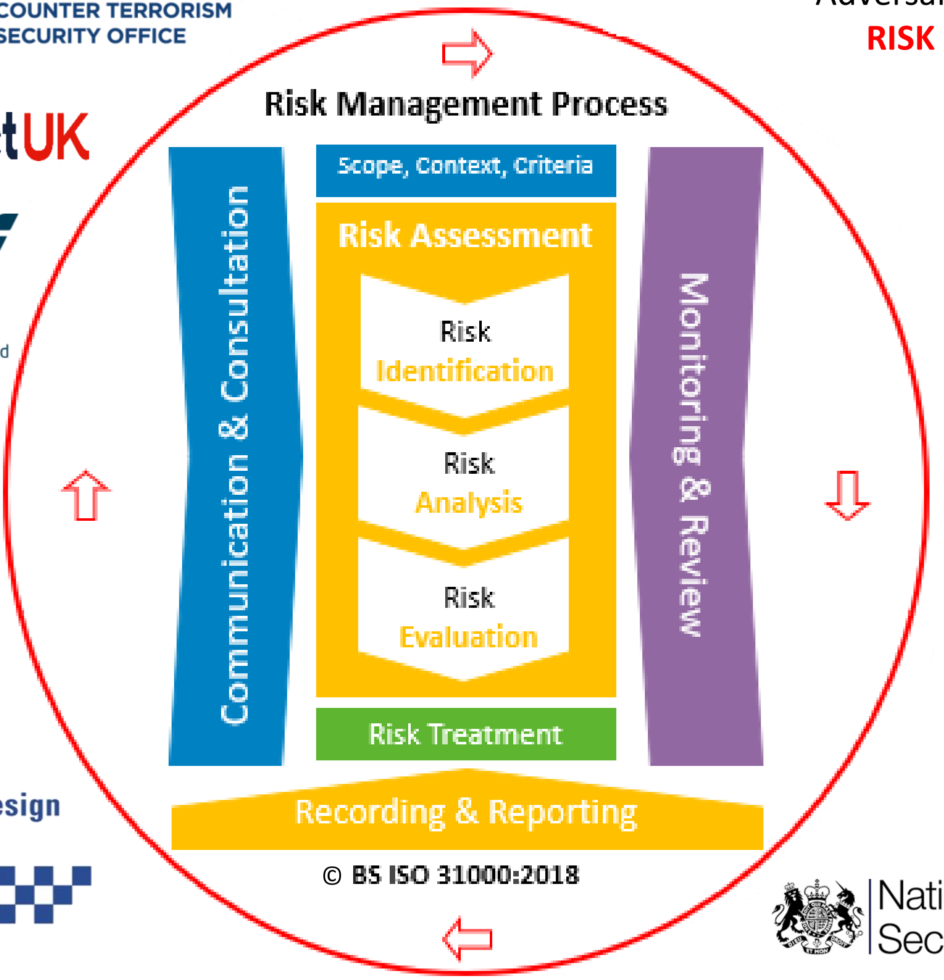

The Adversarial Risk Chain

©Paul Martin
The Rules of Security
2019 Oxford University Press

NaCTSO NATIONAL COUNTER TERRORISM SECURITY OFFICE

ProtectUK

NSI Security Improved


Risk Management Process

© BS ISO 31000:2018

Secured by Design SBD

National Cyber Security Centre

PD ISO Guide 73: 2009 Risk Management - Vocabulary
BS ISO 31100:2018 Risk Management – Guidelines
BS EN 31010: 2019 Risk Management– Risk Assessment Techniques
BS ISO 31100:2021 Risk Management – Code of Practice
PD ISO/TS 31050:2023 Risk Management – Managing Risk to Enhance Resilience

National Protective Security Authority

Protective Security Governance

Stakeholder Engagement. The SMR is a collaborative activity requiring participation from all stakeholder groups involved in providing a safe and secure working environment. The SMR will engage, explain, and educate those involved with a view to influence the Senior Risk Owner to make a high-quality decision.

Engage

To participate or become involved in

Explain

To give a reason so as to justify or excuse (an action or event)

