AXELOS
GLOBAL BEST PRACTICE

Cyber resilience and IT service management (ITSM) – working together to secure the information your business relies on

Stuart Rance

AXELOS.com

White Paper
June 2015

Contents

1 Introduction

Cyber resilience and IT service management (ITSM) are both concerned with how to manage the information that creates value for your organization and your customers. Cyber resilience is concerned with managing the risks in protecting the confidentiality, integrity and availability of information that the business needs, whereas ITSM is concerned with managing the IT systems and services that store, process and manage that information. There is a lot of overlap between these two areas, but too many organizations manage them completely separately – with different people, processes, technology and governance. This can foster a silo mentality, resulting in ineffective decision making that fails to manage cyber risks properly.

This White Paper looks at how cyber resilience and ITSM can work better together to help organizations be more effective in managing their IT services, in preventing cyber-attacks, and in detecting and correcting attacks that cannot be prevented.

2 What's it all for?

2.1 CYBER RESILIENCE

Cyber resilience is all about managing risk. It can be formally defined as "the ability to prevent, detect and correct any impact that incidents have on the information required to do business". There have been many highly publicised cyber incidents recently, and this has caused cyber resilience to become visible at the highest levels in many organizations. The use of the word "resilience" emphasises that the focus has changed from simply trying to prevent incidents to an understanding that it is equally important to be able to detect and correct incidents that can't be prevented. Cyber resilience is all about balance:

> The Oxford English Dictionary defines resilience as "the quality or fact of being able to recover quickly or easily from, or resist being affected by, a misfortune, shock, illness etc."

- Balance between prevention, detection and correction. Incidents should be prevented where this is cost-effective and achievable. Incidents that can't be prevented must be detected quickly and corrective actions must be taken to manage the impact and restore normal service
- Balance between people, process and technology. However good the technology, if people do the wrong things then information will be at risk, and even if the people and the technology are fit-for-purpose, poor processes can still result in embarrassing and expensive breaches
- Balance between risk and opportunity. Increased security can protect the business, but security controls can also cause inconvenience and have a negative effect on agility. A balance must be struck between insufficient controls that might lead to significant losses, and excessive controls that could slow down the business and limit the ability to exploit new opportunities.

2.2 ITSM

ITSM simply means how you manage the IT systems and services that deliver value to you and your customers. Even if you don't use the term ITSM, if you run IT systems then you are doing IT service management. ITSM processes help you provide a consistent quality of service, setting customer expectations and then ensuring that you meet them. ITSM covers a wide range of activities, including:

- Running a service desk, to manage and resolve customer requests and incidents
- Planning and implementing changes to IT systems and services
- Negotiating and agreeing service levels with customers, to help set and manage expectations, and to drive IT plans to ensure these expectations are met
- Proactive planning to help meet customer expectations for capacity, availability, security and service continuity
- Developing the skills, knowledge and competence needed to deliver the IT services
- Working with customers to understand their future requirements, and planning to meet these
- Running projects that design and build new or changed IT services
- Planning and managing a budget to ensure that money is available to pay for IT systems and services
- Measuring, reporting and continually improving how IT is used to help create value for the business.

This is not a complete list of ITSM activities, but it gives an idea of the scope of ITSM.

3 The overlap between cyber resilience and ITSM

There are many areas of overlap between cyber resilience and ITSM but too often they are managed in independent silos, resulting in conflicts that are both unhelpful and unnecessary. On the other hand, good management that takes the overlap into account can create synergies which lead to improved efficiency and effectiveness. Examples of areas that have significant overlap include:

- **Governance**. For cyber resilience, effective governance ensures that the needs of all stakeholders are taken into account and that cyber controls meet the needs of the business. This includes understanding legal and regulatory requirements, as well as business imperatives and the technology context. For ITSM, effective governance defines the direction, policies and rules that ensure services are planned, designed and managed to meet the needs of the stakeholders. The enterprise should provide governance of both cyber resilience and ITSM to ensure that goals, objectives, roles and responsibilities are aligned and work together in the interests of the overall organization
- **Business continuity management**. Many businesses have some continuity planning in place, but continuity management for IT services and business continuity management often work in isolation, rather than operating together. Business continuity management should allow all those involved in continuity planning to work seamlessly together, to ensure that critical business processes can operate even when things go badly wrong, e.g. after a fire. For cyber resilience, effective business continuity management can help to detect and correct major security events, reducing their impact and ensuring that the business can operate. For ITSM, effective business continuity management provides the context and requirements for IT continuity management, allowing ITSM to plan for the protection of information systems and the delivery of IT services that meet customer expectations
- **Availability management**. For cyber resilience, information must be available when it is needed. If information is not available then this can have a major impact on the ability to do business. Cyber risks that could cause availability issues include distributed denial of service (DDoS) attacks, cryptolocker or other attacks that encrypt data and demand a ransom for decryption, or simply someone deleting data after breaching security controls. For ITSM availability management involves implementing plans to ensure agreed service availability targets are achieved, as well as measuring and reporting service availability. These both consider the availability of the same information, and must work together to avoid conflicts, and duplication

- **Incident management**. For cyber resilience, security incident management is an essential corrective control to enable rapid and reliable recovery from attacks that could not be prevented. For ITSM incident management is a major area of investment, providing support to users and restoring service as quickly as possible when IT issues occur. These processes must work together to ensure that all incidents are well managed, and that disruption to the business is minimized. ITSM incident management can provide a framework for managing all incidents, but it needs input from cyber resilience to ensure that security incidents are contained and escalated in the best way.

For each of these examples, and many other similar areas, it is essential that cyber resilience and ITSM work together to provide value to the business. If they are managed separately then this can lead to wasted resources, conflicting requirements and ultimately successful cyber attacks that can have far-reaching impacts on your market reputation, customer satisfaction and financial growth.

4 A lifecycle approach for managing information

Published best practices and standards are an essential starting point for design of both cyber resilience and ITSM. You could design your management system from scratch, thinking through every aspect for yourself, but this would require a huge amount of effort and it would be hard to come up with something as good as could be achieved by adopting a best practice framework that other people have already designed for you. You would almost certainly miss some critical aspects, leaving your organization and your customers at risk.

What is a management system?
Every organization has a management system that is used to guide and control what it does. This may be a formal management system following a standard like ISO 9001, or simply an informal set of activities, measurements and guidelines that ensure people know what they are supposed to do.

The world's most widely recognized framework for ITSM is ITIL®, which describes a lifecycle approach to managing IT services. The ITIL lifecycle describes five stages: service strategy, service design, service transition, service operation and continual service improvement which have formed the basis for *RESILIA™: Cyber Resilience Best Practice*. These same lifecycle stages can be adopted for managing cyber resilience, helping you to find synergies between service management and cyber resilience, and encouraging collaboration between previously disparate parts of the organization.

- **Cyber resilience strategy**. Strategy ensures that the activities you carry out to protect the organization's information assets are aligned with the needs of the organization and its multiple stakeholders, and it provides the understanding and resources needed to achieve the organizational goals. Without strategy it is likely that even the best designed cyber resilience controls will fail to meet enterprise needs
- **Cyber resilience design**. Design ensures that the management system and controls are designed in a way that will deliver the strategy, ensuring that risks are understood and that controls are designed in a way that balances their cost and negative impact with the benefits that they bring. Without design it is likely that some risks will have insufficient controls, while other risks have too many, and that controls won't work together to provide the overall protection that the organization needs
- **Cyber resilience transition**. Transition brings the design into operation, while managing the risks that this involves. It also ensures that business and IT changes are managed in a way that supports the cyber resilience needs of the organization. Without transition it is likely that the design will not be correctly implemented, resulting in increased risk, and that business and IT changes will introduce new risks that are not understood or managed well
- **Cyber resilience operation**. Operation is the part of the lifecycle where the controls actually have an effect on risk. Risks are prevented where possible, and those that can't be prevented are detected and corrected. Without operation it is likely that attacks will not be detected and that incorrect corrective action will be taken, resulting in increased business impact from incidents that could have been contained

- **Cyber resilience continual improvement.** Continual improvement defines the attitudes, behaviours and environment across the organization that ensures cyber resilience continues to provide the protection needed in a constantly changing environment. Without continual improvement it is likely that changing threats, vulnerabilities and business needs will not be understood and that risk will increase over time.

