hscic Health & Social Care Information Centre

SIAM Information Assurance

Target Operating Model for HSCIC Information Assurance Practice

Author: Austin France (Info-Assure Ltd)

Date: 31.1.14

Not Protectively Marked

Contents

Background

Info-Assure was engaged by HSCIC to design a strategic operating model for the in-house Information Security function. The function will initially provide Information Assurance and Security Operations services to Spine2. It will later be extended to the wider community to replace services currently provided by outsourced service providers.

Objective Of Target Operating Model

The new operating model was designed with the following objectives;

- Align with wider HSCIC Service Integration and Management (SIAM) Model
- Define Services to be provided by the Security Function to Spine 2 and future programmes
- Define the Team Structure
- Define interfaces between the security teams and programme Service Consumers
- Estimate existing capability and set out the vision for target capability
- Align With Cyber Security Review Findings to increase capability and improve overall security posture of the organisation
- Provide in-house capability to carry out security improvements and to address known cyber security issues
- Use industry standard terminology to assist engagement with external stakeholders such as CESG

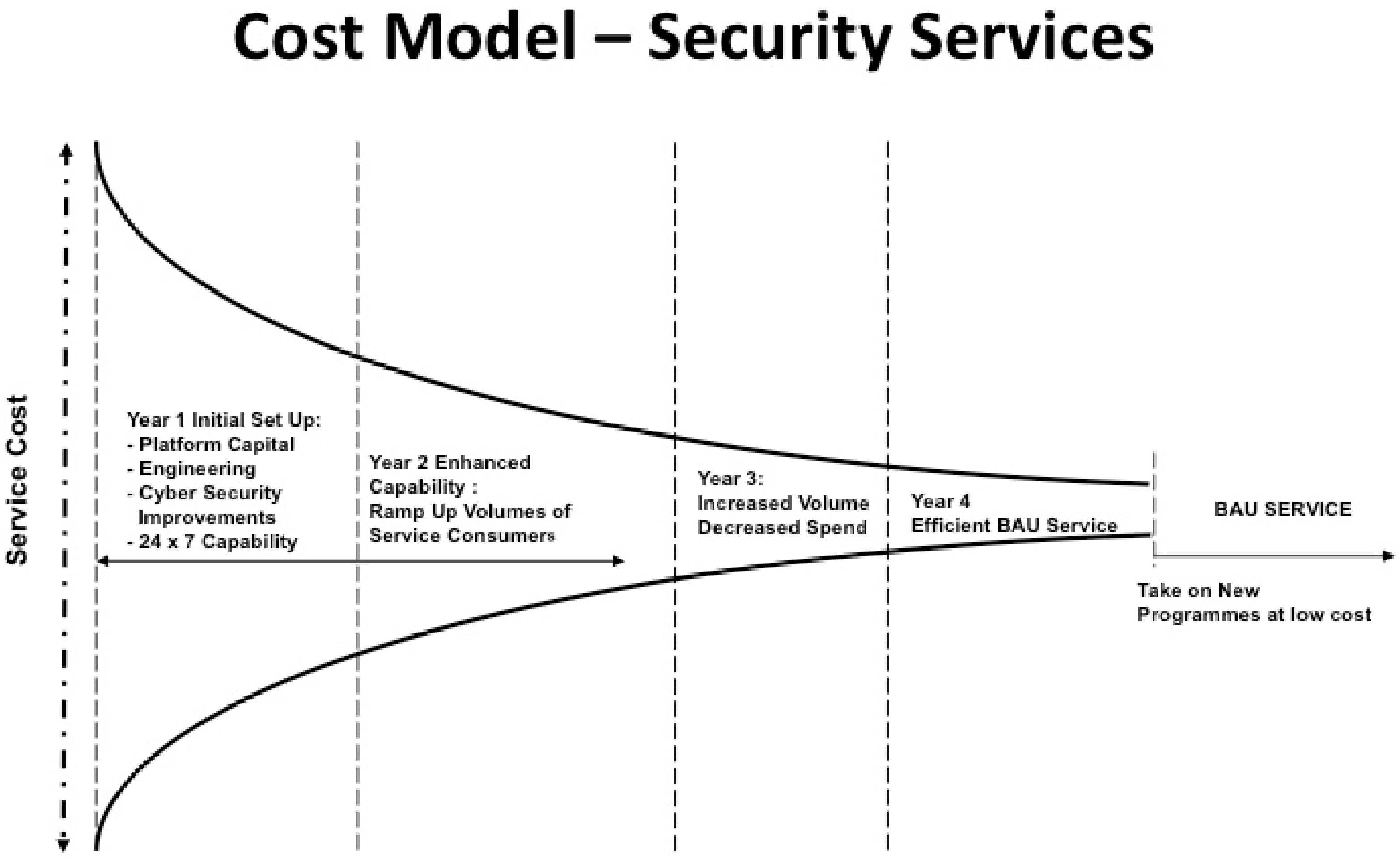
Costs and Benefits of Operating Model

The target operating model enables the organisation to meet the objectives outlined above.

