KPMG
cutting through complexity

INFORMATION TECHNOLOGY SERVICES

Are you ready for failure?

Architecting the Resilient Enterprise

CIO ADVISORY | 2015

CONTENTS

INTRODUCTION

In 2011 severe flooding in Thailand disrupted the supply of computer hard drives that was felt for a year. Also in 2011 a Tsunami struck Japan and crippled auto output for months due to broken supply chains. In 2012 a number of social media sites went offline when unprecedented flooding caused by Superstorm Sandy flooded the basements of several buildings housing data centers in New York City. Even though the servers and generators were located on floors above the flooding, fuel tanks and fuel pumps in the flooded basements failed, starving the generators of fuel and taking out their backup power. More recently, one of the largest American banks revealed that a significant security breach exposed sensitive data belonging to 76 million individuals and seven million businesses. Just a year ago, a security breach at a large retailer impacted 40 million customers and led to the departure of the CEO and CIO, direct costs of U$148 million, and uncounted indirect costs from reputational loss.

Geo-political instability in Eastern Ukraine and the resultant sanctions placed on Russia are expected to push Russia into a recession* while the World Bank estimates the economic impact of a huge Ebola epidemic in Western Africa could reach U$32.6 billion by the end of 2015. But business disruptions are not just the result of external events; organizations more often suffer when internal processes and systems fail. A major outage in a payments system at the Bank of England was caused by a technical issue related to routine maintenance and it was just a year ago that a glitch in a computer system at the RBS Group (Royal Bank of Scotland) resulted in £175 million set aside for compensation payments.

While the number and types of causes of business disruption continue to increase, the digital era requires businesses to support wide-ranging demands for always available products, services and systems. Today's customers expect to use a laptop, tablet or smartphone at any time to transact business, whether it's paying a bill online, depositing a check before going to bed, checking in for a flight or streaming their favorite TV show. Downtime for any reason, planned or unplanned, is no longer tolerated yet with the greater potential for disruption and increasing system complexity, it has become a significant challenge to design systems capable of coping in such an environment. It's time to move beyond disaster recovery and prepare for technology resilience. KPMG defines technology resilience as:

"The ability of technology systems to withstand operational stresses, cyber attacks and constant change."

KPMG believe that resilience is best attained not by after-the-fact "bolt-on" solutions but by fostering a culture that enables resilience to be built into systems from the beginning. This Point of View seeks to offer an actionable framework for understanding how organizations can move towards technology resilience.

* Source: The Guardian, 2 December 2014.

WHY NOW?

The need for the technology resilient enterprise is all around us. It seems that each month brings some new story of a major IT-related outage, security breach or other event that causes business disruption. Sometimes these are momentary with no real consequences while others persist for longer periods of time, causing significant financial and/or reputational losses. The situation is only going to get more challenging as a result of a number of trends, including:

- **Increasing complexity of systems.** The increasing digitization of the enterprise results in more IT-enabled solutions that must be integrated with existing systems and data leading to greater complexity, while the need for speed and agility requires more frequent change that increases risk.
- **Growing frequency and variety of cyber attacks.** The Department of Homeland Security in the United States estimates that as many as 1,000 retailers could have malware in their cash-register computers. For example, a major US retailer notified its customers that as many as 60 million credit card numbers were stolen over a period of months while another large US retailer suffered a similar breach less than a year ago that affected 40 million cards.
- **Regulatory Reform.** Since the financial crisis and global recession, the regulatory environment has grown more intense, and the pace of regulatory change is accelerating. This is especially true for financial services firms as they struggle to adapt to regulatory reform initiatives such as Dodd-Frank in the United States and the global banking reform measures of Basel III. But all industries are impacted in some way. According to KPMG's CEO Study, adapting to government regulation is their second most critical challenge after expanding geographically[1].
- **Rising expectations of customers.** The proliferation and consumerization of technology has led to an increasingly tech-savvy population with steadily higher expectations. Customers expect to engage with businesses on their terms, paying bills by phone in the middle of the night, interacting with a customer service representative via live chat, or ordering a movie for immediate streaming on their tablet. We expect to be able to do business 24/7.
- **Stress on legacy platforms to deliver new products and channels.** With the exception of start-ups, most organizations have significant numbers of legacy applications in their portfolio, with some more than twenty or thirty years old. As the business responds to the threats and opportunities from digital disruption by developing new products and channels requiring new capabilities, it often places extreme stress on these legacy platforms, stresses they were never designed to cope with.
- **Ongoing drive to cut operational costs and maintain services.** As organizations strive to become more efficient by cutting costs, there is a danger that the wrong resources are targeted. From an IT perspective, this could manifest itself in postponing upgrade cycles, reducing staffing, and other activities which can increase risks and undermine resilience.
- **Increasing number and intensity of climatic and geophysical disasters.** According to the EM-DAT emergency database maintained by the Centre for Research on the Epidemiology of Disasters, the total number of natural disasters reported each year has been steadily increasing in recent decades[2]. For example, severe drought in the Western United States recently resulted in a number of large wild fires that destroyed hundreds of homes at the same time as above average rainfall in parts of the Eastern U.S. led to record flooding.