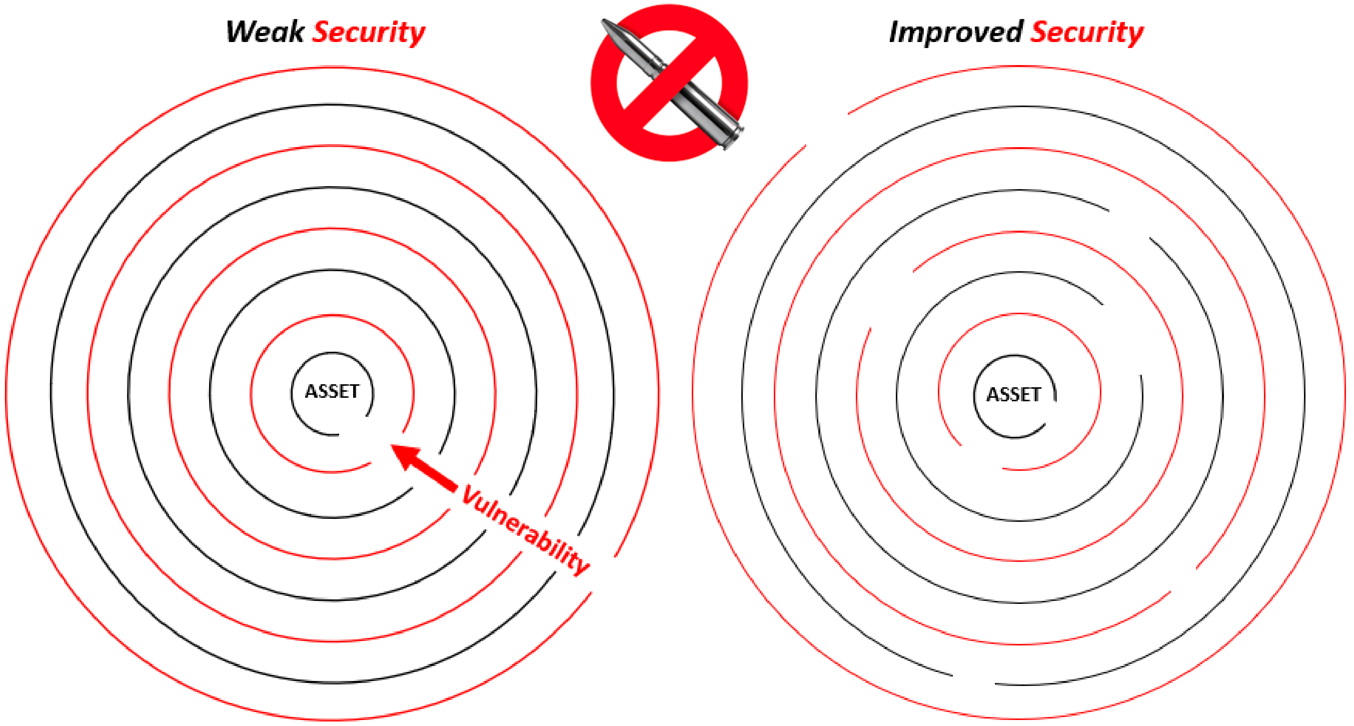
Educate

To give (someone) training in or information on a particular subject

Influence

To have an effect on the character, development, or behaviour of someone or something

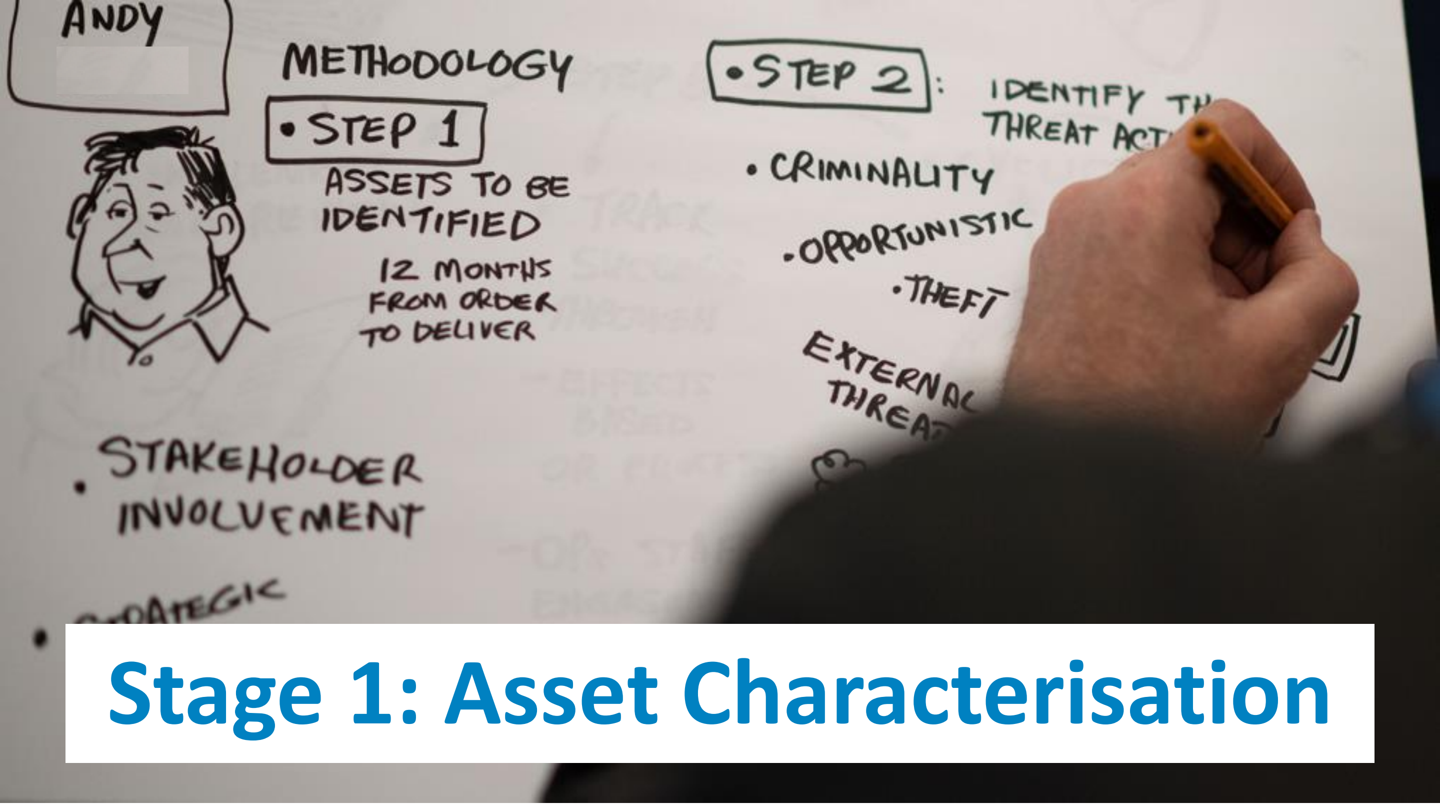
Defence In Depth



Layered Approach. The protective-security controls typically consists of multiple layers of defence; however, each layer will have a gap that must be identified and closed to reduce the probability of a success full attack.

Deter *the attacker*	**Detect** *at the earliest time*
Delay *the attack*	**Respond** *as planned*

Each layer of defence should provide one, or more, of the following protective effects. It should aim to ***deter*** the adversary from attempting an attack through fear of failing or being caught in the act; it should ***detect*** the attacker at the earliest possible time — ideally, before the attack commences and during the hostile reconnaissance phase; it should ***delay*** the attacker from reaching the asset by having to negotiate layer after layer of protective measures; and thus, provide time for the security team (or asset owner) to ***respond*** in a pre-planned way to confront the attacker to prevent further harm or damage occurring.



Stage 1: Asset Characterisation

Understand what needs to be protected…

It is important that those deciding how to protect something first understand what it is they are required to protect. No two organisations are the same. The organisation's Values or assets that are important to one might be less important to another. It is, therefore, essential to study the organisation or site being reviewed to identify the most important people, property, information (or intellectual property), and the public's perception of the organisation – i.e., the brand reputation that require protecting.

Those conduction the SMR should:

Select or **define the business area**, location, system, or process that will be subjected to a Security Management Review. This should be specific, measurable, achievable, realistic, and timely (**SMART**). Identify who '*owns*' the asset.

Identify the stakeholders who have an interest in protecting people, property, and information and invite them to participate in the SMR.