It is understood that there will be up-front costs associated with establishing the commoditised services such as protective monitoring. These costs will be higher for early adopters of the services but will drop off significantly with increasing volume due to economies of scale and greater operational efficiency, until they reach commercially competitive levels or below.

Figure 2 below illustrates this concept of reducing service cost of commodotised security services with increased volume of subscribers over time.

A cross-charging approach for services provided by the in-house security function will enable it to become a revenue generator over time.

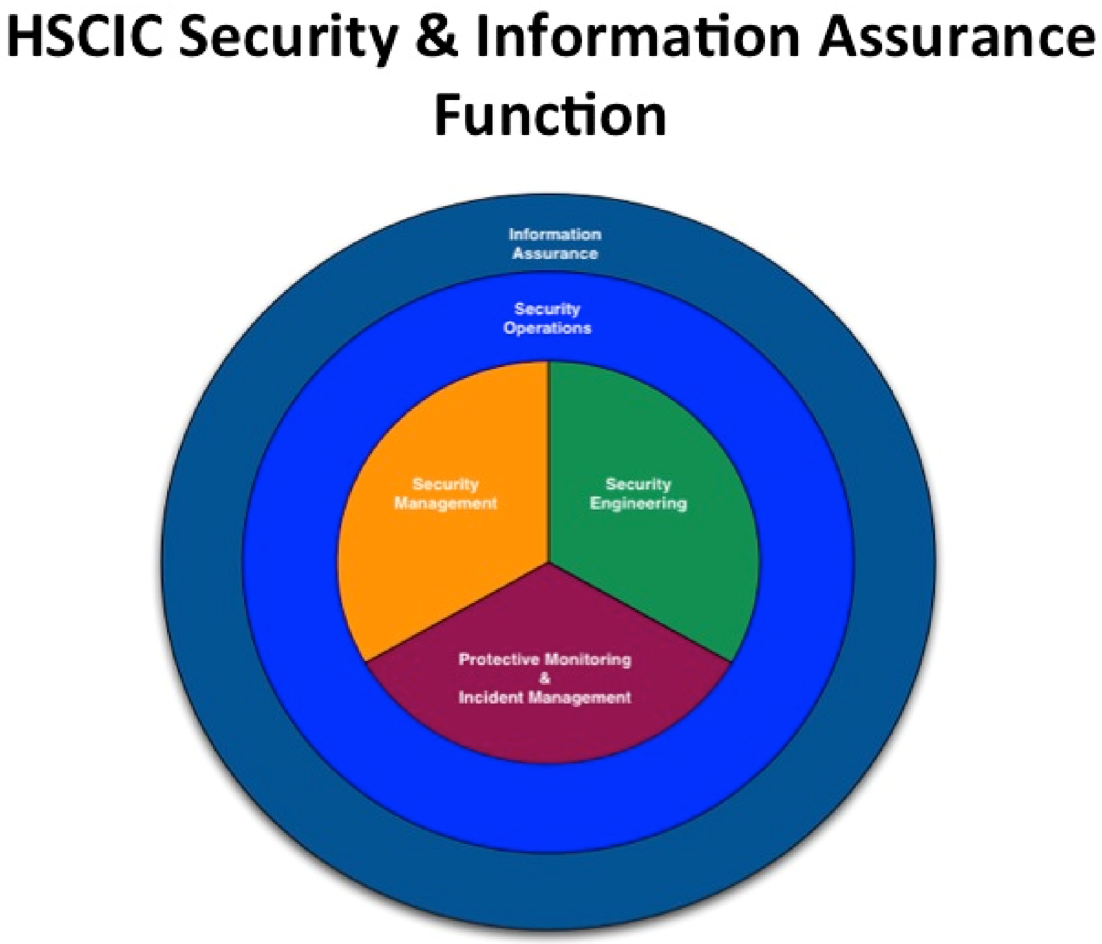


Not Protectively Marked

HSCIC Security & Information Assurance Function

The HSCIC Security function will include an Information Assurance Practice to set out overarching strategy and policy, and to provide information risk services.

