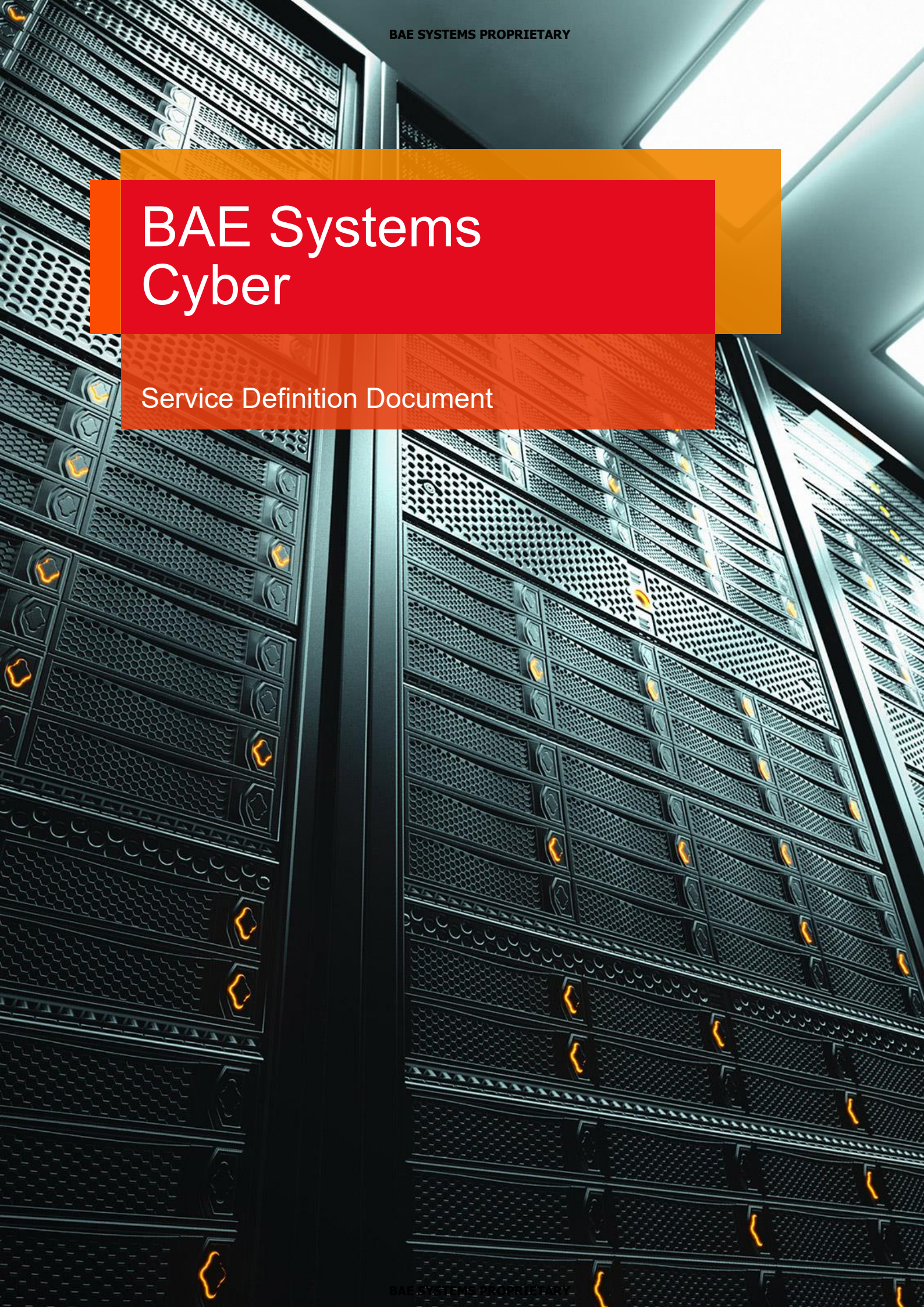

BAE Systems Cyber

Service Definition Document

1 Risk and Intelligence

The Risk and Intelligence offering enables customers to understand and manage risk in a pragmatic and cost effective manner in light of the changing technology landscape, escalating threat and evolving standards. As providers of both cyber security platforms and a comprehensive suite of cloud security services, our security experts have a deep understanding of threat, risk and the mitigations required to manage the full spectrum of security based risks to an organisation. We enable our customers to understand and manage risks arising from the use of cloud services by combining analytics and our world class threat intelligence to support good risk management decisions aligned with both HMG and international best practice/standards.