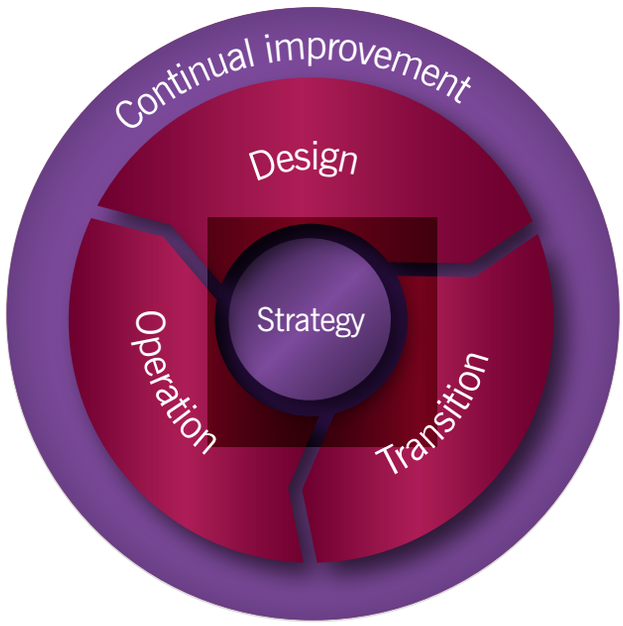

Figure 4.1 The RESILIA lifecycle (as adapted from ITIL)

There are many ways that cyber resilience and ITSM can benefit from working together within each of these lifecycle stages. The guidance in ITIL describes ITSM process that support every lifecycle stage, and each of these processes can both help cyber resilience, and be supported by cyber resilience controls. Similarly cyber resilience has controls that are relevant to each stage of the lifecycle, and each of these controls can contribute to and support ITSM, and can be facilitated by ITSM practices.

To take just one simple example. ITIL defines an event management process as part of service operation. This process is responsible for detecting events, making sense of them, and taking appropriate action to ensure they are properly managed. Cyber resilience defines many detective controls, which can help to detect attacks so that corrective action can be taken. The ITSM event management process can support cyber resilience by:

- Providing a framework for detection of cyber resilience events and notifying them to appropriate personnel
- Monitoring assets to detect events that may be significant to cyber resilience
- Detecting unusual patterns of behaviour in people, processes or technology that may indicate an attack.

In return cyber resilience can support ITSM event management by:

- Designing detective controls to ensure unusual activity can be discovered
- Defining thresholds to be monitored to detect unusual activity
- Selecting and configuring tools to monitor and report cyber resilience events.

Every process and every lifecycle stage has similar opportunities for cyber resilience and ITSM to support each other, and to provide greater business value by focussing on how to maximise the value of information needed to conduct business.

5 Who is responsible?

If it's so clear that cyber resilience and ITSM must work together to provide the information needed to do business, what's stopping this from happening? In large organizations, the issue is often organization design. ITSM may be seen as an operational issue, and managed as an internal function within the IT organization. Cyber resilience is typically managed by an information security team who work separately, issuing instructions on what everyone must do to protect information. Interfaces between these teams can be difficult as they typically have very different goals and objectives, and they report to different parts of the organization. It's also possible that the IT team think information security gets in the way of developing new and innovative services, and the information security team think that IT doesn't understand the need to protect information. In smaller organizations there is often insufficient understanding of ITSM or of cyber resilience, and there may be pressure to "just get on with the work" without a individual or team being assigned any specific responsibility. This can lead to time being spent on things that are less essential rather than dealing with the priority issues and problems.

Of course cyber resilience isn't just the responsibility of dedicated staff. Everyone in the organization is responsible for helping to protect the assets, for example by managing their passwords properly and not being seduced by phishing attacks that try to compromise their security. Similarly everyone who uses IT has to take some responsibility for ITSM, for example by logging their incidents the right way and by not making changes to IT systems without authorization.

Some organizations have adopted the DevOps philosophy, eliminated handovers and have cross-functional teams who own all aspects of the development and operation of IT services. These cross-functional teams may take responsibility for cyber resilience as well as other aspects of the solutions they deliver, but even in this case there is a need for governance of cyber resilience, and for overall design of cyber resilience controls that can be used in many different solutions. DevOps can help to reduce the friction and ensure that cyber resilience and ITSM work well together at the design, transition, operation and improvement stages of the lifecycle, but it can't take away the need for an overarching approach to cyber resilience governance and design.

