ITIL® Guide for Cyber Resilience

EBOOK

UpGuard™

CONTENTS

01 INTRODUCTION

Corporate IT has long carried the weight of the enterprise's infrastructure on its shoulders, but with organizations more than ever dependent on digitized assets to remain operational and competitive, the pressure on IT operations to maintain uptime and strong security is at an all-time high. Whether it's the cost of business downtime or data breach-inflicted brand damage, the penalties of failure on either of these fronts is dire. This is a challenge faced by all enterprises, and many frameworks have been laid out to help firms design infrastructures that are both robust and secure.

MORE THAN EVER DEPENDENT ON DIGITIZED ASSETS

The Information Technology Infrastructure Library, or ITIL® for short, is one such leading framework to emerge. A new model for managing IT security risk called cyber resilience has also emerged in response to the rising threat of cyber attacks aimed squarely at enterprises. This ebook explores the benefits at their confluence that enable organizations to run smoother, more resilient operations in the face of increasing digital threats.

When it comes to cyber resilience, many IT professionals complain about a dearth of pragmatic implementation guidelines. The fact is that resilience can be achieved using a myriad of approaches, ITIL® being one of them. Additionally, a great degree of implementation latitude exists within ITIL®— the framework can be adopted either in part or full, and processes can be chosen or adopted as needed. This makes it ideal for laying out the groundwork for an enterprise's cyber resilience strategy. Later, we'll explore how cyber resilience can be streamlined within the scope of ITIL® and how the framework provides enterprises with a powerful model for both achieving a strong security posture and business continuity.

02
ITIL

Consistency and integrity are crucial to a sound IT environment. This premise is as true today as it was back when ITIL® was first created in the 1980s. The framework's initial goal was to allow for consistent practices to be applied across increasingly disparate enterprise IT infrastructures through the rendering of IT as a service. Today, this view of IT from a service delivery perspective— or IT service management (ITSM)-- is widely adopted by most enterprises. And for most of these firms, ITIL® is the chosen way to "do" ITSM. The body of knowledge and guidelines that comprise ITIL® are developed and maintained by Axelos, a joint-venture company created by the U.K. Cabinet Office and Capita PLC.

CONSISTENCY AND INTEGRITY ARE CRUCIAL

As its name implies, ITIL® is made up of a library of five core publications that cover each phase of the IT service lifecycle. Each of these will be discussed later in the context of cyber resilience.

Phase	Purpose
ITIL® Service Strategy	Lays out the foundations for adopting a service strategy, such as asking the critical "why" questions
ITIL® Service Design	Provides guidance in developing/designing service management capabilities
ITIL® Service Transition	Defines processes for bringing new or changed services live in a controlled, predictable manner
ITIL® Service Operation	Lays out the mechanisms to support service uptime and quality on a day-to-day basis
ITIL® Continual Service Improvement	Aligns/realigns IT services to dynamic business needs through the ongoing assessment of services that support business processes

Simply put, ITIL® enables enterprises to manage their IT services more effectively and efficiently. By using the framework's processes to deliver IT services to customers (i.e., the business), IT can better align its functions with the needs of the enterprise at large. The body of knowledge consists of process descriptions, flow charts, success factors/metrics and best practices for helping IT improve efficiency levels and maintain optimal operations.

03 CYBER RESILIENCE

You may have heard the term digital or cyber resilience discussed in various enterprise risk management and cybersecurity circles. If not, you're likely to come across it soon enough, hopefully as a preventative tactic for bolstering security as opposed to a reactionary measure, post-data breach. Notwithstanding, data breaches are inevitable; cyber resilience aims to lessen their business impact and enable enterprises to bounce back from security compromises through a combination of risk management and layered cybersecurity.

First coined by McKinsey & Co. in Beyond Cybersecurity: Protecting Your Digital Business, resilience entails both merging digital risk management into strategic business initiatives and "baking in" security into the IT environment—as well as the entire organization at large. Companies looking to achieve resilience must "undergo fundamental, organizational changes, including integrating cybersecurity with business processes and changing how they manage IT.