It is no longer a matter of if but when some event will threaten or cause a major disruption, as the types of threats and frequency of their occurrence accelerates.

It is increasingly difficult for any organization to avoid or eliminate all of the potential vectors of business disruption. What is needed is a different approach that fuses people, processes and technology to create the resilient enterprise.

Due to the diverse types of threat, no single resilience approach covers all the elements that are required. Some of the problems with existing models, tools and standards are:

- **Exclusively process focused.** Resilience goes beyond processes. You can have a process in place but if people are unaware of it or it is not part of the day-to-day operating culture then it is unlikely to be effective. Resilience requires a holistic approach that incorporates processes, people and technology.
- **A check box exercise.** A rigid methodology can lull people into a false sense of security as the objective becomes more about checking boxes than thinking through issues, understanding impacts and formulating appropriate responses. Checklists are good to ensure consistency and completeness but they are not a substitute for thinking, planning and preventing.
- **Lack of structure for proper analysis.** Long-term sustainability does not come from simply fixing problems when they arise; it comes from getting to the root cause by analyzing what happened and then applying this knowledge to prevent the same problems from occurring again.

1 KPMG CEO Study "Setting the Course for Growth: CEO Perspective", http://www.kpmg.com/us/en/topics/pages/ceo-study.aspx
2 The International Disaster Database, Centre for Research on the Epidemiology of Disasters (CRED), http://www.emdat.be/

WHY NOW CONT...

- **All about disaster recovery.** A well designed and tested disaster recovery capability is essential to resilience but it is just one part. Most disruptions are not the result of a disaster, and resilience is about availability not just recovery. When it comes to customer-facing systems any outage will have an adverse impact on customer satisfaction and for e-commerce systems loss of revenue is likely. Furthermore, resilience is a set of ongoing processes, not a one-time planning event[3].

In response to these shortcomings, KPMG member firms have developed the Technology Resilience Framework as a way to bring together the best parts of existing standards and apply differentiated services to help fill in the missing elements to create a holistic resilience approach.