It uses the latest threat intelligence and risk knowledge to inform the Board level of an organisation, supporting the risk posture, prioritisation of capability, and strategy for risk management. This flows down to project and live service level engagements to deliver risk analysis, security improvement and implementation assurance through the IT lifecycle for the design, implementation and management of Cloud services.

We work with your business and technical stakeholders to establish the questions you need cyber risk to answer and through our proven methods and analysis provide answers and practical recommendations. We can help you identify the specific questions you want to answer with cyber risk analysis. We assess the security of your business operations to prioritise practical recommendations for risk reduction and use unique insight into current cyber threats to assess the scale and nature of how the cyber risk landscape affects how your organisation operates. We communicate at executive level answers to your questions about cyber risk.

Our risk and intelligence services may cover IT, Operational Technology, organisation, cultural and physical domains and working within the scope of regulatory frameworks including Cabinet Office, General Data Protection Regulations (GDPR), Network Information Security Directive (NIS) and others.

2 Security Engineering

Security Engineering service creates new secure systems for organisations or assesses and improves the security of existing systems. Our capabilities span security architecture, security testing and secure implementation, utilising specialist cyber and cloud knowledge to produce solutions that are secure by design which can protect against specific threats.

Our approach allows you to understand the level and shape of the investment your organisation needs, to identify cost savings and thus ensure that you are spending your security budget on what is right for your organisation.

We help organisations improve their security engineering and organisational robustness, including performing architecture reviews and controls assessment (including in combination with penetration testing) to provide technical assurance of the ability of organisations, Cloud services, or applications hosted in the cloud, to withstand cyber-attack, identifying appropriate measures to ensure the resilience of a platform and developing business-driven, risk focused security architectures that traceably support business objectives using a proven methodology.

We also provide deep expertise in specialist areas such as vulnerability research, reverse engineering and offensive security research.

Our Security Engineering services may also cover Operational Technology systems and platforms, including industrial, SCADA and transport or defence environments.

3 Security Operations

Our cyber security operations expertise enables organisations to protect against the full range of risks to their cloud-based operations and assets. From providing visibility of the threats, the ability to respond to attacks, through to training and knowledge transfer, our solutions provide an extensive cyber security capability for the cloud.

The Security Operations offering enables customers to define, implement and sustain operational monitoring and incident response capabilities to a level commensurate with the organisation's risk exposure and focussed on defending its key cloud-based assets. They include a range of advisory and delivery services, including integration with BAE Systems threat analytics technology.

Casual attackers may be defeated by well-maintained defences. But targeted attacks are launched by determined adversaries who use research and repeated attempts to identify weak links and evade safeguards incrementally.

We advise organisations on their security operations, including defining the security operations required based on the threats faced by the client, delivering tailored maturity assessments with associated gap-analysis and developing a security operations roadmap and performing detailed design work to help define the business and/or technical blue prints required to build their security operations capability.

We implement the required security operations within a client organisation, including executing the design, implementation and operation of the security operations capability and helping clients improve their capability, including process and architectural improvements, and demonstrating value from security operations to deliver pragmatic and tangible benefits.

4 Privacy and Trust

Privacy is an evolving and complex landscape. Organisations must build "digital trust" with their users in order to successfully operate in the cloud. We work with our customers to help them manage privacy in a way that builds customer trust and embeds excellent privacy practices into their operations. This requires full engagement with the privacy agenda and proactive engagement with customers and users to build the trust and establish where and how trusted services can gain maximum engagement with their target audiences.