Security Operations will interface with programmes on a service provider basis much like the services currently provided by external suppliers. Security Operations will be made up of Security Management, Security Engineering and Protective Monitoring teams.


HSCIC Security & Information Assurance Function
Information Assurance
Security Operations
Security Management
Security Engineering
Protective Monitoring & Incident Management

Security Services and Interactions

Service descriptions have been defined in detail and shared with business stakeholders. These service descriptions can be found in appendix A of this document. The services are outlined at a high level in figure 3 below.

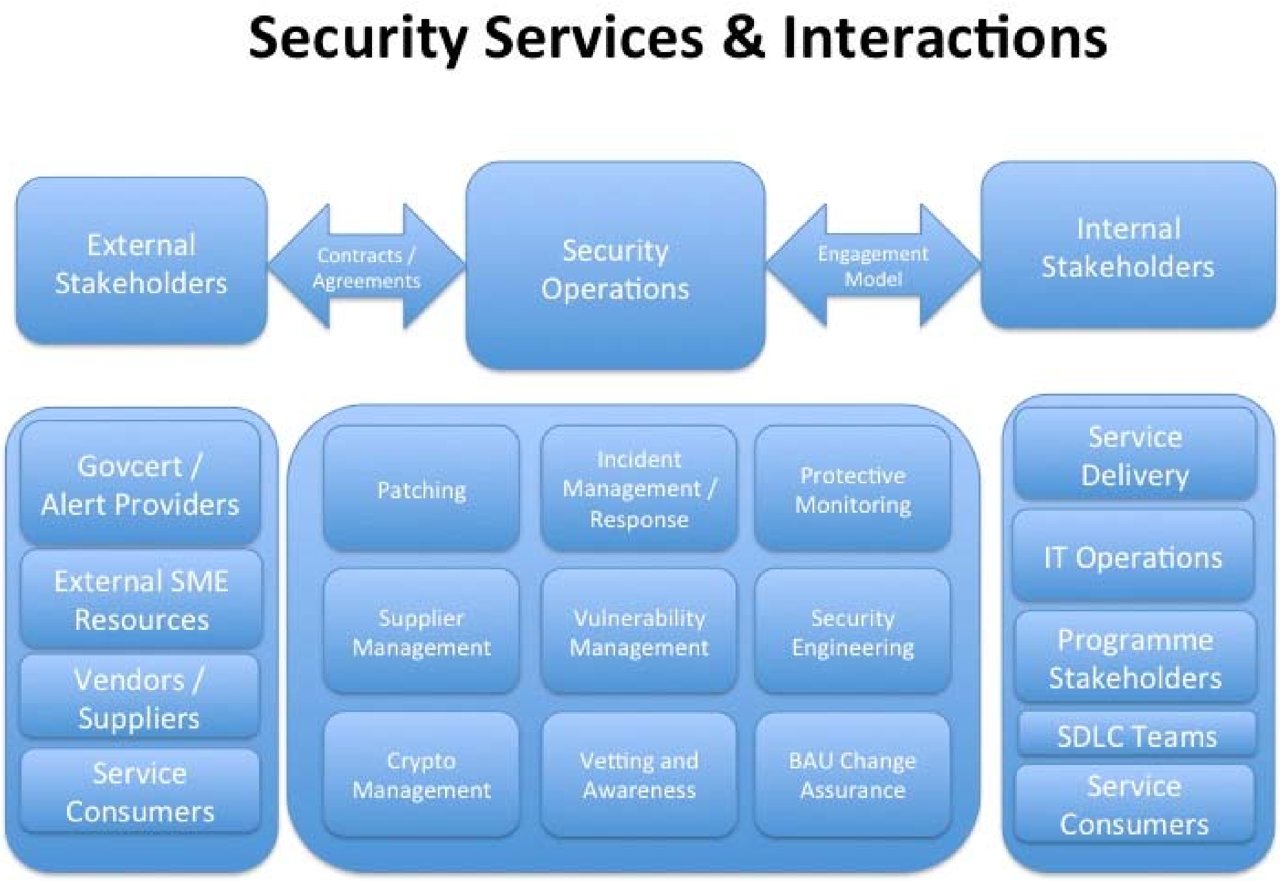


Figure 3

Team Structure

A team structure has been defined to resource the Information Assurance and Security functions. Resource levels have been estimated based on discussions with the existing teams and industry standard metrics for the provision of 24x7 services where required.