Seek technical advice from a suitably qualified and experienced **protective-security practitioner**.

Appoint a **responsible person to lead the SMR** and empower them to consult with all necessary stakeholders – including those that may originate from outside of the organisation.

Follow the money

Appoint the **Senior Risk Owner** to make the final decisions. The SRO has the appropriate level of authority, is accountable for the business deliverable, has the budget, and can allocate sufficient resources to implement the findings of the SMR. Assess who would go to jail if the appropriate levels of controls were not implemented.

1. Asset Characterisation

ASSET

Stage 1 Outcome (products):

1. Description of the asset.
2. Owner of the asset/system.
3. Person responsible to protect the asset.
4. Senior Risk Owner (budget holder).

Stage 1: Asset Characterisation - *The Small Print…*

We must first understand what we need to protect to ensure the organisation's business plan can be delivered. Who or what is essential to success. What is required to continue delivering the product that creates value, brings in the money, or delivers the success for which the organisation exists. Is the 'brand' reliant on customer relationships or public reputation.

The limit of this research needs to be defined or quantified so the SMR is achievable. An SMR might focus on the complete organisation (strategic), a sub-department or group of sites (tactical), or an individual asset, person, or business process or system (operational).

Once you've set the boundaries, identify your Senior Risk Owner. This is typically the person who has the accountability to deliver, the legal liability, or the responsibility for the budget, setting the group priorities, and the power to allocate resources – including people.

In addition to the Business Plan, it is beneficial to understand the organisation's Values, Standards, Code of Conduct, and read the Quality, Safety, Sustainability, Environmental, Business Continuity, and Emergency Management Plans. These core documents provide an insight into the business operating model and organisational culture.

Now that we have a SMART objective for the SMR, we need to identify the key stakeholders who understand the asset, process, or what it takes to deliver the Business Plan. They will help identify the importance of critical assets or processes, what they consist of, how they work (i.e., do they need power, connectivity, water, or source materials), and what would happen if they failed to operate as designed.

The input from the heads of departments or functions within the organisation is fundamental to creating a universal understanding of what needs protecting and will help when conversing with the technical stakeholders later in the process.

Asking the heads of functions or department managers how one could wreak maximum damage or disruption by attacking their business operating model or systems is a useful way to identify equipment and system vulnerabilities and highlight those elements that are essential to smooth operations. This would allow for the designation of various levels of criticality of components across the system, rather than having just one criticality rating.

Is the activity, asset, or information deemed 'business critical' and has it been designated a minimum time in which it's availability or reduced operational capability is acceptable?

It is important to understand the full impact of a security event and not just the cost of the damaged or lost property. Does the operating system already have resilience designed-in? Will the lost or damaged equipment reduce the production capability or stop it all together?

Does the loss impact a safety or quality certification that would need repeating? Would the event amount to a criminal offence, reportable safety incident, or regulatory requirement triggering an investigation by external agencies that may negatively impact the organisation's reputation or customer's trust?

Business Critical

Stage 2: Adversarial Threat Assessment

Adversary: "a motivated and capable person or group acting with malicious intent; the human cause of an unwanted incident."

An adversary is a person who is actively opposed or hostile to someone or something.

The adversarial threat assessment is about understanding the adversary; understanding their motivation and capability and why they might choose to attack the organisation or it's people. This process does not identify or quantify the negative consequence of weather events, industrial safety accidents, or social and political occurrences. An adversarial threat will always originate from a person and mostly when people behave with malicious intent.

There is an assumption that the layered security arrangements in place across the organisation will reduce the probability of an attack originating from an external threat actor to an acceptable level. However, the source of adversarial threat to the organisation may also emanate from the Insider Threat actor.

The National Protective Security Authority (NPSA) defines an *Insider* as being *"Any person who has, or previously had, authorised access to or knowledge of the organisation's resources, including people, processes, information, technology, and facilities*".

It may be the case that the Insider will collaborate with non-employees to ensure they maximise the benefits from their adversarial activities.

The goal is to understand the adversary's motivation, capabilities, and their strengths, and how they might defeat your defences.

2. Adversarial Threat Assessment

Stage 2 Outcome (products):

1. A list of people/groups (adversaries) who might attack the asset.
2. Their motivations and capabilities.
3. Their attack methodologies.
4. Their strengths.

THREAT

Stage 2: Adversarial Threat Assessment - *The Small Print…*

If you understand '*why*' and '*how*' you already have part of the solution.

Understanding Motivation. If the motivation of the attacker is acquisitive in nature, the offender mostly wants to repeat the crime more than once. They may plan their attack, conduct their own risk versus reward assessment, seek out opportunities, or choose the best time to steal when the odds are more favourable to them. They will mask their theft, so the loss is hidden. They often wait until the right 'opportunity' presents itself and then they attack.

A disgruntled worker often seeks retribution immediately and may act without considering the consequence. This leads to overt malicious damage, use of violence, or behaviours contrary to the organisation's Code of Conduct. This type of behaviour could occur immediately after a disciplinary event, just after the employee receives bad news, or as a culmination of events where they feel they are being undervalued or disrespected. These events may be a sign of desperation where the employee can't see an alternative course of action.

However, if you subscribe to the theory that '*revenge is a dish best served cold*', then a disgruntled worker chooses not to act in desperation but may take time to plan their retribution knowing that the consequence will be greater once their attack is discovered. This leads to acts of sabotage rather than overt malicious damage, an example of which could be multiple holes drilled along a pipe in a place that is not typically seen during a supervisor's periodic check. Therefore, by understanding the motivation (or mens-rea) of probable attackers, the type of attack can be determined with a higher degree of accuracy.

Understanding Capability. The capability of an attacker is typically assess based on the success of prior attacks, the skill sets of the group likely to be involved, and the opportunity for the adversary to mount a successful attack. It may also increase if the attacker has the right tools, sufficient time, and a method to move their ill-gotten gains from the crime scene.

Where proportionate control measures are in place, that deny this capability, the likelihood of a successful attack occurring is reduced, therefore; once again, if the security specialist understands the capability required to mount a successful attack, they can take steps to deny the attacker from having access to the property, the tools, or the time to commit the attack.