6 Cooperation and collaboration

A good way to improve the efficiency and effectiveness of both cyber resilience and ITSM is to encourage the people responsible for these activities to work together. In an organization that uses DevOps to design, transition, operate and improve their IT this may be fairly easy, but the rest of us have to really work at it.

Most organizations have some cooperation between cyber resilience and ITSM personnel, but simple cooperation is not enough to achieve real benefits and ensure that risks are properly managed. What is needed is collaboration, which is a much deeper and more productive relationship. Collaboration is about working together to achieve shared goals, rather than simply working together. The differences between collaboration and cooperation are summarised in this table 6.1.

Collaboration	Cooperation
Working together to achieve a common goal	Working together, but possibly with different goals
Shared goal setting and decision making	Separate goal setting and decision making
Driven by the collaborators	May be driven by management, or by the co-operators
Usually have individual goals as well as shared goals	Usually have individual goals only
Requires emotional engagement	Requires working together
Collaboration takes precedence over roles, processes, etc.	Roles and processes more important than cooperation
Everybody wins	Everybody gets something, but not everything they want

Table 6.1 Differences between collaboration and cooperation

Collaboration can occur within teams, as well as between teams, and in a great organization collaboration can extend to suppliers and partners as well – leading to everybody involved in the whole value chain taking joint responsibility for achieving the shared goals. This is often experienced in companies that embrace agile working and concepts or in projects or programmes that adopt an agile approach (such as PRINCE2 Agile™). These environments place how individuals interact, collaborate and communicate at the centre of their practices. As part of a collaborative approach to cyber resilience and ITSM, it is possible to design tools and processes that cut across organizational silos and deliver real value by helping to ensure that the organization gets the greatest possible benefit from the information it owns. Ideally every process should focus on organizational needs, rather than the needs of one part of the organization, every person should be measured on the contribution they make to organizational goals, not to the goals of their small part of the business, and every tool should facilitate collaboration rather than simply deliver to the needs of one team or one process.

7 Five tips for building cyber resilience and ITSM collaboration

Here are my five top tips to help ensure your organization is getting the best possible value from cyber resilience and ITSM:

- Learn about sources of best practice for cyber resilience and ITSM

  There is lots of great guidance available to help you design a management system that will deliver your cyber resilience and ITSM requirements. Don't start with a blank sheet, go out and learn about best practices and standards that have been developed to help you. Depending on your personal learning style you may just want to read the guidance, or you may prefer to go on a formal training course. Here are some of the sources that you should learn about:

  - **RESILIA** is a best practice framework for managing cyber resilience, published by AXELOS in June 2015. RESILIA covers management of cyber resilience using the lifecycle approach described in this paper. This makes it easy for organizations who adopt RESILIA to integrate cyber resilience with their ITSM practices
  - **ISO/IEC 27001** is the international standard for an information security management system. It says what you must do, but does not provide much detail on how it should be done. There are many standards in the ISO/IEC 27000 series that specify particular aspects of information security management
  - **NIST Framework for Improving Critical Infrastructure Cyber security** describes a "risk-based approach to managing cyber security risk". This is published by the US National Institute of Standards and Technology and although its focus is on protecting critical infrastructure, the guidance is used by many organizations for protecting every kind of information asset
  - **ITIL** is a best practice framework for ITSM. It is not prescriptive but recommends that you adopt the parts that fit your needs and then adapt these to your particular circumstances. This "adopt and adapt" approach has helped ITIL to be used by many thousands of organizations around the world
  - **ISO/IEC 20000** is the international standard for IT service management. Like ISO/IEC 27001 it says what you must do, but does not provide much detail on how to do it. As an international standard it defines requirements against which an organization can be audited, to demonstrate their capabilities.

You shouldn't try to adopt everything in these sources of guidance without thinking very hard about how the ideas will fit into your organizational culture, but incorporating best practice ideas can help to improve your management system and ensure you haven't forgotten vital elements.

- Ensure your management system covers the whole of the service lifecycle

  It is common in both cyber resilience and ITSM for organizations to focus on the areas that they are familiar and comfortable with, and to completely forget about other areas which may be more abstract, or require more thought.