We advise organisations on privacy principles and digital trust, including understanding the art of the possible to enable optimisation within privacy demands and constraints, and investigating the differing requirements for digital identity (citizen, customer, staff etc.) and defining strategic approaches to managing these.

We design and / or implement privacy principles and digital trust, including evaluating business process and data flows to ensure privacy by design principles are implemented throughout the organisation or programme and designing the key elements of end-to-end identity management within a particular business process, in particular integration with identity providers.

Typically we may look at General Data Protection Regulations (GDPR), the Data Protection Act (DPA), Privacy and Electronic Communication Regulations (PECR) and other regulations depending on jurisdiction.

5 Cyber Transformation Programme

Our cyber transformation programme services will support and enable organisations to design, implement, adopt and manage security change and transformation to enhance the overall maturity of an organisations security architecture/practices. Our Security Transformation Services are focussed on ensuring organisations are able to undergo change and transformation, whilst still achieving the targeted security and risk benefits. Our Security Transformation Services enable organisations to:

- Identify, scope, plan, deliver and realise the benefits from security transformation programmes, projects and initiatives.
- The identification and development, benefits identification, tracking, management and realisation, change management, reporting, stakeholder management and delivery.
- Ensure the targeted end-state and security and risks benefits are achieved in the face of changing external threat, technology, competitive and geopolitical landscapes, and internal organisational change and evolution.

Our approach and implementation is tailored to the organisation's own structure, constraints and business context. Our teams integrate into the organisations wider change transformation, security, risk and governance structures, along with internal and external stakeholders to enable delivery as part of the organisation, and its wider supplier ecosystem.

As part of Security Transformation, we may include any of our other services, as necessary to deliver the transformation objectives such as access to our specialists security and cyber capabilities including research, development, penetration testing response advisory and consulting services, whether in the ICT or Operational Technology domain.

Our threat-led and risk based approach ensures the scoping, delivery and management of security programmes remains relevant to the business and organisational challenge and context, and changes in the wider ecosystem.

6 Security Management Services

Our Security Management services offer information assurance, compliance and accreditation management, as well as security and penetration testing and a range of further security-focused capabilities. This service reduces the risk of information compromises and security breaches, and improves response effectiveness in these situations.

We enable customers to scope, run and manage the security of the organisation at any or all of tactical/operational, management and strategic layers. Our Threat-led Security Management Services are integrated into the overall organisational security risk and governance, and internal and external stakeholders, include third party suppliers, to continuously:

- Review, assess and manage the risk to your organisation. Responsibility for management and maintenance of accreditation status and risk across your ICT and Operational Technology (OT) estate.
- Integration and working with internal and external stakeholders and supplier.
- ISMS definition, management and maintenance.
- Provide business relevant reporting, KPIs KRIs and KGIs to leadership and governance team as part overall organisational risk governance.
- Support projects and programmes throughout their lifecycle, and integration into operational and transformational initiative, activities and functions.
- Delivery of security technical design authority, assurance and support.
- Incident management, reporting and response.
- Leadership and strategy.

Each service is scoped and tailored to your operational and organisational context, to integrate into your organisation, as required, to support and augment our current capability. Our services may be delivered to support, bolster or augment existing capability or deliver security management and coverage of dedicated business areas, functions or capabilities. Our Services make use of our capabilities and insight including our threat research, intelligence risk, and specialist cyber capabilities to support the security and risk management of our customers.

Our Service ensure that a consistent and appropriate approach to security is applied across both your ICT and OT domains, through integration and collaboration with internal teams, functions, wider Service Integration partners, Managed Suppliers, Cloud Suppliers and other third party organisations and stakeholders, including regulatory if required. While responsibility for accrediting individual systems rests with the relevant Business Areas or Managed Suppliers, the Security Management Service may retain responsibility for the accreditation status of the overall ICT and OT estate and the risk profile that it presents.