Secure Development Life Cycle (SDLC) security consultancy services will be provided by the team at a later time and hence they are included in the model. These services will not be formally in place for Spine 2 inception.

Further work will be carried out by the management team to align existing resources with the new team structure.

The proposed future team structure is shown in figure 4 below.

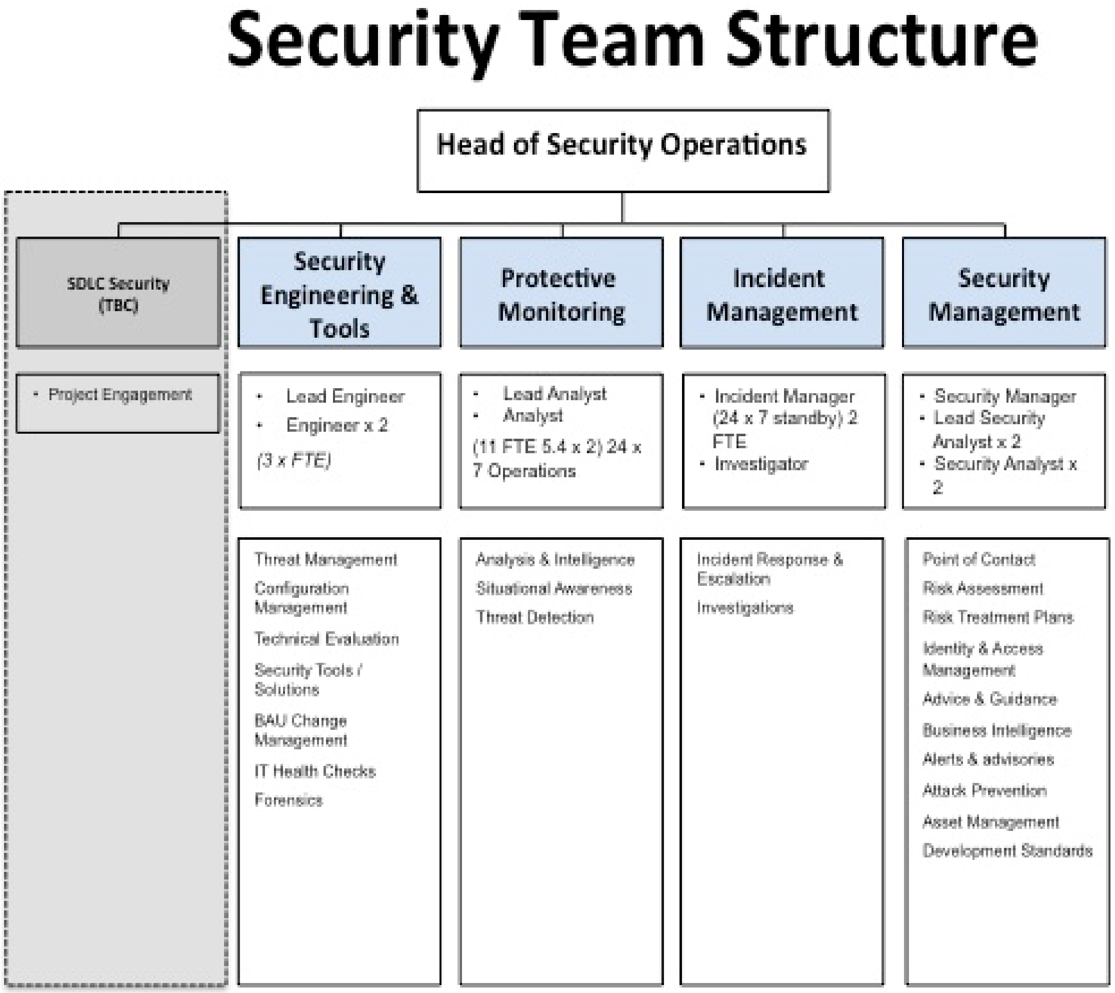


Figure 4

Engagement Model

Effective engagement with internal and external stakeholders will be critical for the success of the Information Assurance function.

Operational Level Agreements (OLA's) will be established for each service interface to define the engagement model. This will ensure that all service consumers understand how to engage with the Security Function. The engagement model will be cascaded formally within the ITIL service management framework and facilitate cross-charging.

The high-level engagement model is shown in figure 5 below.