At the strategic level, the most important consideration is governance. Without proper governance, both cyber resilience and ITSM tend to focus on technology solutions, rather than on meeting the needs of stakeholders. Governance must be owned by executive management, and should ensure that cyber resilience and ITSM work together effectively. If you don't already have governance of both cyber resilience and ITSM in place then you need to engage with your board (or other owners) to ensure they understand why governance is needed, and how it can be put in place. Guidance to help with this can be found in ISO 38500 (the international standard for IT governance) and ISO/IEC 27014 (the international standard for information security governance).

The other area of the lifecycle that often has too little attention is continual improvement. However well you design your management system and your controls, you will always need to improve. Controls that worked perfectly at one time will not continue to be effective because of:

- New threats and vulnerabilities, that you must monitor and respond to
- Changing business needs, due to competitive pressures, new customers and contracts, new acquisitions and new business opportunities
- A continually changing technology environment, with new infrastructure, new applications and new services that need new, updated or completely redesigned controls to achieve the same effect.

Continual improvement is mainly about the attitudes and behaviours of your people, but you also need the right tools and processes to help facilitate this. Guidance to help implement continual improvement can be found in ITIL (for ITSM) and RESILIA (for cyber resilience).

- Design integrated processes that support both cyber resilience and ITSM

  There are a number of processes that need to support both cyber resilience and ITSM. Although these processes have a different perspective for ITSM and for cyber resilience, it makes sense to design each of them as an integrated whole, rather than creating multiple processes that attempt to do the same thing. Here are examples of some of the processes you should think about:

  - **Incident management**. Your ITSM incident management is responsible for restoring normal service to users while minimizing the impact of any service disruption. From this perspective a cyber incident is just a specific type of incident, that may need handling in a particular way but that still needs to be logged and managed like any other incident. From a cyber resilience perspective, incident management is one of the main corrective controls available to you. It needs to detect and contain incidents, then investigate and recover from them. It may also need to preserve evidence or to create audit trails of actions taken. There may also be a need to protect the confidentiality of incident information, which may make it difficult to manage the incident using the standard ITSM tools. All of these issues can be managed within a single integrated process, resulting in improved efficiency and effectiveness
  - **Continuity management**. Management of business continuity and of IT service continuity are needed for both cyber resilience and ITSM, and these need to be the same continuity processes for both. It is not possible to have distinct continuity processes for cyber resilience and ITSM, as only one of them could be invoked when there is a major incident. What is needed is for both cyber resilience and ITSM to provide requirements for this process, and to provide capabilities as needed, for development, testing and operation. This needs to be managed as a single integrated process
  - **Change management**. ITSM change management is concerned with facilitating the rate of change the business needs while protecting the business from any adverse impact of change. In cyber resilience the focus is more on protection, and on ensuring that vulnerabilities are not introduced when changes are made. This also needs to be managed as a single integrated process

- **Asset management**. Cyber resilience and ITSM have different needs from asset management, and they consider different sets of assets. ITSM asset management is usually carried out as part of configuration management, and its main purpose is to ensure that information about the configuration of assets supporting the delivery of IT services is available when and where it is needed. Cyber resilience uses asset management to identify the assets that need to be protected, this typically includes many assets that are outside the scope of ITSM, as they are not related to IT. For example cyber resilience may need to consider how information on paper is to be handled. Although they have a different scope, there is a wide overlap between these approaches, and it is possible to design a single integrated process that meets the needs of both much more efficiently than running this as two independent processes.

There are so many other processes that need to be considered in this way that I cannot include them all here. You should review all of your cyber resilience and ITSM processes to look for opportunities to combine them in a way that will deliver greater value at lower effort.

- Define integrated end-to-end metrics that are focussed on the needs of your customers
  Eli Goldratt, the man behind the Theory of Constraints[1], once said "Tell me how you measure me, and I will tell you how I will behave". Metrics have an enormous impact on how people behave. If you define separate metrics for cyber resilience and ITSM, with separate goals and reward systems, then you will encourage behaviour which is not joined up and people are likely to focus on the short term needs of individual groups within the organization. If, on the other hand, you define integrated metrics that are all aligned to the real needs of your organization and your customers then this will encourage integrated joined up behaviour.

