RISK MANAGEMENT
Benefits and Considerations
The potential benefits of risk management, in terms of security, operations and finance, too often remain unrealised by those businesses who approach cyber security merely as a ‘box ticking’ exercise.

In some quarters cyber security is focused on the production of security-related deliverables to the satisfaction of a risk manager and strict adherence to control frameworks in order to achieve certification. You may be led to believe that all you must do is produce a set of security documents prior to final acceptance. For example, a security case incorporating a Technical Risk Assessment, Risk Treatment Plan, results from Assurance Testing and some Security Operating Procedures.

Consequently security support is only enlisted at a late stage to produce paperwork for a business solution that has not been considered from a cyber security viewpoint. The typical ‘workaround’ is to engage in a last minute activity to bolt on security late in the development cycle (or even in the manufacture phase). More often than not the outcome from such an approach is a series of costly modifications that make the capability secure, but unfit for its intended purpose and an impediment to business processes.

Risk Management need not be complicated or expensive. However, like any other management activity, it must be based on sound expert knowledge, business judgement combined with the rigorous application of best practice. In this case, best practice is based on a risk management process, which formally captures and, where appropriate, mitigates potential impacts that will affect the business.

By applying sound risk management processes within the business, and at the specific project level, a clear link can be achieved between the business objectives and cyber security risks.

This will ensure that investment decisions related to control measures are proportional and are effectively managing the risks to the business.

1 In MOD terms a DAIS Accreditor
4 In MOD terms a Risk Management & Accreditation Document Set (RMADS)
The appropriate governance regime ensures a linkage between the business leadership and the department that implements and operates the Information Technology. Risk management of cyber security risks needs to be aligned with the overall business risk management. There needs to be a clear governance structure as to who will make risk management decisions and what information they require to make those decisions. The senior business leaders need to be clear as to what cyber security risk they are willing to tolerate in pursuit of their business objectives. Any delegated authority needs to be clearly articulated and escalation paths understood.

There are various risk management methodologies/frameworks, which one is utilised is dependent on the nature and size of the business, procuring organisation and regulatory requirements of the sector. Whichever approach a business/organisation adopts, it should be proportional to the enterprise in question and the rigour applied, based on the potential negative impacts if things go wrong.

A security case captures security-related threats, critical assets, vulnerabilities, risks and mitigations; it captures the security landscape and associated business and risk management decisions. In its entirety, the security case enables the business to make an informed decision on whether the holistic security approach protects the business interests to an appropriate level (based on a clear understanding of residual risk and business risk appetite).

The risk management decision made by the business cannot normally be granted based on contract completion (e.g., on delivery of a secure solution) as approval to operate depends on other factors such as operational resources, physical mitigations (e.g., access controls), training, security awareness, business continuity/planning & supply chain security. It is important for businesses to understand that risk management of cyber security risks cannot be achieved solely by the provision of services/systems from supplier. It requires the active engagement of employees who apply appropriate procedures, based on acquired security knowledge and awareness.

If a business fails to plan the activities, does not ensure that activities are executed correctly or does not follow risk management processes, then system/service designs and associated documentation will be inadequate. Poor cyber planning will not enable the business to be assured that the appropriate risks have been identified and that these have been adequately mitigated.

There is a plethora of manufacturers/organisations who will claim that, by implementing their technology, using their bespoke service and incorporating their security mechanisms, tools or toys, the business system will be "secure". The reality is that risk cannot be completely eliminated and the risk management process ensures that residual risks are considered by the organisation. In doing so, the organisation must review their information risk appetite/tolerance, while ensuring that business objectives are met and the expectations of risk stakeholders within the business are accommodated.