7 Penetration Testing Services

7.1 Summary

Our CREST certified Penetration Testing Services provide fixed price and day rate based penetration testing services for comprehensive application and infrastructure penetration testing. Penetration testing serves a number of benefits, including testing an organisation's defences against targeted and untargeted attack, ability to detect intrusions and security vulnerabilities with each service tailored to address the differing vulnerabilities and attack vectors.

Our Penetration Testing services support an organisation to determine whether its products, applications, networks and structure are sufficiently resistant to cyber security threats and to understand their vulnerability to attack. We provide Security and Penetration Testing services to government agencies and departments, banks, and the telecommunications, e-health, aerospace, IT security and legal sectors.

BAE Systems is a Council of Registered Ethical Security Testers (CREST) member company in both the UK and Australia, the emerging global standard for the delivery of penetration testing. The BAE Systems Security and Penetration Testing services in the UK and Australia are registered under this scheme and all of our global penetration testing services are delivered to the same rigorous standards and methodologies. The BAE Systems penetration testers are on a training path to obtain individual CREST certifications in ethical hacking and we aim to ensure all testing is led by a CREST qualified consultant. In addition, BAE Systems can provide IT Health Checks in accordance with the CESG CHECK scheme, in which instance BAE Systems utilise Perspective Risk as a subcontractor where appropriate and in prior agreement with the Customer.

7.2 Application Security and Penetration Testing

BAE Systems' Application Security and Penetration Testing service focuses on business applications hosted on organisation-owned or outsourced ICT infrastructure and tests these for security vulnerabilities that may be exploited in an attack. Typical targets for application-level security testing include in-house and commercial off the shelf applications including: web applications and services; client-server applications; expert and bespoke applications; and mainframe applications. As our senior technical personnel are qualified software engineers as well as IT security professionals, we are able to provide a level of specialisation and differentiation in the testing of security for non-standard systems including: legacy systems, midrange/mainframe integration, proprietary protocols/encoding, thick and thin client systems, and other system types where automated testing is not possible.

7.3 Infrastructure Security and Penetration Testing

BAE Systems' Infrastructure Security and Penetration Testing service focuses on ICT infrastructure and facilities supporting the delivering of business services and tests these for security vulnerabilities that may be exploited in an attack. Targets for infrastructure security testing include: Internet-facing infrastructure; internal fixed network infrastructure; wireless infrastructure; server infrastructure; end-user computing equipment; and other special purpose infrastructure such as mainframes, storage area networks and cloud computing environments. The most valuable client outcomes for penetration testing services can only be achieved through a combination of: exceptional expert penetration testing personnel; an in-depth body of current IT security knowledge; application of proven technical methodologies; alignment with IT security and risk management standards; and a strict quality control system across the penetration testing effort. Our penetration testing team meets all these requirements.

7.4 Code Security Review

BAE Systems' Code Security Review service allows organisations to identify software flaws which lead to security vulnerabilities, which are often the result of the developer failing to observe secure coding principles and practices. The service is focussed on conducting quality assurance checks prior to release of an application, allowing us to reduce the number of potential security bugs within the code significantly before this enters production. Our application security team have extensive experience in the assessment of a wide range of systems including: ASP.NET/C#/VB/WCF, C/C++, Java/JSP/Struts/Spring, Perl, Python/Django, Ruby on Rails, PHP, Web Services/XMLRPC and AMF.

8 Cyber Incident Response

Our Cyber Incident Response services for G-Cloud comprise models based on whether an incident has already occurred or whether you are preparing for potential future incidents.

8.1 On-demand Cyber Incident Response

For clients who have identified that a cyber-security breach has occurred and may be on-going, we offer a rapid response, on-demand service. We aim to provide immediate advice – suggesting immediate next steps to prevent further damage and secure evidence – and a rapid active response.