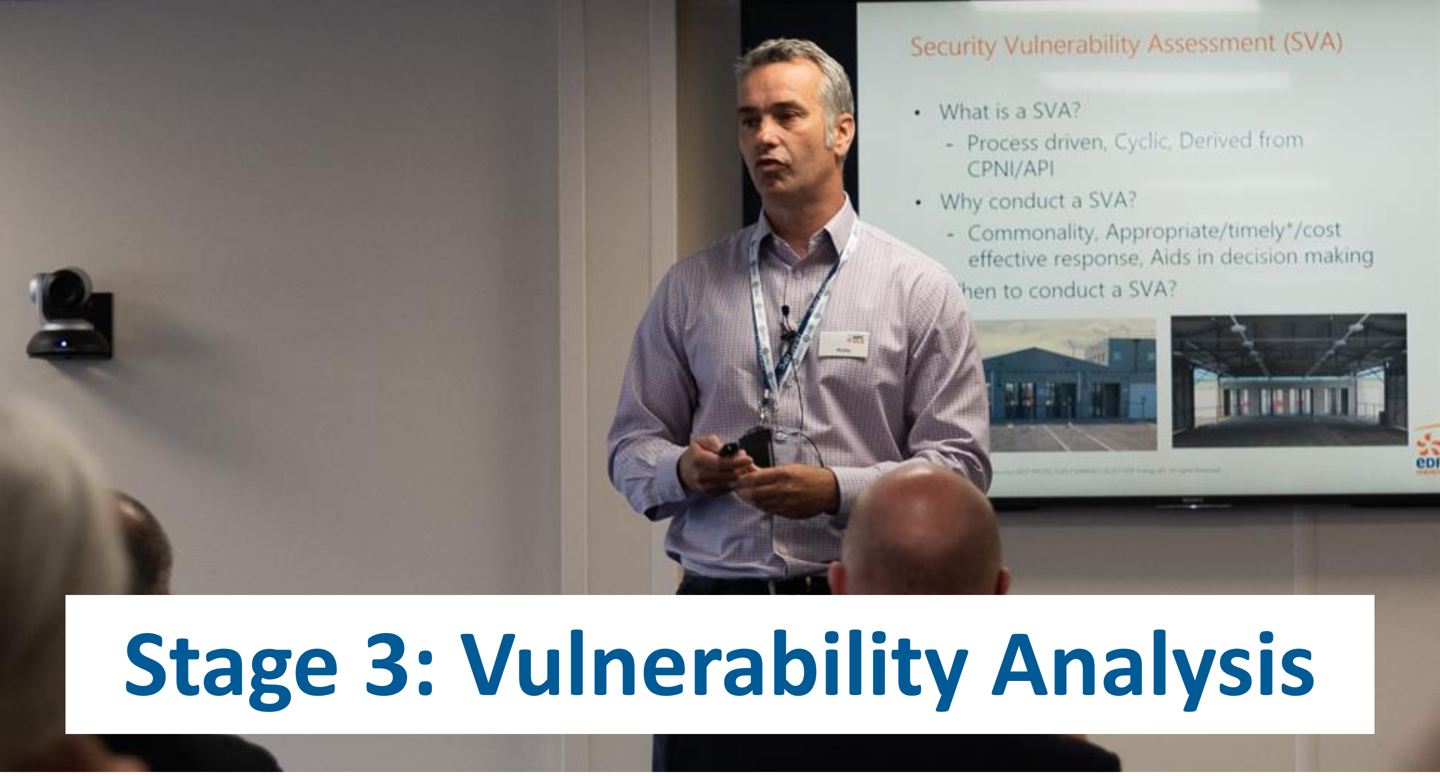
Identifying the Attack Methodology. It is necessary to understand the methodology used to attack the organisation. By asking basic questions, an offender profile can be created. Does the adversary prefer to seek out secluded or hidden areas, do they attack during the nightshift, or do they prefer to steal certain types of property or information? By analysing crime [or event] patterns, the security specialist can identify vulnerable or attractive assets that may require enhanced levels of protection. The method and type of attack is inextricably linked to the motivation and capability of the attacker.

The threat assessment would include documenting the threat actors' strengths and weaknesses – i.e., to steel they would need to remove, pack, hide, and transport the equipment. How easy is this and how much effort would then need to expend for the likely reward.

Threat Assessment Report. The result of this stage would be an assessment report for each adversary or group documenting their motivation, their attack methodology, the tools required, the opportunities that must be present, and any evidence where they have previously carried out their attack – on site, on similar sites, or in a wider context.

The CAP Way™ *StoryBoard*® 03 offers a method to record an adversarial threat assessment. The adversarial threat assessment report should be a controlled document and only shared on a 'need to know' basis.

Consider physical & cyber-attacks


Security Vulnerability Assessment (SVA)
What is a SVA?
- Process driven, Cyclic, Derived from CPNI/API
Why conduct a SVA?
- Commonality, Appropriate/timely*/cost effective response, Aids in decision making
hen to conduct a SVA?

Stage 3: Vulnerability Analysis

Vulnerability: "a gap in a layered security programme that may be exploited by a motivated and capable adversarial threat actor."

Once we know what, when, and where the assets requiring protection will be, and the who, how, and why they might be attacked, we now need to analyse the efficacy of the current, or planned, protective-security arrangements. This should include the physical, technical, cyber, and procedural controls in place across the organisation for all reasons, i.e., this might be a safety barrier to prevent people walking in to a hot-works area, or a need to register into a hazardous area to acknowledge an understanding of the safe systems of work. Whilst not designed with security in mind, these existing arrangements may have qualities that support a protective-security programme — this is the most efficient way to safeguard the integrity of the asset.

The aim of vulnerability analysis is to match the adversary's strengths and attack methodology against the existing or planned defences and, thus, identify and document the gaps.

By '*thinking like the enemy*', the security specialist can critically review the controls in place and establish how easy it would be to attack the asset or system.

It is important to conduct this analysis at the time that the attack is more likely to occur, i.e., overnight, or when the employees are away on their lunch break. This information should have been identified during the previous adversarial threat assessment.

Can the attacker access the work area, collect proprietary information from the printer, steel three employee's personal bags, and walk away unchallenged?

3. Vulnerability Analysis

GAP

Stage 3 Outcome (products):

1. An understanding of the current security arrangements.
2. A list of vulnerabilities (***gaps***) in the current security arrangements that could be exploited by the threat (adversary).