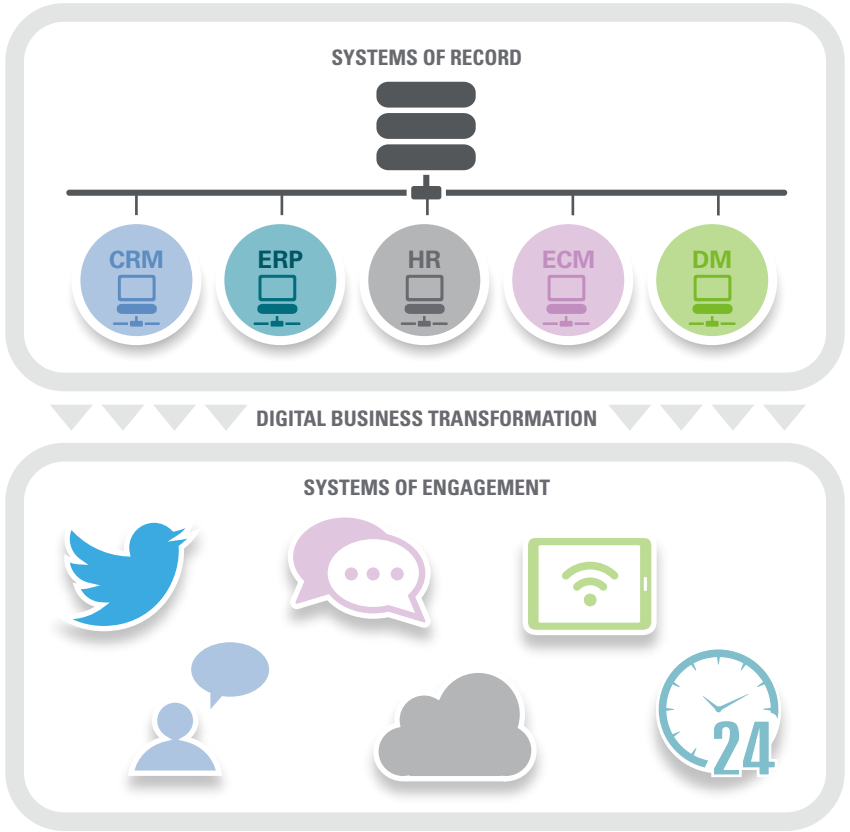
A FRAMEWORK FOR TECHNOLOGY RESILIENCE

In addition to traditional transaction based systems (systems of record), many business processes are increasingly automated from end-to-end, as digital business strategies require a growing number of customer-facing systems (systems of engagement). The result is that most organizations are completely dependent upon information technology assets to conduct business.

At the same time, technology systems are subject to a wide range of stresses ranging from operational errors to natural disasters, while others are under constant attack from cyber criminals. The accelerating pace of business change places additional stress on IT to keep up. The key objectives of technology resilience are to:

- **Align technology resilience to the business.** Building resilience requires that business processes and capabilities be tightly aligned with their underlying technology platforms and assets. Without this alignment and understanding of the linkages, it is nearly impossible to attain resilience since any single overlooked component represents a potential vulnerability.
- **Reduce complexity.** IT systems have grown increasingly complex. The ability to maintain and manage these complex systems is not keeping pace, leading to a high risk that organizations will find themselves reliant on systems that they no longer fully understand or are able to effectively manage. Resilience demands that complexity be reduced in existing systems through a legacy modernization program, and in planned systems by adhering to enterprise architecture[4].

FIGURE 1: SYSTEMS OF RECORD VERSUS SYSTEMS OF ENGAGEMENT



Transactions	Focus	Interactions
Facts & Commitments	Core Elements	Ideas & Nuances
Single source of truth	Value	Discovery & Dialog
User is trained	Usability	User "knows"
Regulated & Contained	Accessibility	Ad Hoc & Open

3 Move Beyond Disaster Recovery and Prepare for Business Technology Resiliency, Forrester Research, September 13, 2012. This date feels old. Can we skip providing the date and instead give the web link, as above?
4 Optimizing the Application Portfolio, KPMG Advisory Institute, October 10, 2014. Provide weblink: http://www.kpmg-institutes.com/institutes/advisory-institute/articles/2014/10/optimizing-application-portfolio.html

A FRAMEWORK FOR TECHNOLOGY RESILIENCE CONT...

- **Improve change delivery and operations approaches.** Research has demonstrated that almost 80% of outages are self-inflicted primarily as a result of poor or non-existent processes around change and problem management[5]. Significant improvements in availability can be achieved simply by improving operational management processes using established methodologies like ITIL and CobiT.
- **Understand the impact of resilience investments.** Building technology resilience will require investments in hardware, software, people and skills. Like any investment, it is important to understand the return on them. Not every application or service is critical and requires continuous availability, so it is important to match investments in resilience with the expected benefits and risks.
- **Drive resilience by design mindset.** To obtain the maximum benefits from resilience, it must become a core part of the culture and be incorporated as a standard input to any technology-related decision process. For example, as part of the overall IT governance process, every technology business case requires a section on resilience.

ALIGN RESILIENCE INITIATIVES WITH THE BUSINESS

The Technology Resilience Framework incorporates the people, process and technology aspects of resilience. They revolve around a fundamental hub of business alignment to ensure all aspects of the technology considerations stay in tune with the priorities, concerns and strategy of the wider business.

Resilience comes in many degrees and almost always imposes additional costs, ranging from small to significant. To put this in perspective, one of the largest U.S. banks has spent $250 million on cybersecurity in 2014, and this represents just one component of resilience. Many organizations are already behind the curve when it comes to resilience and will need to retrofit legacy systems at the same time as they architect and build resilience into new services. With budgets already lean and IT organizations stressed, investments in resilience must reflect the strategy and priorities of the business in concert with the potential risk.