Our On-Demand Cyber Incident Response Service is designed to offer you emergency support when you need it most – when an incident has been discovered. This service can be called upon without any prior contract in place with us. We can perform our work in an evidentially sound manner if litigation is a likely outcome of the investigation.

We will start with an initial meeting in which we will confirm and record the initial facts known about the incident. We will advise on potential options for immediate mitigation actions and prioritise data sources for collection.

Once the nature of the incident is understood our team can begin to undertake the required incident response tasks. Our support will comprise the following key activities.

1. Confirm what is known about the incident and understand your key personnel, systems and processes. We will confirm any immediate response required to mitigate critical risks.
2. Capture data, such as logs and disk images, which will contain evidence.
3. Expose the attack by analysing the data and reveal what damage has been done.
4. Remediate the incident by safely repelling the attacker and putting measures in place to confirm remediation and prevent re-infection.
5. Resume business as usual activities and monitor for new attacks.

We will conduct analysis of the initial data to understand the extent of the incident and other data sources and analysis that may be required to answer your questions (such as how did it start, has data been wrongfully taken, how can we remove the threat). We will prioritise the most relevant data and tasks to reach remediation actions and a clean, secure estate as soon as possible.

Throughout the incident we will provide you with regular updates on key findings; ensuring that you are aware of the progress and any urgent actions that need to be taken. We will provide a full report at the end of the investigation detailing the work done, findings and recommendations for further work and estate hardening as necessary.

8.2 Incident Response Readiness

For clients who wish to prepare their organisation ahead of an incident, we offer services to both assess your current incident response capabilities and help you improve where required. A tailored version of this service is recommended at the beginning of a retained service to enable your first responders and our team to react as quickly and effectively as possible when an incident occurs.

We offer a range of services to help your organisation be prepared should an incident occur. These services can be offered standalone or as part of our retained service.

Protecting your estate from incidents is vital; however it is not possible to prevent every incident. We regularly help companies respond to major incidents and understand how much a clear and effective response can help mitigate the impacts of an incident.

Our offerings are aimed at ensuring you can react effectively and rapidly when required. The offerings can be tailored to suit your organisation and requirements, however the typical services include:

- Incident Readiness Assessment
- Incident Readiness Improvement

These are described in the sections below.

8.2.1.1 Incident Readiness Assessment

We will work with you to understand your current incident response capabilities, incident readiness and business needs. We will then tailor our analysis and recommendations to focus on the key areas of risk. The common areas of review and recommendations are:

- Incident response plan (including escalation and key people).
- Data availability and acquisition (logs, disk images etc.).
- Arrangements with third parties (e.g. infrastructure management).
- Understanding of network structure.
- Investigation capabilities.
- Remediation and recovery capabilities.

We will typically perform the above by reviewing current documentation, speaking with staff in key parts of the business (such as IS teams) and running incident rehearsals to uncover any key issues in current capabilities and understanding.

The output from this service is an assessment report containing:

- Review of the current state.
- Requirements for improvement.
- Prioritised, actionable, plan to close the gap – including ‘quick wins’.
- Explanation of risks of current state along with benefits of improvements to support a business case to move forward.

8.2.1.2 Incident Readiness Improvement

This service is aimed at improving and developing incident response capabilities within organisations. The scope of readiness improvements will be very dependent on the current state of incident response in the organisation however typically includes work such as:

- Building or tailoring processes for incident response, including playbooks, quick reference guides and ‘principles’ for response to guide staff involved.
- Specifying systems, software, roles and responsibilities.
- Training of staff (can include support in hiring staff also if required).
- Running incident rehearsals for staff across the organisation and working with teams to implement improvements based on lessons learnt.
- Defining plans for future training, rehearsals and process updates.

Improved incident readiness will enable your organisation to rapidly and effectively react to incidents, ultimately lowering the risks of a major impact on the business from an incident.

The above can be tailored to your requirements – we can provide work from updating documentation through to defining and developing an entire new CSIRT functionality.