  For example typical metrics for change management might include:

  - **Cyber resilience**
    - Number of changes that cause security incidents
    - Number of vulnerabilities introduced by changes.
  - **ITSM**
    - Percentage of changes that cause incidents
    - Percentage of changes that have to be backed out
    - Percentage of emergency changes.

  These might be really important things to measure, but if you speak to your customers about change management they may tell you that the most important two issues are meeting their need for agility and speed of change, and protecting them from incidents caused by changes. When you review the metrics above you can see that they are only focussed on one of these issues, so of course the behaviour will be very conservative, protecting the organization without sufficient attention to the need for agility. It would be much better to define two very high level customer-focussed goals, and then to ensure that the metrics support these, for example.

  - Protect customer from the negative effect of change
    - Percentage of changes that cause incidents
    - Number of vulnerabilities introduced by changes.
  - Meet customer need for agility
    - Percentage of changes that are implemented within agreed times
    - Percentage of changes that deliver agreed business benefits.

This change in emphasis results in a much more balanced set of metrics that will encourage the behaviour the customer wants. You should review all of your metrics for both cyber resilience and ITSM in this way, looking for opportunities to merge them and align them with customer-facing goals.

- Encourage collaboration between your cyber resilience and ITSM people

  All of the above tips depend on how well your people work together. Even if you follow all the guidance in the four tips above, this will never deliver the right value you if you don't get the right level of collaboration between your people.

  Make sure you have understood the difference between cooperation and collaboration, and think about ways you can encourage the right level of collaboration. Don't allow one team to dictate terms to the other, but ensure they are treated as equal partners in helping to create value for the real customers. Ensure that they work together to define integrated processes and metrics, as part of a holistic management system that meets all of your needs across the whole lifecycle.

  Probably the most important way to encourage the collaboration needed is for executive management to demonstrate the behaviour that is needed. Don't run cyber resilience and ITSM as separate functions in different parts of the organization. Don't measure and reward them separately. Create an organization that encourages people to work together for the benefit of all, and everyone will benefit.

End Notes

1. Eliyahu M. Goldratt, The Goal (1984). North River Press.

About the Author

Stuart Rance is a consultant, trainer and author, and owner of Optimal Service Management Ltd. Stuart works with a wide variety of clients in many countries, helping them use ideas from IT service management and information security management to create business value for themselves and their customers. He is a Chartered Fellow of BCS (FBCS CITP), a Fellow in Service Management at prISM (FSM®), and a Certified Information Systems Security Professional (CISSP®).

Stuart shares his expertise widely, regularly presenting at events and writing books, white papers, blogs and pocket guides on all aspects of IT. He is the author of ITIL Service Transition, 2011 edition, and author of the ITIL V3 Glossary. He has written many pocket guides for itSMF, for the official ITIL portfolio and is one of the authors of the *RESILIA™: Cyber Resilience Best Practice.*

About AXELOS

AXELOS is a joint venture company, created by the Cabinet Office on behalf of Her Majesty's Government (HMG) in the United Kingdom and Capita plc to run the Global Best Practice portfolio. It boasts and already enviable track record and an unmatched portfolio of products, including ITIL®, PRINCE2®, and RESILIA™ – the new Cyber Resilience Best Practice portfolio.

Used in the private, public and voluntary sectors in more than 180 countries worldwide, the Global Best Practice products have long been associated with achievement, heightened standards and truly measurable improved quality.

AXELOS has an ambitious programme of investment for developing innovative new solutions, and stimulating the growth of a vibrant, open international ecosystem of training, consultancy and examination organizations.

Developments to the portfolio also include the launch of PRINCE2 Agile™, the ITIL Practitioner qualification and a Professional Development programme, fully aligned to AXELOS Global Best Practice, for practitioners.

Latest news about how AXELOS is 'Making organizations more effective' and registration details to join the online community can be found on the website www.AXELOS.com. If you have specific queries, requests or would like to be added to the AXELOS mailing list please contact Ask@AXELOS.com.

Trade marks and statement

Figure 4.1 The RESILIA lifecycle (as adapted from ITIL®)

Sourced and published on www.AXELOS.com.