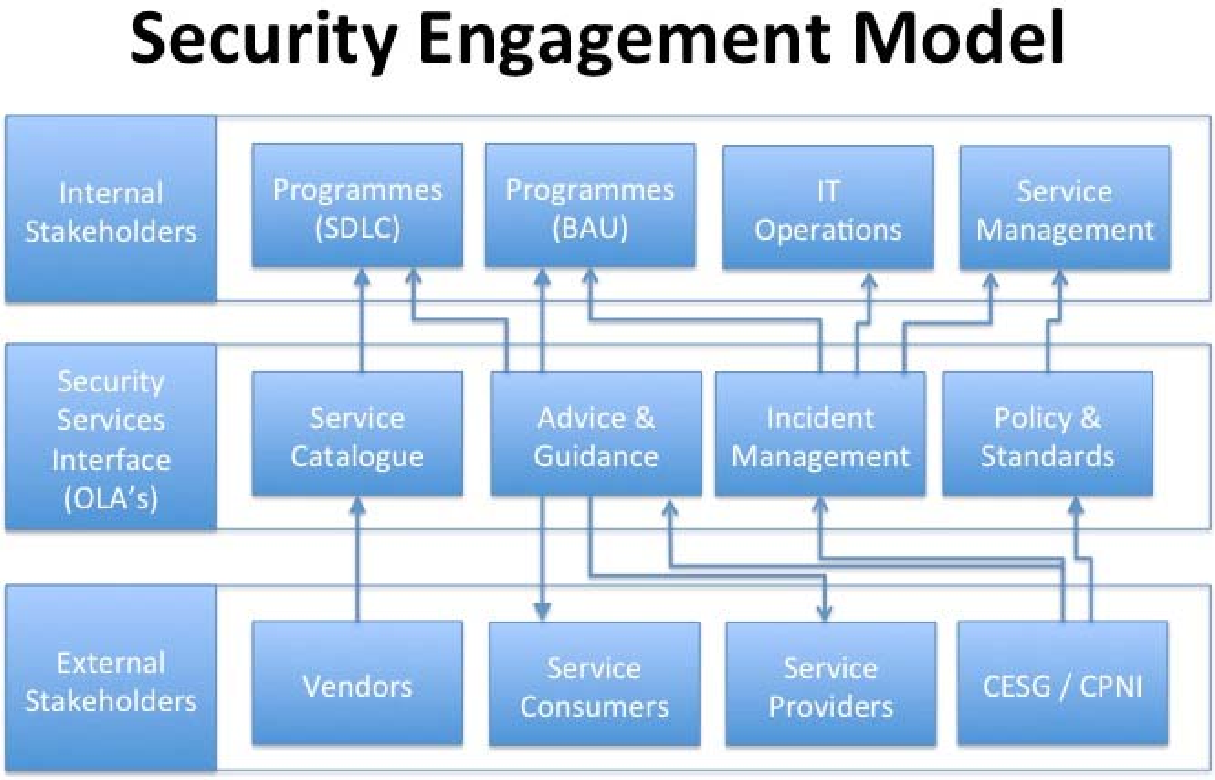


Figure 5

Capability

Significant capability exists within the The HSCIC Information Security function. Historically the organisation has relied on large strategic suppliers to provide the majority of Information Assurance activity.

As part of the definition of the operating model, capabilities required to deliver the services have been identified. Existing capability is illustrated below.