> "Cyber resilience is all about managing risk... the ability to prevent, detect and correct any impact that incidents have on the information required to do business"
>
> - Cyber Resilience and IT Service Management (ITSM), Axelos

CYBER RESILIENCE LEVERS

McKinsey outlines the following 7 levers for achieving cyber resilience that help integrate security into the overall business:

Lever	Activity
1	Prioritize information assets based on business risks.
2	Provide differentiated protection for the most important assets.
3	Integrate cybersecurity into enterprise-wide risk management and governance processes.
4	Enlist frontline personnel to protect the information assets they use.
5	Integrate cybersecurity into the technology environment.
6	Deploy active defenses to engage attackers.
7	Test continuously to improve incident response across business functions.

Axelos offers an alternative definition of cyber resilience that perhaps better underscores its role as mitigator of business risk: “the ability to prevent, detect and correct any impact that incidents have on the information required to do business.” Firms need to strike a balance on several fronts— between prevention, detection and correction, as well as between people, process and technology.

04 VISIBILITY BEFORE RISK

A balance of risk and opportunity must be attained on a broader business level to achieve cyber resilience, since enterprises need IT innovation to remain competitive. For example, enterprise cloud adoption is at an all time high, despite its security implications. Cyber resilience enables firms to counterbalance technology's return on investment with inherent digital risks.

As an initial step, a firm grasp on exposures and deficiencies must be achieved for assessing digital risk. Visibility is a key enabler of cyber resilience in this context. Whether it be scaling private infrastructure to the cloud or acquiring another firm's digital assets, organizations require comprehensive situational awareness in order to take on more digital risks.

VISIBILITY IS A KEY ENABLER OF CYBER RESILIENCE

Proper visibility starts with discovery and continuous monitoring over vital IT assets— cyber attackers certainly cannot be thwarted all the time, but having the proper visibility and validation mechanisms in place will expedite incident response time by quickly alerting you of environmental changes not in line with policy. Knowing where vulnerabilities, misconfigurations, and security gaps live will paint a clearer picture of your organization's security fitness. And having a clear view of your internal and external risk posture is a critical component of cyber resilience, because you can't protect what you don't understand.

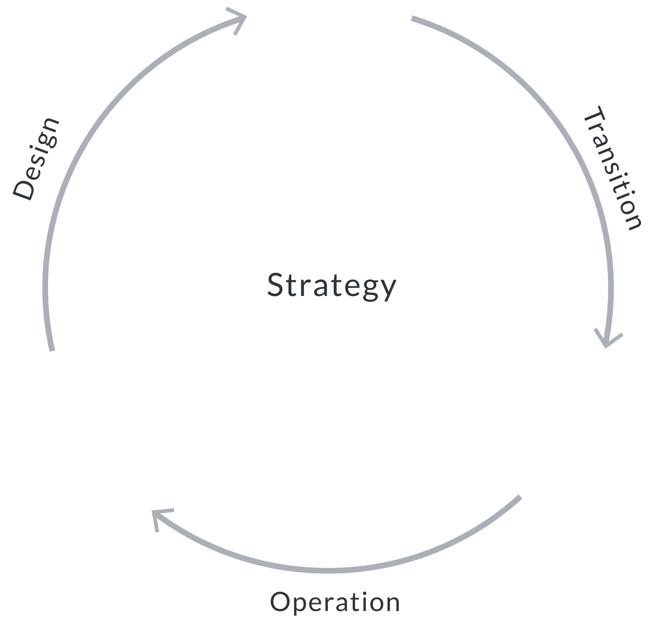
PARALLEL BENEFITS FOR THE ENTERPRISE

Effective ITSM enables enterprises to continuously provide and improve services by aligning IT closer to the needs of the business. In the same vein, cyber resilience espouses the normalization of cybersecurity into enterprise strategic planning and risk evaluation measures. Instead of relegating security to IT operations, resilient firms must treat it as a concern of the business at large. This approach positions enterprises to thrive in a landscape of evolving threats from both competitors and increasingly sophisticated cyber attackers.

05
ITIL FOR CYBER RESILIENCE

Both ITSM and cyber resilience are about aligning people, processes, and technology; ITIL® provides a tangible set of repeatable, reliable processes for managing these elements. And because ITIL® is the preeminent framework for ITSM, it can also serve as a crucial instrument for achieving cyber resilience. Since both treat enterprise security as a component of risk management, ITIL® is indispensable for building cyber resilient controls that are scalable, sustainable/efficient, and responsive to evolving threats.