Stage 3: Vulnerability Analysis *The Small Print…*

Adopt a systematic approach. The security specialist should audit or assess the existing or planned layers of defence in three phases; 1) read the plans and operational requirements for each element of the protective security programme; 2) conduct a visual and physical review of the systems or products; and 3) listen to the security operatives or employees whilst they explain their duties or tasks.

Dependent on the time available, the vulnerability assessment should focus on the most business-critical assets identified in Stage 1 of the SMR and those that might be most attractive to the motivated and capable threat adversaries identified in Stage 2.

Think like your adversary. The auditor should place themselves in the mind of the attacker when analysing the protective qualities of each layer of defence. The most obvious protective layers are the site fence and gates; the access control systems at the entrances through which people, vehicles, and materials enter or leave the site; the video surveillance system; or the intruder detection systems that are activated when the workplace is unoccupied. Do they deliver against their design specification, do the operators understand how to use them, and does the information collected via the technical systems influence responsive behaviours or process improvements?

However, holistic security programmes also include pre-employment screening, employee awareness programmes, incident investigations, incident and emergency response plans, and in-house assurance audits. How well known are these processes and do all employees understand the part they play in protecting the organisation.

Think cyber. With enhanced digitisation, automation, and system connectivity via the Internet of Things, the vulnerability assessment should consider the defences against both physical and remote attacks, i.e., on the building management systems, the data management processes, and the business critical or unique information storage repositories. Are the power or water supplies vulnerable. Could an attack on the critical safety systems close the site or stop work completely.

Start online. An adversary will often commence their attack planning through online research, harvesting as much information as they can without exposing themselves to danger. How vulnerable is the organisation – is it oversharing unnecessarily. Does the online profile showcase robust defensive measures, i.e., alert, and well-equipped uniformed officers, or does it provide useful information that helps plan the attack, i.e., digital site tours, office floorplans, or contact details of key employees.

Accidental adversaries. Employees often unwittingly create security vulnerabilities through ignorance of a preferred behaviour (a rule that enhances protective security) or complacency due to a momentary loss of concentration whilst focussing on alternative priorities (i.e., "I was trying to do my job and forgot about…"). An analysis of the incident trends or disciplinary investigations will identify conditions that allow unwanted events to occur that could be exploited by an adversary. Poor behaviours that go unchecked often lead to poor organisational cultural changes that result in injury, loss of trust, criminality, or even death.

Match strength with weakness. A vulnerability analysis is much more than rattling the fence, drinking tea with the security officer, or checking the incident log; it's about matching the attack methodology of an assessed adversary against the organisation's holistic security programme and emergency management plan. Where gaps are identified they should be documented for including in the next stage of the SMR process.

The Vulnerability Analysis Report. The result of this phase would be documented, listing the vulnerabilities associated with the asset type and highlighting those assets or systems that the adversary may consider attractive and could be easily damaged or stolen. This would be a controlled document. Unauthorised access to a Vulnerability Analysis Report would significantly help an adversary plan their attack.

Stage 4: Adversarial Risk Assessment

Adversarial Risk: "A measurement of likelihood and impact of a successful attack by a motivated and capable threat actor."

Using an understanding of the adversary's attack methodology, the opportunities they need, and tools required to mount a successful attack (stage 2 of the SMR) and combining this with the manager's knowledge of the asset and how it will be installed (stage 1 of the SMR), whilst also considering the gaps in the existing or future protective-security arrangements (stage 3 of the SMR), it is now possible to assess the likelihood and consequence of a successful attack.

Making informed decisions. Once assessed, and allocated a score, the adversarial risks can be arranged in severity order and presented to the Senior Risk Owner for them to make an informed decision. This will help them decide if, where, and when they allocate their finite resources to better protect those assets that are critical to delivering the business plan. They can also choose to accept the risk and do nothing. Therefore, the results of the Security Management Review process will help to document this decision.

Think like your adversary. By thinking like the attacker, and creating realistic attack scenarios, the security specialist can assess the ease of probable attacks. This will then help create a series of adversarial risk statements to be scored during this stage of the SMR. The risk statement is typically written in three parts; 1) the cause [due to the lack of….], 2) the event [the XYZ will be stolen], and 3) the consequence [causing a 3-month stoppage on the production line].

4. Adversarial Risk Assessment

Stage 4 Outcome (products):

1. A shared understanding of the risks.
2. A list of risk statements (risk register).
3. An impact assessment for each risk.
4. A score for each adversarial risk.

See overleaf for an example risk statement

Stage 4: Adversarial Risk Assessment *The Small Print…*

Creating an Adversarial Risk Statement. It is recommended that the adversarial risks identified within the scope of the SMR are recorded by creating a three-part structured 'risk statement' as follows:

Part 1: define the cause — **Part 2**: document the event — **Part 3**: describe the effect on the asset or system.

It is unwise to simply state that 'there is a risk of theft', and then attempt to quantify the consequences without first providing some context to when, where, why, and how that theft may occur. Once identified, the realistic adversarial risk can then be scored by likelihood of it succeeding and the impact or consequence after it occurs. This then provides a subjective risk score. An example of an adversarial risk statement is:

Risk #	Risk Statement	Likelihood	Consequence	Risk Score
1	Due to the lack of control at the entrance of the work area there is an increased risk that unknown person(s) can sabotage installed equipment rendering it unusable. This could impact commissioning, increase cost, or delay production and lead to reputational damage.	5	3	15 - High

Standard Scoring of Adversarial Risk. To deliver a meaningful and standard result, the organisation requires a tool or system to consistently measure adversarial risk. *The CAP Way™ StoryBoard®* 02 provides an example Adversarial Risk Scoring Tool that helps measure risk where the consequence indices reflect the Senior Risk Owner's tolerance to risk.

If available, it is always useful to share operational experience or event trends for previous attacks that have negatively impacted the organisation or similar assets or systems being reviewed. This helps communicate the presence of an obvious and realistic danger. This will influence the likelihood score.

Scenario-Based Workshops. An impactful way of developing a common understanding of the consequence of an attack is to convene a stakeholder workshop and use a credible scenario to tease out the 'so what' once the attack has occurred, the loss realised, or the damage is identified.