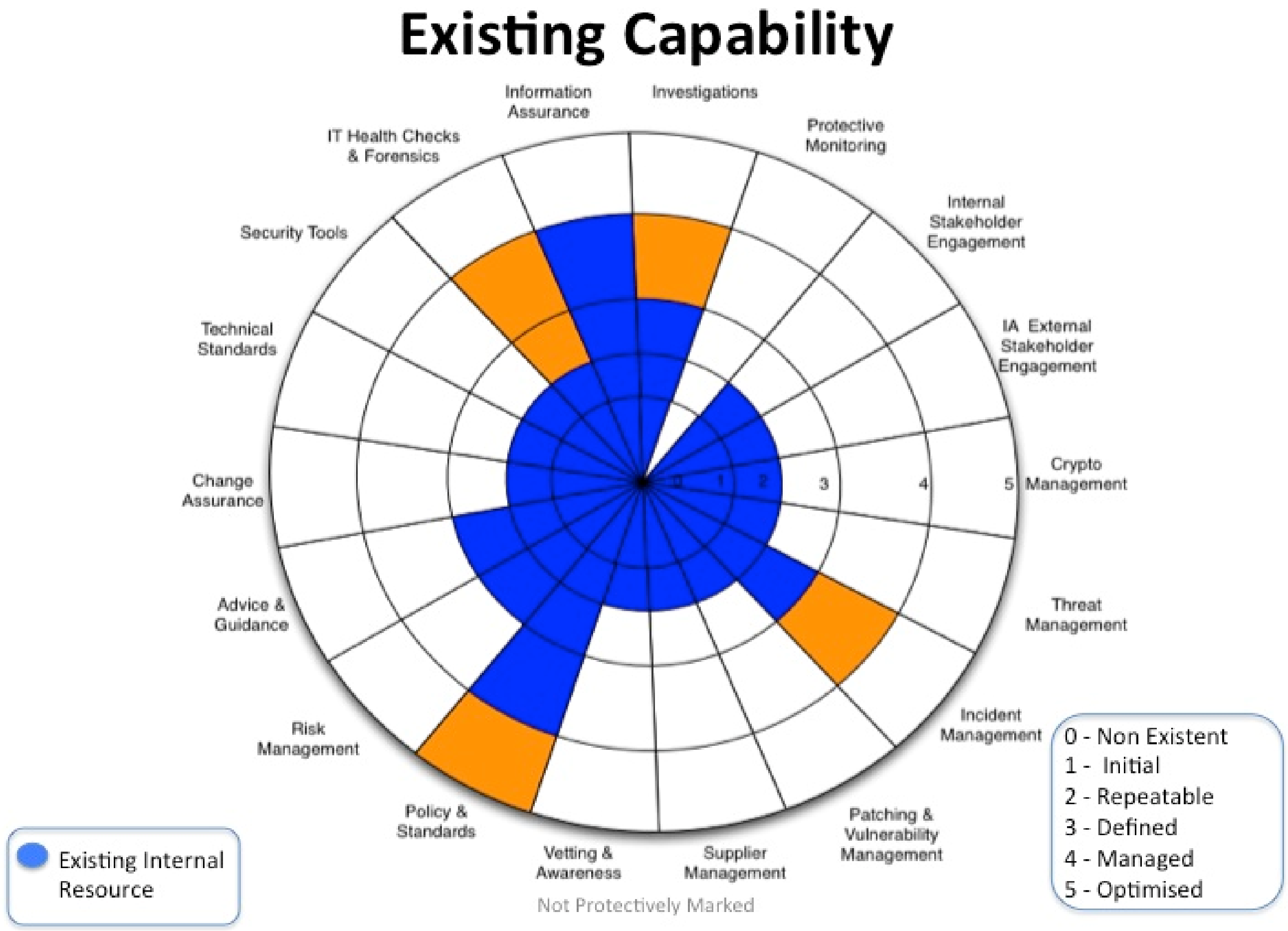


Figure 6

Figure 6 above illustrates existing capability with the mix of internal and external resources in place.

In order to bring full capability in-house to a level that is optimised, the organisation must build on existing resources through;

- Training and up-skilling existing resources
- Recruiting new internal FTE resources
- Developing relationships with specialist providers in the areas identified below through G-Cloud framework

