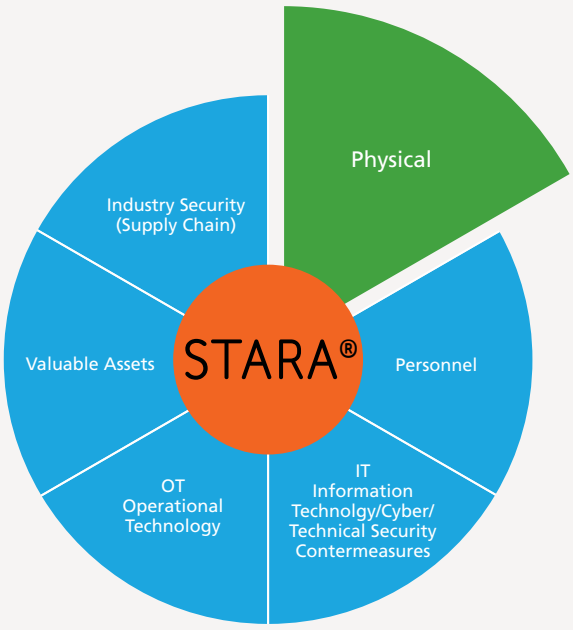
PIRAM™

Physical Infrastructure Risk Assessment and Management

As part of the BAE Systems Security Threat and Risk Assessment (STARA®) framework which provides a holistic approach to helping large organisations determine and assess security threats and risks covering the full spectrum of threats, BAE Systems PIRAM™ provides an organisation with an assessment and testing of the physical security of its critical assets. This relates not just to cyber assets, but can assess the physical security around any kind of asset that an organisation feels is of critical value to its operations, whether it is data (e.g. held on a server in a comms room) or a physical asset (a bank vault, an engine room in a power station, a TV studio, a network control room of a major road junction etc.).

The PIRAM™ capability assesses the maturity of an organisation's physical security in two modules – through **"overt"** means via a Physical Security Architecture Assessments (PSAA) and **"covert"** means in the form of physical penetration-tests (PPT). These modules are designed to assess both the effectiveness of physical security controls as well as how humans interact with them (socio-technical factors). These modules can be delivered individually, together, or as part of a wider STARA engagement.



These modules can be delivered individually, together, or as part of a wider STARA engagement.

Figure 1: PIRAM, as part of the framework for the Security Threat and Risk Assessment for Business and Industrial Operations

PSAA – A maturity assessment of physical security controls

The PSAA will review all of an organisation's physical security controls (such as fencing, lighting, CCTV, alarm systems, access controls etc.) at its chosen location starting from outside the perimeter working inwards. The necessity of this **"outside-to-in"** review is twofold:

- to observe how all controls work together and how humans interact with them – Defence in Depth.
- to determine the effectiveness of controls in protecting an organisation's assets not just from external threats but also from the possibility of threats working from a privileged position within the organisation – the insider threat.

This assessment is done with the full cooperation of the on-site security team in order to get a real understanding of what they are most concerned about when defending their site every day.

We highlight the gaps in an organisation's defences but also suggest short and long term approaches to remediation to keep assets secure.

PPT – The physical compromise of logical assets

A physical pen-test is the most authentic way to measure the maturity of an organisation's security culture. An unannounced covert attack on a client's defences will provide an accurate real-world baseline of the level of its readiness to repel real threats by replicating attack scenarios that an organisation could realistically face within its known threat landscape.

To achieve maximum benefit, it is conducted as a **'Black Box'** test, where with no prior inside knowledge of the organisation and its security controls, our experts will attempt to bypass physical security controls and gain unauthorised access to client's premises. As part of the PPT module, we will conduct hostile reconnaissance of the location both virtually through a detailed Open Source Intelligence (OSINT) gathering exercise, as well as in person on the ground, when we will covertly observe the site from a distance, studying patterns of life and looking for vulnerabilities in defences.

During the test, a combination of techniques are used including the deployment of technical bypass tools such as RFID hacking, ID card cloning and lock picking. Social engineering is also used to deceive staff into permitting the testing team entry to the location they are tasked to defend. Or sometimes we will just walk through an open door!

Although the test is unannounced to the organisation as a whole, target sites, ethics, scope, objectives and rules of engagement are always agreed in detail with the customer's management team at the outset and follow mutually agreed guidelines. This safeguards the well-being of all those– both on the customer side and on the testing team – and ensures maximum benefit of the test to the client.

Reporting and Training

Following the assessments, the PIRAM teams will provide a combined, or individual Final Reports for each module, along with an Executive Briefing document, if requested. This report will describe the process end-to-end, highlight its key findings, and offer commentary on the significance of the highest priority vulnerabilities. If requested in advance, the final report can include a Vulnerability Register and a Risk Register for each or both modules.

A further section on remediation suggestions can also be added which will prioritise the highest scoring vulnerabilities and / or risks. If requested, our team can provide guidance and training to your staff covering security culture and awareness, guard force training and policy and procedure development. This may include:

- a Lunch and Learn presentation to all staff summarising the test and its outcomes and focussing their attention on heightened security and threat awareness as a result;
- a **'walkthrough'** style training session with security guards and / or front-of-house staff at the in-scope site that focusses on how to prevent attacks through increased threat awareness – what to look for, how to spot hostile reconnaissance etc.;
- a **'wash-up'** style exercise with staff involved with the test, walking them through what happened with a lessons learned approach.

To learn more about the BAE Systems PIRAM™ or STARA® engagements, please contact us.

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/digital

linkedin.com/company/baesystemsdigital twitter.com/baes_digital

Digital Intelligence

BAE SYSTEMS