The CAP Way™ has an *Adversarial Risk Impact Assessment Form* to facilitate and record the findings of this workshop. By holding a stakeholder workshop for each asset, process system, equipment type, or areas, the scenario-based *Adversarial Risk Impact Assessment Form* would identify the total impact of an attack, including financial, schedule, reputational, or other impacts.

This workshop would use the collective knowledge to document the response to the event or emergency, list who and when each stakeholder would be notified, if and to what extent work would be stopped, would an investigation be required, how would the damage or loss be quantified, would it impact on the safe systems of work, how and who would repair the damage, and would this repair work unduly impact on delivering the business plan.

Adversarial Risk Register. The result of this stage would be a series of adversarial risk statements relating to the asset type. These risk statements would be uniquely numbered and registered into an organisational adversarial risk register. When required, these risk statements would be inserted into a bespoke document and presented to the Senior Risk Owner for them to make an informed decision.

The CAP Way™ recommended risk register would be an MS Excel document with each tab reflecting the risks associated with the asset type, i.e., proprietary information, building management system, production line, control room, server room, office block, car park, etc. The register would be a controlled document, but individual risks could be extracted, adapted as required, and included in an adversarial risk report for use across a wider audience – on a 'Need to Know' basis.

Stage 5: Design Arrangements

Designing an Integrated Solution. Having reviewed the adversarial risks associated with the organisation's assets or systems, the Senior Risk Owner will ask the security specialist to draw up numerous protective-security options, estimate the outline cost of each, and create a realistic schedule to deliver each option. This will require the security specialist to engage others to explore cost-efficient and achievable alternatives.

A Need for Defence-in-Depth. There is not a 'silver-bullet' for the protection of all assets and no one security measure will provide a fool-proof solution to all types of adversarial attack. There is a need for multiple layers of protection to provide the much desired 'defence-in-depth', each element of which should help deter, detect, and delay an attack to provide the necessary time to initiate a pre-planned and proportionate response. This concept is explained more in *The CAP Way™ StoryBoard®* 04 *Managing Security Vulnerabilities: Defence in Depth*; and *StoryBoard®* 24 – *Collaborative Protection: Working with Others in the Organisation*.

Interim Protective-Security Needs. There may be a need for a short-term interim protective-security solution to mitigate the adversarial risk until the approved solution is operational; however, ideally, the design process for the permanent solution should commence at the earliest time possible. The higher the risk the greater need for immediate mitigation.

Behavioural-based Security. A simple, affordable, and expeditious solution is to change the workforce behaviours (driven by policy or procedures) shared through impactful communications, effective training, and management supervision.

5. Design Security Arrangements

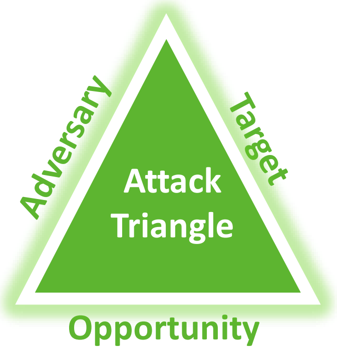
Stage 5 Outcome (products):

1. Operational Requirement.
2. Security Plan.
3. "as built" drawings.
4. Residual risk register.
5. Listed in SMR Register.

We don't do security,
we do everything securely…

Stage 5: Design Arrangements *The Small Print…*

Expanding Existing Security Arrangements. Most of the outcomes delivered through the design stage of the SMR for existing sites or for existing systems or processes are intuitive, often based on the experience of those involved, and regularly seen as an extension of existing security systems, workforce behaviours (proscribed through procedures), or influenced by the conscious bias of the security specialist or Senior Risk Owner. Existing protective-security methods should always be tested in the context of the risk being mitigated and the ability to deliver at scale across the assets, buildings, or systems requiring protection. Placing electronic access control on all building doors and installing surveillance cameras to observe every asset or space is unrealistic and very cost prohibitive. Innovation, flexibility, and a potential need for continual change are essential components to provide sustainable methods to protect an ever-changing workplace, publicly accessible location, or short-term event.



The Attack Triangle. Each layer of protection must positively impact one of the three elements of the attack triangle. The aim is to reduce the opportunity for the adversary to interact with the asset (their target) using the simple premise of, ‘*If they can’t physically or digitally touch it, they can’t damage, steal, or deny the use of it*’.

Adversary: a motivated and capable person or group acting with malicious intent; the human cause of an unwanted incident.

Opportunity: a time or set of circumstances that makes it possible to do something.

Target: a person, object, or place selected as the aim of an attack.

Collaboration with Others. The tendency to leap to technology and deploying security officers must be discouraged in favour of adapting existing workplace safety, environmental, sustainability, building management systems, quality assurance, or emergency management plans, processes, or procedures — most of which are documented within the organisation’s strategic suite of management documents that were identified during Stage 1 of the SMR.

Small changes to existing processes may provide enhanced levels of protection without the need to inflict additional bureaucracy or time consuming ‘barriers’ to efficient working practices. Empathy for the success of others, mutually beneficial processes, and enabling solutions are often the most impactful.

Changing Behaviours. The most cost-effective approach is through behavioural-based security and the adoption of processes that deny the opportunity for the adversary to plan, execute, or prosper from an attack. By removing the opportunity for the attack to succeed, or minimising the negative impact of a successful attack, the ability to return to normal business activities at the earliest opportunity will improve.

The Operational Requirement. Once the Senior Risk Owner has decided to close a gap in the existing protective-security defences, the security specialist should write an Operational Requirement (OR) highlighting the outcome to be achieved; in effect, setting out the specification to which the future solution should meet. This document should only include sufficient information to enable the stakeholders to design and estimate the cost of a limited number of concepts or solutions, with an outline delivery timeline, to allow the Senior Risk Owner to indicate a preferred option. This can then be further developed prior to the final approval and budget allocation.

Criteria - set by others
Constraints - legal compliance
Considerations - of the stakeholders

Stage 5: Design Arrangements *More Small Print…*

Combine '**protective security**' with '***industrial safety***'

Integrated Security. The most impactful security programmes consist of multiple elements each of which complement one another. Designers should first consider changing behaviours such as denying unnecessary access to unauthorised people, enhancing supervisory oversight, or implementing a two-person rule to avoid insider risks. Affordable solutions also include an increase in security posture with more frequent uniformed security patrols, increasing the number of security signs and information posters, and encouraging workers to attend relevant, important, and role-specific security awareness training sessions.