Fundamentally the process involves:

- Establishing what are the critical business assets, normally related to people, processes and technology and assessing the impact in the event of their compromise.
- Determining the cyber security risks to the business by establishing who wants to attack the business, what vulnerabilities they might want to exploit and their motivation/capability to carry out an attack.
- Addressing the risks by determining the appropriate approach to manage them. The organisation may make the decision to tolerate, treat, transfer or terminate the risk.
- Integrating the technical and non-technical controls within the overall system/service design taking into account the other functional and non-functional lines of development.
- Providing initial and ongoing evidence that the measures implemented are operating correctly through evaluation of products/components, auditing of event logs, testing and vulnerability assessments.
Risk Management
What is important to your business?

It is vital to ensure that there is a clear understanding of what data is processed by the solution, what functionality it provides to employees/customers and its importance to the business. These are business-critical assets, which can take the form of information, data, processes and the technology that store, process and forward them.

A Business Impact Assessment can determine the impact, in terms of Confidentiality, Integrity and Availability, if business assets are compromised. Impact should be assessed in terms of the real world consequence of a cyber risk being realised, rather than the technological consequences.

In HMG/MOD circles, business-critical information is identified by a security classification, which can be mapped to a military, political or diplomatic consequence. Unauthorised modification or non-availability may effect the military capability; making it unreliable or denying its use completely. Within industry, data may be critical in terms of Intellectual Property, personal data or commercial strategy. Data loss, modification or unavailability may have an adverse impact on reputation and financial performance, either in terms of market share or fines imposed by statutory bodies.

Aggregation and association should also be considered. Dataset ‘A’ may not be seen to be critical to the business function, in its own right, however, when combined with analysis from another source its criticality may increase. This is key, when it is used to justify and implement courses of action; if the data is inaccurate or not available, then business decisions may be flawed. From a business design point of view multiple business services hosted across several vendors from diverse locations, may be considered less critical than multiple services, hosted by a single vendor at one location.

Some assessment of impact lends itself to numerical values based on financial figures, such as loss of revenue, statutory penalties or market share. Other risks, such as reputation, diplomatic or loss of life, are more subjective.

Establishing the correct impact levels requires significant scrutiny, not only by security professionals but also by business executives to strike the right balance. Evidence and metrics should be gathered from past incidents to help quantify and justify the assessment of impacts. A senior business authority should make informed judgements about the potential business impacts as any investment or restriction in business process to mitigate risk will need to be underwritten by the organisation.

Applying too high an impact level to assets could lead to the application of costly controls that may be disproportionate to the impact of the compromise. Conversely, applying too low an impact level will lead to a lower tier of controls and may open the organisation up to greater risk.

The Business Impact Assessment feeds into the risk assessment, thus it is important to understand the impact to people, processes and technology in the early stages. Any subsequent changes may have a significant impact on the risk management process.
**Risk Management**

**What are we trying to manage?**

The first key step is to establish the scope of the risk assessment. It may be obvious, but it is not always clear. You have to determine the business objective of carrying out the risk assessment. If there is an existing infrastructure and you are assessing the changes, then the scope of the assessment should be confined to the security risks of introducing the change, whether it is changes in location, processes, people, supply chain or technology. If you are introducing a completely new capability, then you would be looking to assess the security risks for the entire scope of the new capability. Notwithstanding businesses do not operate in isolation, so you have to include any reliance on existing dependant services and facilities that are not necessarily within the scope of the assessment.

Once the scope is established the assessment methodology can be selected. In some cases, businesses/organisations may express a preference for a particular methodology based on policy and familiarity.

Methodologies vary but most follow similar lines in that they identify:

- Who has the ability and opportunity to attack the scope of the assessment; quantify their motivation and their capability.
- What vulnerabilities inherent in the technology might exploit to compromise the Confidentiality, Integrity and Availability.
- The risks by evaluating both the likelihood of the risk occurring and the impact if the risk is realised.

An appreciation of the business processes, technologies, who, where and how the capability will be operated will provide a basis for establishing who may attack the business and what vulnerabilities can be exploited. This can be supplemented by third party alerts and advisories, which provide threat and vulnerability reports provided by a Corporate Security Operating Centre (SOC) or a Government Organisation. The business process may require the sharing of data or provision of support with another organisation or group of people in which there is not the same level of trust as the parent organisation.