RESILIENCE FUSES PEOPLE, PROCESSES AND TECHNOLOGY

Resilience is not a single product or service that you go out and buy. While there are elements of resilience like extra servers and storage, virtualization software and cloud services that can be purchased to provide elements of it, resilience requires a fusion of people, the processes they execute, and the tools and technology they use to execute those processes. You can build a resilient data center but if an operator fails to properly execute a change process it could bring the entire system down. Our framework for technology resilience consists of three domains and nine components (three components in each domain), as depicted in figure 2.

FIGURE 2: ELEMENTS OF THE TECHNOLOGY RESILIENCE FRAMEWORK

5 The Visible Ops Handbook, IT Process Institute Provide weblink
6 http://www.bloomberg.com/news/2014-08-29/jpmorgan-hack-said-to-span-months-via-multiple-flaws.html

A FRAMEWORK FOR TECHNOLOGY RESILIENCE CONT...

Resilience begins and ends with people

An organization's people are of primary importance in shaping the resilience agenda, and along with partners and third parties are responsible for carrying out the operational processes associated with it. The people dimension is critical for resilience because the majority of unplanned outages are caused by people, through poorly or non-executed processes, mistakenly deleting data, etc. The people considerations for resilience include:

- **Capability** – The skills and capability of an organization's people need to be understood in the context of how those skills and their deployment provides the organizational resilience needed. This is not just in terms of what people can do but staffing levels and how these factors change in times of organizational stress, such as during a major incident. Responding to a major incident often involves working around the clock until the incident is resolved, stretching resources and taking them away from other duties. Likewise, responding to a major incident can expose gaps in incident management, troubleshooting, cybersecurity, etc. Skills gaps and resource constraints must be identified and plans developed to proactively address them, whether through training of existing staff, incremental hiring, or contracting with an external vendor.
- **Vendor management** – Most organizations today operate in conjunction with external vendors and partners as key contributors in the delivery of services, both externally and internally. The number of externally provided services will continue to grow as IT adopts new operating models in response to the growing digitization of business, increasing the reliance on third parties[3]. Vendor management examines how these relationships work, measures supplier performance and, where required, benchmarks that performance against industry standards.
- **Culture** – A robust organization needs to have a culture that makes resilience part of its DNA so that it is embedded in the way things are done. Culture looks at the way people think about the business and their attitudes towards it. It looks at how the culture manifests itself and how it plays into building resilience into the production of systems, processes and people structures. Resilience must be valued and goals, objectives, metrics and incentives must be aligned to demonstrate support for that value.

Processes helps ensure consistency

Orchestrating processes across the enterprise together with coordinating all of the facets of service delivery, change management, and the over-arching system of governance under which they all operate, are fundamental to supporting resilience:

Change – Change is the biggest factor in causing incidents and outage, and so is one of the most important areas of the Technology Resilience Framework. The framework looks at all phases of testing, validation and verification and the delivery assurance processes in change, including project office, go-live planning operational handover and management processes post-implementation.

- **Governance** – Governance focuses on the decision processes addressing strategy, architecture, design and engineering. Also, as required, this extends to any external governance, such as legal requirements or that of applicable regulators.
- **Service** – The most important technology outcome for the business is ultimately the service that is delivered, both to internal functions and to customers. The service framework deals with the analysis of service management processes and how these support the delivery of resilient technology services.

Technology focuses on availability and sustainability

The big technology levers in the resilience framework address availability and the management of IT, environments both logical and physical, and the complex collection of vulnerabilities presented by cybersecurity:

Availability – The availability of systems is critical and so analysis of this element seeks to understand how resilience is promoted through the organization's operating model, the technology components that support continuity of business, systems' capacity planning, and the IT supply chain that satisfies the demands of those functions.

Environments – The robustness and fitness of the different compute environments that come together to provide a pathway from development to production is a key element in resilience. As well as the platform domain, this area also takes in physical environments, such as data centers, and the resilience of the infrastructure around them. For example, do the most business critical systems reside in the most resilient data centers? Are data centers located in stable, secure locations?

Vulnerability – The effective operation of systems and processes that provide cyber security are vital to any organization. The vulnerability to compromise of systems and data needs to be understood and managed as a key risk factor. The recent hacking of a major film and entertainment company, for example, resulted in the theft of data ranging from executive emails to complete unreleased movies. Are systems and data segregated with different levels of security and access rights depending on their sensitivity or value, or is there a one size fits all approach to security?