The "***two-person rule***" is a security practice that requires the presence or cooperation of two authorized individuals to perform certain actions or access certain sensitive information. This rule is often implemented in high-security environments, such as military facilities, government agencies, and critical infrastructure installations, to add an extra layer of control and reduce the risk of unauthorized or malicious activities.

The next level of protection may include providing secure storage for information, tools, or attractive assets to deny the adversary access to them. Consider implementing a challenge culture by curious employees when they recognise suspicious behaviours or conditions, and providing reporting mechanisms for engaged people who wish to notify management, or Security, of their concerns.

Additional to a proportionate security culture, it may prove necessary to enhance the physical or technical security infrastructure to close identified gaps in the defence. This often requires capital investment, the initiation of a design and installation project, and sufficient time to bring the upgrades online. This may also require considerable stakeholder engagement and approval from Facilities Management or senior leadership.

Update Security Documentation. Once the revised security arrangements are operational, and where significant change has occurred, it is necessary to update the security related documentation; this may include the organisation's Security Management Plan (SMP), a site or system-specific security plan, or the organisation's Security Operational Procedures (SOPs). Where the security service provider or supply chain partners are affected, it may also be necessary to change their documents, Assignment Instructions, or SOPs.

Management of Change. If technical systems or infrastructure is installed, adapted, or augmented, then updated 'As Built' drawings and installation packs depicting the revised configuration are necessary. It is important that the security system preventative maintenance plans are updated to include the additional infrastructure.

Understanding the impact of the expanded systems and additional infrastructure has on the existing network is critical to the smooth running of the operating security systems and 'change' must be managed appropriately.

If they can't physically or digitally touch it, they can't damage, steal, or deny the use of it.

Stage 5: Design Arrangements *More Small Print…*

Residual Risk. The option or combination of options, which achieves the lowest level of residual risk should be implemented, providing that grossly disproportionate costs are not incurred. Residual risk can be defined as the risk that remains after the selected measures have been implemented. While it is not expected to eliminate all risks, the SMR process aims to reduce risk to as low as reasonably practicable (ALARP).

So, this means, when evaluating or deciding on controls, it is necessary to achieve the lowest level of residual risk. There is a need to recalculate the residual risk once the revised controls are operational. If the residual risk remains high, ALARP has probably not been achieved, and it may be necessary to revisit the SMR process.

Record the SMR. Completed SMRs should be recorded within the organisation's SMR Register. This Register does not serve to record the entirety of the SMR findings, but simply records the occurrence of the SMR, the focus of the review, and listing the subordinate documents created during the SMR process.

Communicating Sensitive Information. It would be unwise to create a document consisting of a detailed description of the asset, system, or building layout; a full analysis of the existing gaps in the defence; and then include a series of adversarial risk statements. The aggregation of this information within a single document would create a vulnerability. The protective security classification of such a document would inevitably exclude many of those who would need to act on specific elements of this information.

Clearly, the security specialist and the Senior Risk Owner must have a full understanding of the findings from each Stage of the SMR. However, it is not necessary to include everything into one comprehensive document.

adopt the '***need-to-know***'
and the
'***need-to-hold***' principles

There is a requirement to adopt the 'need-to-know' principle when communicating information and the 'need-to-hold' principle when sharing information. Although people might have a need-to-know something to allow them to make an informed contribution or decision they do not need to hold their own copy of a sensitive document.

Data Protection Rules. The data protection rules enshrine a duty for accuracy, security, and for information to be held for as little a time as possible to enable the purpose to be achieved for which the information is collected. Once this purpose has been achieved, it should then be deleted or destroyed. It is unnecessary for all the SMR stakeholders to receive and hold digital copies of the asset characteristics, the threat actors, the gaps in the protective-security systems, and the adversarial risk statements.

The "***need-to-know***" principle is a fundamental concept in the field of data protection and information security. This principle is designed to restrict access to sensitive information only to those individuals who require it to perform their job functions. The underlying idea is to minimize the risk of unauthorized access and disclosure of sensitive data. Implementing the *need-to-know* principle is an essential part of a comprehensive data protection strategy. It helps organizations minimize the risk of data breaches, insider threats, and unauthorized access by ensuring that access to sensitive information is granted judiciously and aligned with business needs.

The "***need-to-hold***" principle is a similar concept whereby the user of sensitive information should retain personal or sensitive information only for as long as it is necessary to fulfil the purposes for which it was collected. This principle is closely tied to the idea of data minimisation, which emphasises collecting and processing only the data that is strictly required for the intended purpose.

Stage 6: Review Arrangement

Most organisations operate within complex and diverse workplaces consisting of multiple buildings, work sites, or processes involving expensive or hazardous items, equipment, or instruments. Moreover, this may involve several teams working simultaneously and often side-by-side.

The characteristics of the work area, activities being performed, and the associated hazards are different when moving between each building, each floor, and often between adjacent rooms. Similarly, the ownership, accountability, and responsibility to provide a safe, compliant, and secure work area changes across the site and therefore, each building, floor, room, or work area may require a bespoke protective-security model to safeguard the integrity of the assets or systems.

Much of the why, what, and how the organisation's people, property, & information can be protected is mentioned elsewhere in this Guide. However, there is an absolute need for continuous review of those protective-security arrangements to ensure they remain proportionate, effective, and evolve with the business plan and operating processes.

Responsibility to Review the Security Arrangements. Typically, the responsibility to assure the efficacy of the protective-security arrangements that create and maintain a safe workplace will fall to the department manager, team leaders, process owners, supply chain management, or service providers. Essentially, the accountability lies with the leader of those that perform activities in the place provided to deliver their element of the organisation's business plan. It is recommended that the 'responsible person' collaborate with the security specialists and continuously audit, review, verify, and improve their protective security arrangements.

6. Review Security Arrangement

Stage 6 Outcome (products):

1. Updated executive endorsement.
2. Updated SMR documents.
3. An annual SMR Review Register
4. Increased certainty of business success

See overleaf for when to conduct a review

Stage 6: Review Arrangements *The Small Print…*

Reasons to Review the Security Arrangements. Fundamentally, there are five reasons why a work area or activity across the Project would be reviewed; they are:

1) When establishing a site, facility, or service to set a 'benchmark' and/or support the design of security arrangements/controls.
2) An individual, organisation, or sub-team leader is allocated responsibility to protect the people, property, or information.
3) An existing site, facility, or service undergo a significant reconfiguration, change of use, or change of Senior Risk Owner (accountable person).
4) The adversarial risk score substantially changes on the receipt of new information, or when management deem it necessary.
5) Periodic revalidation of previous SMRs, the frequency of which shall be determined by the criticality rating of the site, property, or asset.