**Risk Management**

**How do we manage the risk?**

Having established the applicable risks it is important to agree how they are to be managed. The business has to make the initial judgement and determine what its options are to manage the risks. The approach can fall into a number of categories:

- **Tolerate**
  - The business can elect to just live with the risk, provided it is within its risk appetite.
- **Transfer**
  - Transfer the risk to another organisation and get them to manage it. In financial terms this could be the provision of the appropriate insurance policy or set aside of contingency funding to cater for it.
- **Treat**
  - Which, as it implies, is the implementation of controls, whether these are technical or non-technical. By far the greater number of risks will be treated.
- **Terminate**
  - A course of action or use of technology may have to be terminated if the risk is considered unacceptable, because the impact is so great to the business.

The risk equation should take into account the business’ risk appetite, which articulates the level of risk that can be tolerated in pursuit of the business objectives. Any risks deemed to fall above the defined risk appetite level will need such implementation of additional controls or higher levels of assurance to ensure that they are adequately mitigated.

Setting risk appetite is a board level judgement, since applying too low a risk appetite will be costly in terms of additional controls/assurance or denying access to certain technology or even markets. A judgement also needs to be made as to the cost benefits of engaging within a particular market sector or using a particular process/technology.

The risk appetite may vary across different departments within a business, dependent upon the different business activities, their importance to the organisation and the associated technical risk.

Some of the controls will directly address the risk and achieve particular outcomes, e.g. detect and quarantine malware or encrypt data, so as to render it inaccessible to unauthorised individuals. Other controls will detect undesirable activity e.g. Port scan on an external facing firewall or abnormal internal network behaviour using an Intrusion Detection System (IDS). Certain controls facilitate corrective action, such as restore the system from a known good back-up. Finally, controls may limit the impact; Network segmentation (both physical and logical) reduces lateral movement, so adverse activity is confined to a particular network segment. Another example is the provision of a Disaster Recovery (DR) site to maintain the continuity of service, if the primary data centre becomes unavailable.

These security controls and the level of security assurance required from each provide an agreed set of security requirements that must be implemented within the system or service design and the security architecture. Every control has an associated cost and it is important that the control offers value for money in relation to the risk it is controlling. Where possible a control should have the ability to help mitigate a number of risks. Conversely a defence in depth approach should be applied; no risk should be treated by a single control.

It is the Risk Assessment and the associated risk treatment plan, which inform the wider business risk management activities. These provide the rationale as to what the risks are, what needs to be implemented to mitigate those risks and the level of assurance required. IA Professionals need to ensure that the customer’s security and business stakeholders such as business process owners, risk managers and Information Owners are engaged. It’s the business stakeholders that need to agree that the right risks have been identified and the strategy to mitigate them is adequate and proportional.

---

6. https://www.ncsc.gov.uk/index/about
Risk Management
It’s not just about security

There is a temptation to arbitrarily mandate a prescriptive set of policies imposing constraints on the business processes without fully thinking through the consequences. Logically, the security requirements should be tested against other business needs such as Training, Trials, Human Factors, Safety, Integrated Logistics Support (ILS), roles and responsibilities and business transformation to ensure that they are supportable and can meet the desired business objectives.

The nature of the equipment, software and technologies that support the storage, processing and transfer of the data assets, in conjunction with a clear understanding of what data is held where, will enable the organisation to gain value for money for any solution.

It may be tempting to apply a single set of stringent controls on all aspects of the system/solution. This may give rise to the application of disproportionate controls, both technical and non-technical, on the vast majority of the infrastructure; especially for an element of critical data that is only stored, processed and accessed from a small element of the network by a small user community.

In most cases, technical measures will typically require a level of personnel, physical and procedural measures to support the security enforcing functionality that they provide. This could place a requirement on the user community or could, for instance, be delivered as part of a managed service. In either case, there may be a need for further training, both for ordinary users of the service/system and for more specialist, privileged users, to ensure that any technical/procedural controls are effective.