CONTINUAL IMPROVEMENT



Adapted from Axelous.com

To make the correlation even stronger, Axelos has adapted its ITIL-based IT Service Lifecycle into a cyber resilience framework called Resilia. The following table maps ITIL®'s IT Service Lifecycles to Resilia's Cyber Resilience Lifecycles and McKinsey's Cyber Resilience Levers.

Phase	Purpose	Cyber Resilience Lever(s)
ITIL® Service Strategy	Cyber Resilience Strategy	1,2,3
ITIL® Service Design	Cyber Resilience Design	1,2
ITIL® Service Transition	Cyber Resilience Transition	5
ITIL® Service Operation	Cyber Resilience Operation	4,6
ITIL® Continual Service Improvement	Cyber Resilience Continual Improvement	3,7

Suffice to say, ITSM and cyber resilience overlap significantly, and adopting ITIL® as a strategy for ITSM has the added benefit of making the organization more resilient. For example, continuity management for IT services and business continuity management are just different faces of the same coin. ITIL®'s principles for ITSM can therefore be applied to cyber resilience, enabling the faster detection/remediation of security events and lessening of their business impact.

Alternatively, UpGuard's model for cyber resilience covers 3 distinct phases: discover, control, and fortify. This condensed lifecycle provides more actionable details that describe the transitional phases for a strong resilience posture. The journey starts with visibility and ends with resilience.

Outage

- Limited Environment Visibility
- Recurring Frequent Outages
- Configuration Drift

Non-Complaince

- Frequent Unauthorized Changes
- Regulaed Industry Compliance Changes
- Inconsistent Build Verification Standard

Breach

- Poor C-Suite Risk Prioritization
- Arduous Audits/ Reporting
- Manual Vendor Risk Assessments

Discover >

- Configuration Discovery
- Configuration Differencing
- Vulnerability Analytics

Control >

- Automated Runbook Generation
- Configuration Compliance Automation
- Automated Change & Release Reconciliation

Predict

- CSTAR Resilience Scoring
- Security Configuration Analysis
- Vendor Risk Assessment Benchmarking**

Operational Awareness

UpGuard Discover

UpGuard Control

UpGuard Resilience

In the Discover phase, a foundation is established in gaining infrastructure visibility: how systems are configured, how environments differ, what security gaps exist. This visibility sets the stage for future improvements. After determining what you have, the Control phase allows you to bring your environment into a desired state. By making infrastructures reproducible and reliable, configurations can be validated on an ongoing basis to meet standards established by service levels or compliance measures. With visibility and control in place, enterprises can then build scalable, resilient defenses to Fortify their environments. Cyber threats are always evolving; with a strong foundation based in awareness and validation, you can develop defenses that are layered, adaptable, and of course— resilient.

TIPS FOR ALIGNING CYBER RESILIENCE WITH ITIL®

Learn from the Source

A plethora of materials can be had online for learning about ITIL® and cyber resilience—McKinsey’s website and Axelos’ ITIL® portal are good starting points. The latter provides a pragmatic body of knowledge used by leading enterprises for ITSM; these guidelines can also be used to support cyber resilience efforts.

Prep for Collaboration

Because cyber resilience elevates security to an enterprise-wide concern, collaboration between IT operations, security, and other parts of the organization is critical— without the proper information un-siloing, firms cannot maintain a continuously resilient posture.

Test and Measure Regularly

Resilience needs to be measurable and regularly tested. To ensure ongoing resilience and stability, firms needs to define integrated end-to-end metrics aligned with the customers and business’ needs. It’s not enough to assume that your infrastructure is in a given state— validate those assumptions continuously with ongoing environment and configuration testing. ITIL® lays out the groundwork for ITSM that readily translates to cyber resilience. In parallel, UpGuard’s Discover, Control, and Fortify model offers another pragmatic view into how enterprises can achieve cyber resilience.