The enhanced capability is represented in figure 7 below

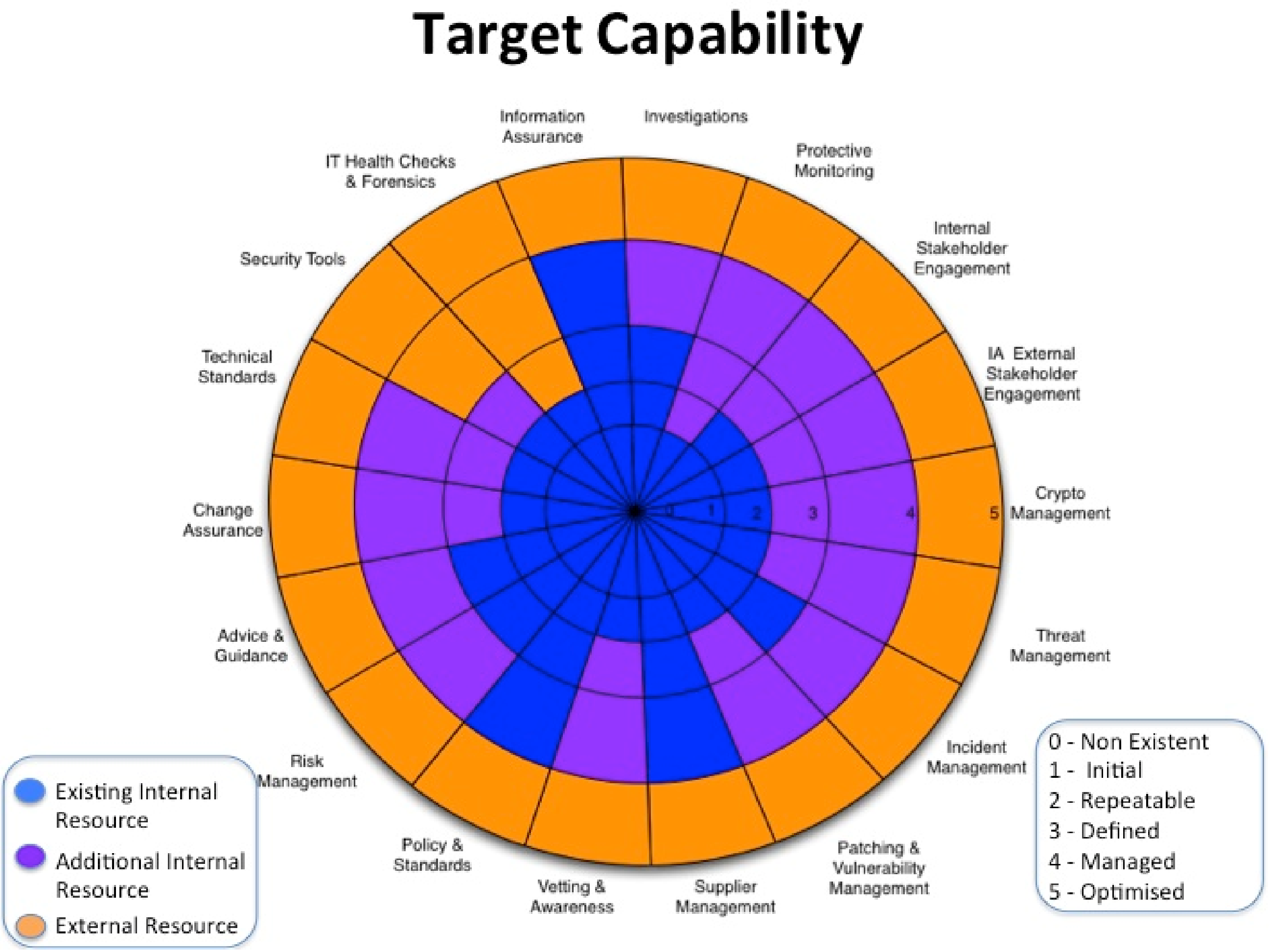


Figure 7 Target Capability

Next Steps

- Ramp up in house and external capability to meet Spine2 requirements through in house training, recruitment and supplier engagement via G cloud
- On-going engagement with wider internal stakeholders to ensure requirements are understood and that the IA message reaches the intended audience
- Work with IT operations and service management to ensure that resolver groups include appropriate security interface
- Define cross charging model for security services
- Define OLA's for security service consumers
- Create a plan to address cyber security review findings within the new security function

Appendix A Service Definitions

Service Definition – Security Management

Security Management Service Overview

A Security Management service will be offered to ensure that HSCIC Security has the necessary management oversight and to provide HSCIC Service consumers with security management services. Security management activity will include;

- Provide a Point of Contact for HSCIC Service Consumers and external stakeholders within HSCIC
- Develop working relationships and agree engagement model for all stakeholders
- Risk Assessment Service
- Risk Treatment Plans
- BAU Change Management / Assurance
- Identity & Access Management
- Advice & Guidance
- Communicate Alerts & advisories
- Attack Prevention
- Asset Management
- Subject Matter Expertise
- Supplier Assurance

Security Management Service Operation and Management

The Security Management Team will report to the Security Operations Manager. The Security Management Team will consist of:

- FTE Security Manager x 1
- FTE Lead Security Analyst x 2
- FTE Security Analyst x 2
- Technical Specialists (call off as required)

Service Definition – Security Engineering & Tools

Security Engineering Service Overview

A security engineering service will be offered to HSCIC Service consumers in order to;

- Design build and maintain security solutions on behalf of HSCIC Security Function
- Design build and maintain security solutions on behalf of Service Consumers
- Develop ‘gold standard’ builds for infrastructure components
- Provide a design authority and input to BAU Change CAB Forum
- Evaluate and select vendor solutions
- Provide configuration management Service for Service Consumer Assets
- Penetration Testing and IT Health Check
- Forensics
- Vulnerability Management