The provision of technical measures, such as Intrusion Detection/Prevention Systems, Anti-Virus, Firewalls and encryption products, are only truly effective if supported by appropriate resources that monitor these devices, in conjunction with appropriate processes and procedures to react to any alerts or incidents. In addition, these mechanisms need to be supported through-life with the provision of up-to-date signatures to detect new and emerging threats as attackers adapt and find new ways of exploiting existing and new technologies.

There is usually a need for agility and the necessity to satisfy the customer. If a user is constrained by a solution, then users will look to actively circumvent any controls to meet the customer’s needs. Therefore, any solution must complement and enhance the business process. Thus, early and continual engagement with the customer’s user community should be actively encouraged to ensure that the end product meets an acceptable level of usability.

A careful Business vs Risk balance needs to be struck particularly when fully countering a risk might adversely affect usability, cost, schedule, safety or performance. Where such a balance cannot be resolved within the project delivery team, or the security risk is too great for the business risk manager to accept, then the decision to accept the risk is escalated to an appropriate authority within the business.

This requires the residual risk to be quantified based on the original risk assessment and an appropriate board-level member to make an informed decision6. The assessment has to articulate what the risk is and its potential impact, what the security gap is and why it cannot be plugged, what is the likelihood of it being exploited and what other measures are in place to managing the risk.

Business

- Usability, safety
- Cost, performance, schedule

Risk

- Likelihood
- Impact

6 In MOD terms this is a Risk Balance Case (RBC), which is endorsed usually by a two-star MOD appointment or government equivalent.

Conclusion

Fundamentally, a business needs to understand the cyber security risks that will have an adverse impact on the business and then manage those risks. A control-centric security approach to establish compliancy is useful, but, if applied without an appreciation of the risks, will provide a false sense of security. Careful application of risk management, coupled with an existing compliancy regime, ensures there is true alignment of the controls.

In order to develop a secure business, a clear understanding of the business processes, the associated risk appetite of the business and the effect of the security architecture on the user community are essential.

As the solution/service goes into operation, continued risk management is necessary to maintain an understanding of the risks that may affect the business. A visible and comprehensive security assurance plan, including audit, compliancy and vulnerability assessment activities needs to be articulated in the organisation’s IA Governance policy to ensure that the security controls that are implemented remain effective.

These assurance activities need to be supported by a change management plan that considers all changes and determines the impact from a security viewpoint; this ensures that the ongoing security posture remains appropriate for the data processed and the technologies utilised.

The business will also have to adapt to the emerging threats from persistent and highly motivated attackers, who find new ways to exploit vulnerabilities. As the business evolves, the impact of compromise of some business assets may vary. The value of design data may increase, if it is particularly successful within a given market. The business may be more successful, thus making it a more attractive target for more sophisticated attackers. Conversely, the financial success of the business may mean it can tolerate financial losses that, previously, would have made it insolvent.

Business risk managers should consider their incident management plans. This captures actions required, an escalation process and decision-making points.

Risk Management
It’s continuous

These need to be undertaken for a given incident type and any contractual or statutory obligations to report to external bodies.

This plan needs to encompass aspects such as:
- Breaches in physical or personnel security.
- Responses to a technical attack, such as malware, or alerts from a security enforcing mechanism, such as Intrusion Detection Systems/Firewalls.
- Processes to return the business back to secure operation.

It should also consider the requirement to support any internal investigation or an external investigation by a statutory body or police agency.

Early engagement with appropriately qualified security experts, combined with the timely planning and execution of risk management processes, are essential.

By applying sound risk management processes, both on specific projects and within the general organisation, a clear link can be achieved between the business and cyber security risks to ensure that investment decisions related to control measures are proportional. Not only this but, at a board room level, it can help business leaders make more informed, effective investment decision, and reap the consequential operational and financial benefits.