06 CONCLUSION

The business risks brought on by digitization continue to increase as enterprises reap the fruits of technological innovation. To mitigate these risks, ITSM/ITIL and cyber resilience practices have been created to provide enterprises with a methodical, sustainable, and adaptable approach to IT and security. The synergies between ITIL® and cyber resilience abound, but their most important shared quality is that they both aim for closer alignment with the needs of the business. Cyber resilience requires that security be managed at an enterprise-wide strategic level. Similarly, ITIL® is focused on aligning IT services closer to the needs of the business. ITIL® can therefore be an effective means for achieving both enterprise ITSM objectives and cyber resilience initiatives.

CONSISTENCY AND INTEGRITY ARE CRUCIAL

CSTAR

In the IT operations and cyber resilience arena, the two most common recurring themes are visibility and risk. Ongoing visibility is foundational because without it, continuous improvements simply cannot be made. Resilience espouses treating security as a function of enterprise risk management. UpGuard's cyber resilience platform revolves around these two premises, giving enterprises unparallelled infrastructure visibility for a complete picture of their firm's cyber risk profile. The CSTAR rating system is the preeminent framework for gauging cyber resilience based on both internal and external measures, capturing an enterprise's aptitude in the areas of compliance, integrity, and security in a single, easy-to-understand value. And for ensuring that resilience is continuously maintained, the platform's powerful configuration validation and vulnerability monitoring capabilities prevent inevitable security incidents and outages from disrupting the business.

REFERENCES

Bailey, Tucker, James M. Kaplan, and Chris Rezek. "Repelling the Cyberattackers." Digital McKinsey. McKinsey & Co., July 2015. Web. 14 Dec. 2016. <http://www.mckinsey.com/businessfunctions/digital-mckinsey/our-insights/repelling-thecyberattackers>.

Crawford, Scott. "The Importance of ITIL to (Am I Reading This Right?) ... Security??" ITSM Solutions DITY Newsletter (7 Oct. 2008): n. pag. Print.

Dobrygowski, Daniel. "Cyber Resilience: Everything You (really) Need to Know." Weforum.org. World Economic Forum, 8 July 2016. Web. 14 Dec. 2016.

"Information Technology Infrastructure Library (ITIL) Guide." IT Knowledge Portal. N.p., n.d. Web. 14 Dec. 2016. <http://www.itinfo.am/eng/information-technology-infrastructure-libraryguide/>.

"ITIL (Information Technology Infrastructure Library)." SearchDataCenter. TechTarget, n.d. Web. 14 Dec. 2016. <http://searchdatacenter.techtarget.com/definition/ITIL>.

REFERENCES (CONTINUED)

"ITSM IT Service Management." IT Services Management Portal. N.p., n.d. Web. 14 Dec. 2016. <http://www.itsm.info/ITSM.htm>.

Laskowski, Nicole. "How to Survive Cyberassaults: Seven Steps to 'digital Resilience'" SearchCIO. TechTarget, 16 July 2015. Web. 14 Dec. 2016. <http://searchcio.techtarget.com/ news/4500250105/ How-to-survive-cyber-assaults-Seven-stepsto-digital-resilience>.

Pemberton Levy, Heather. "The Six Principles of Resilience to Manage Digital Security." Smarter with Gartner. Gartner, 8 June 2015. Web. 14 Dec. 2016. <http://www.gartner.com/smarterwithgartner/the-six-principles-of-resilience-tomanagedigital-security/>.

Rance, Stuart. Cyber Resilience and IT Service Management (ITSM) – Working Together to Secure the Information Your Business Relies on. N.p.: Axelos, n.d. June 2015. Web. 14 Dec. 2015.

Vila-Real Vilarinho, Sarah. "Risk Management Model in ITIL." (29 June 2012): n. pag. Print.

UpGuard™

Businesses depend on trust, but breaches and outages erode that trust. UpGuard is the world's first cyber resilience platform, designed to proactively assess and manage the business risks posed by technology.

UpGuard gathers complete information across every digital surface, stores it in a single, searchable repository, and provides continuous validation and insightful visualizations so companies can make informed decisions.

909 San Rafael Ave.
Mountain View, CA 94043
+1 888 882 3223
www.UpGuard.com

EB_0032 / 02.17.2017