Engagement

- Subject Matter Expertise within the Security Engineering team may be consulted by other functions within Security Operations on a resource managed basis.
- Engineering consultancy may also be provided to service consumers at a cost and subject to demand management

Service Operation and Management

The service will be operated by a dedicated Security Engineering team reporting to the Head of Security Operations

The Security Engineering Team will consist of:

- 1 x Full time Lead Security Engineer
- 2 x Full time Security Engineer
- Technical Specialists (call off as required during)

Service Defnition – Protective Monitoring Service

Service Overview

A protective monitoring service will be offered to HSCIC Service consumers to provide the technology and supporting business processes to monitor system usage in order to;

- Detect and prevent attempted attacks / system misuse
- providing user accountability
- providing a means of treating information system risks
- Meet policy and regulatory security requirements
- Provide skilled staff and process workflow to carry out security incident detection and response

The service will be operated from a dedicated Security Operations Centre (SoC) using industry leading technology, tools and processes. Data feeds will be taken from service consumer environments and fed in to a central log management platform or Security Incident and Event Monitoring (SIEM) platform.

Protective Monitoring Technical Solution

- Facilitation of log collection and storage from each of the core products that make up the overall HSCIC estate and in order to meet the relevant Protective Monitoring Controls
- SIEM (Security Incident and Event Management) function in order to provide event correlation
- Reporting and trending capabilities

Protective Monitoring Activities

- Managing the alerts console 24x7, responding to and investigating alerts in accordance with SLA's
- Providing point of contact for service consumers and external stakeholders
- Escalating security incidents (suspected or otherwise) in accordance with Disclosure and Barring Service security incident management processes
- Reviewing and audit data, in order to identify and investigate suspected attacks
- Review and investigation of audit logs to support other security incident investigations
- Production of reports for service consumer security stakeholders detailing incidents and events identified, the results of follow up investigations, and trends

Protective Monitoring Service Operation and Management

The Protective Monitoring Team will report to the Security Operations Manager . The Protective Monitoring Team will consist of:

- Full time Lead Security Analyst (24x7=5.4)
- Full time Security Analyst (24x7=5.4)
- Technical Specialist (call off as required during set-up and changes to the services)

Service Definition – Security Incident Management

Security incident Management Service Overview

A Security Incident Management service will be offered to HSCIC Service consumers in order to;

- Provide a point of contact for security incident escalation from the Protective Monitoring team, HSCIC Service Management and IT Operations teams and external stakeholders & Partners
- Assess the impact of the security incident on in-scope services and escalate as appropriate
- Manage security incidents based on HSCIC HSSI Process in collaboration with HSCIC Service Bridge
- Coordinate security incident response and liaise with identified stakeholders throughout incident
- Ensure the collection and preservation of evidence for investigatory purposes
- Investigate security incidents, carry out root cause analysis to feed in to security improvement plans

The Security Incident Management Team will be available during core office hours and on an on-call basis outside of normal business hours

Security Incidents or suspected security incidents of an agreed magnitude will be reported to the Security Incident management team by the Protective Monitoring Team, HSCIC Service management teams, or HSCIC Operations teams

Planning Activities

- In addition to live security incident management, the team will also be responsible for the following BAU activities
- Development and testing of security incident response plans and procedures
- Communication of security incident response plans
- Liaison with business, HSCIC Service Management and external stakeholders to establish suitable notification and escalation paths
- Provide advice and guidance to business stakeholders on security incident management
- Training of applicable staff on security incident management procedures

Security Incident Management Service Operation and Management

The Security Incident Management Team will report to the Security Operations Manager . The Team will consist of:

- 2 x Full time security incident managers on on-call rota (24x7)
- 2 x virtual team members (fully trained in security incident management and on the on-call rota but with other related BAU duties)
- 1 x Invesigator

- Technical Specialists (call off as required during set-up and changes to the services)

Appendix B – Stakeholder consulations

Kevin Holland – HSCIC Service Management

Ian Cooke – HSCIC Service Management

Chris Walters – HSCIC Spine 2 programme

Martin Sumner – HSCIC Spine 2 programme

Tom Dean – HSCIC Care.Data programme

Chris Smith – HSCIC Service Bridge

Sam Wood – HSCIC Operations

Peter Spence – HSCIC ICT security Manager

Michael Flintoft – HSCIC Head of ICT

Eve Roodhouse – HSCIC Programme head

James Wood – HSCIC Head of Infrastructure Security

Steve Shaw – HSCIC Operational Security Team Lead

Mike Farrell – HSCIC Infrastructure Security Team