7 "Next Generation IT Operating Models", KPMG Advisory Institute, http://www.kpmg-institutes.com/institutes/advisory-institute/articles/2014/01/next-generation-it-operating-models.html

LESSONS LEARNED SO FAR

Many organizations are either just beginning or in the early stages of implementing enterprise resilience. In our work with early adopters member firms have compiled a short list of lessons learned so far. These lessons include:

- **Organizations do not understand their environments well enough.** Over many years continuous technology investments for market advantage coupled with mergers and acquisitions has produced an inventory of data centers, applications software, networks and third party provider relationships across multiple lines of business and geographies. As a result, resilience efforts struggle to get started as there is a large amount of discovery work required at the outset just to understand the magnitude of the problem.
- **Cost cutting has left organizations without critical mass in some areas.** Delivery of large resilience transformations on top of existing business as usual work is often beyond the organization's capability and resources. Given the current demand for digital enablement, i.e. mobile, cloud, big data, etc., there is even less of an appetite to fund and staff large resilience building programs that do not directly contribute business value in terms of growth or profit. But resilience has clear value that can be quantified in terms of customer satisfaction, customer defection, loss of revenue, and reputational harm, to name just a few.
- **Failure to properly integrate acquired businesses damages resilience efforts.** Organizations that grow via acquisition often implement quick, tactical solutions to integrate acquired businesses. This adds greater complexity, a natural enemy to resilience.
- **Resilience needs to be actively engineered into people, process and technology.** Organizations that build resilience from the ground up and integrate people, process and technology are more often successful in sustaining improved resilience outcomes than those that focus on technology alone.

HOW KPMG CAN HELP

At KPMG, member firms not only help the IT organization run a more efficient business unit, we help the business derive greater value from IT. We do this by providing IT with the insights and capabilities they need to balance the introduction of new, innovative solutions while continuing to maintain ongoing operations in line with cost and quality expectations. Following are two examples of how KPMG member firms have helped clients with their resilience challenges:

LARGE VOICE AND ELECTRONIC BROKING FIRM

Operating across the world, this client was unaware of the geo-political threats their IT facilities faced in the territories they operated in.

The client challenge was to ensure that its IT facilities across the world were well-placed to deliver resilient IT services and meet local regulatory requirements.

Working with the client, leveraging KPMG's Data Center Threat Assessment methodology (part of The Technology Resilience Framework) KPMG professionals provided the client with a view of its global IT facilities and provided a detailed risk heat map for their global data centers. As a result, the client was able to make an informed decision to expand its existing data center rather than build a new one in another location, at a considerable cost saving and encompassing significantly lower risks.

GLOBAL ALTERNATIVE ASSET MANAGEMENT FIRM

Two significant IT incidents causing major outages to key client-facing platforms resulted in significant cost and loss of reputation in the marketplace for our client.

The KPMG team took the client through a structured process to quickly identify the underlying weaknesses in the core IT systems/operations and produced a number of practical recommendations to reduce risks and improve availability. These included:

- Eliminating redundancies and consolidating infrastructure
- Strengthening change management processes to reduce human error
- Creating fire-breaks in the architecture to limit the spread of errors to unrelated systems
- Increasing operational process automation

To learn more about how KPMG member firms can assist you with your technology resilience challenges, please contact one of our team who will be delighted to discuss your specific issues.

CONTRIBUTORS

With thanks to the following subject matter experts for providing their input and guidance on this paper.

Jonathan Godson, Executive Advisor, KPMG in the UK

Craig Symons, Director in KPMG's CIO Advisory Global Centre of Excellence. KPMG in the US

CONTACT US

Denis Berry
KPMG in the US
T: +1 312 919 4302
E: dberry@kpmg.com

Bob Hayward
KPMG in Singapore
T: +65 8151 4192
E: bobhayward@kpmg.com.sg

Lisa Heneghan
KPMG in the UK
T: +44 7718 582368
E: lisa.heneghan@kpmg.co.uk

Marc E. Snyder
KPMG in the US
T: +1 978-807-0522
E: msnyder@kpmg.com

Glenn Tjon
KPMG in Panama
T: +50 7208 0700
E: gtjon@kpmg.com

www.kpmginfo.com/cioagenda