Clearly the benchmark review is more labour intensive, but once created, subsequent reviews may take as little as 10-minutes or form part of the weekly (or periodical) walk through. Checks conducted by department managers of team leaders during their health and safety, or emergency preparedness audits can contribute to the formal security management review process.

Quality Management System. The adoption of this security management review (aka. security quality management system) is a strategic decision for an organisation that can help to improve its overall performance and provide a sound basis for sustainable business delivery. The potential benefits of implementing a security quality management system based on this Guide are:

a) the ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements.

b) facilitating opportunities to enhance customer and client satisfaction.

c) addressing adversarial risks and opportunities associated with its business context and objectives.

d) the ability to demonstrate conformity to specified security legislation, regulation, and policy.

This Guide employs the process approach, which incorporates the ***Plan-Do-Check-Act*** (PDCA) cycle and risk-based thinking. The process approach enables an organisation to plan its processes and their interactions. The PDCA cycle enables an organisation to ensure that its processes are adequately resourced, protected, and managed, and that opportunities for improvement are determined and acted on.

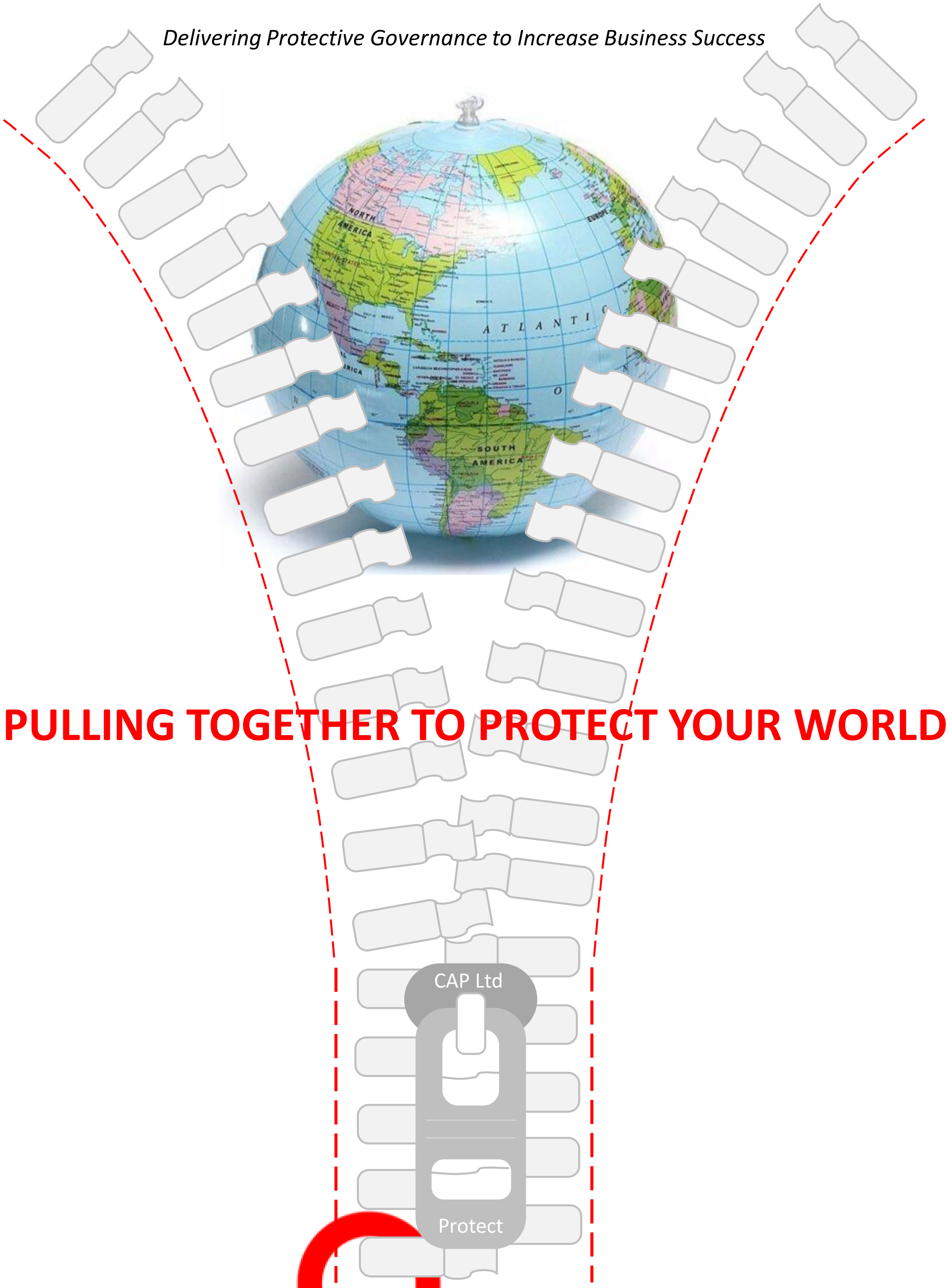
Risk-based thinking enables an organisation to determine the factors that could cause its processes and its quality management system to deviate from the planned results, to put in place preventive controls to minimise negative effects and to make maximum use of opportunities as they arise.

The Security Advisor. The security specialists adopt a role of an advisor to those managers who are responsible for safeguarding the organisation's people, assets, and information. This person, who could also be the Senior Risk Owner, should be the same person who has the responsibility for the safe systems of work, the environmental compliance, and the emergency preparedness plans. It is these people who have a responsibility to generate a secure culture within their allocated work areas and remove the opportunity for malicious actors to impact the certainty of success.

Reference: **BS EN ISO 9001: 2015**
Quality Management Systems Requirements

PLAN-DO-CHECK-ACT

Delivering Protective Governance to Increase Business Success



PULLING TOGETHER TO PROTECT YOUR WORLD

CAP™

CANNON ASSET PROTECTION Ltd

Email: frank@cannonassetprotection.uk