RESILIA™

ProcessFlows

John Freckelton

AXELOS.com

ProcessFlows®
Improving Business by Transforming Process

AXELOS GLOBAL BEST PRACTICE

Case Study
April 2016

Contents

1 Introduction

1.1 WHO ARE YOU AND WHAT DO YOU DO?

My name is John Freckelton and I've been the IT Manager at ProcessFlows for 14 years with responsibility for all the IT Administration (including Network, Security and Internal Incident Management) within the company.

During my tenure I have overseen the integration of regional offices into a global IT infrastructure, the migration of existing systems to head office and the planning and setup of a European office infrastructure in Sofia, Bulgaria.

1.2 DESCRIBE YOUR ORGANIZATION

ProcessFlows is a leading provider of solutions that improve business processes and communications. From the moment information enters an organization, we take intelligent action to recognize and store it securely, so that it can be accessed instantly by authorized users, from the application of their choice. This ensures that, whatever mode is used, the information reaches the correct person on time in the most appropriate format. Since 1987 ProcessFlows has helped over 1200 clients in finance, local government, healthcare and many other sectors to increase efficiency, improve customer service and implement controls for regulatory compliance. More recently we have provided hardware/software sourcing and business process outsourcing.

ProcessFlows employs over 180 staff in the UK and Bulgaria. Our organization is quite diverse and operates five distinct business units:

- Print and fax:
  - This business unit provides managed print and fax solutions, primarily through our partner channel.
- Complex solutions:
  - The Complex Solutions business unit provides business process management and enterprise document management systems.
- Communications (comms):
  - Our comms business unit provides voice, fax and SMS enterprise communication solutions.
- Software sourcing:
  - This is our one-stop-shop for all software licensing requirements, from standard Microsoft licenses to those of the most obscure development plug-ins and widgets.
- Outsourcing:
  - From Bulgaria we provide outsourced services and resources. This covers a wide range of skills including: software development, a multilingual 24/7 helpdesk service, customer services, accounting, telesales and marketing functions.

Image 1.1 ProcessFlows offices, Sofia, Bulgaria

1.3 DESCRIBE YOUR TEAM AND THE WORK IT DOES

The IT team is made up of three full-time staff. Two of us are based at our head office in Winchester, UK, with a third member at our Sofia office to support the 120 staff we have working there. In addition, we utilize a shared service desk (that we sell to our customers) to front our own internal incident management of IT calls and emails during busy periods and outside of core office hours.

Our IT department is typical of most internal IT departments. Our main role involves supporting the day-to-day activities of the business. In addition, at any one time we'll have anywhere up to 15 active internal projects running that will provide either costs savings or improved efficiencies to the business.

2 Adopting RESILIA

2.1 HOW DID YOU BECOME INTERESTED IN RESILIA?

We have worked with ITSM Zone (an IT training provider) for a number of years and are very familiar with the services that they provide. We had previously engaged them for our staff ITIL training and certifications and when they brought AXELOS' new RESILIA™ Cyber Resilience Best Practice certified training to our attention, we were keen to learn more. Like many companies, we had suffered from a number of cyber-related incidents in the past 12 months and knew it was an area we needed assistance with. There was also a need to overhaul our change management strategy, which no longer suited business requirements, and we saw that the RESILIA training also covered this area.

2.2 HOW DID YOU FIND THE CERTIFIED TRAINING?

The Foundation course and its associated learning materials were essential in understanding the concepts of cyber resilience, its alignment with ITIL® and its integral relationship with wider business strategies and processes. This understanding allows each area of a business to be broken down into a logical and identifiable framework into which a cyber resilience strategy can be built stage by stage. The course also provided solid preparation for the exam, although additional reading is always recommended.

2.3 HOW HAVE YOU APPLIED RESILIA TO YOUR BUSINESS?

2.3.1 Change management

As a company, we have been through a number of changes in recent years. We have rebranded (more than once), we have embraced remote working and, as a business benefit, have extended our recruitment net far and wide, no longer constrained by geographical location. We have also expanded to include new offshore premises and re-organized our internal departments into more self-managing business units that each comprises a mix of home-based, office-based and offshore-based workers. The overall effect on the business is that we have gone from a single office in the UK with a relatively relaxed approach to staff and process monitoring and reporting, to an environment where stricter policies, more detailed and readily available monitoring and reporting is essential to enable us to efficiently manage our business and workforce, regardless of location.

Whilst initial steps to achieve this (in the form of timesheets and activity reports generated by IT) proved to be effective up to a point, it quickly became apparent that it wasn't just staff timekeeping and activities that needed better monitoring. We were now losing visibility of those ad hoc tasks, changes and projects that were visible within a single office space but were now almost invisible to those not immediately involved. As a result, some work was being duplicated by staff and valuable resources were being wasted.

In the past, the tendency for our company to make quick changes to the business for instant benefit (whether staff procedures, supplier changes or IT processes) was common and necessary to keep the business agile and effective. The impact of such changes rarely had a negative effect elsewhere in the business and as such, detailed planning was often bypassed in favour of getting those changes implemented and operational. Now, as a much larger company with more complex IT systems and many more staff operating across international boundaries at all times of day and night, seven days a week, we can no longer apply the same approach to change and can no longer accept the associated risks to the business from such unplanned changes.

We needed a new approach to change management, an official and recognized process with buy-in from both management and staff alike. The question then was how to approach this?

Image 2.1 ProcessFlows IT Helpdesk

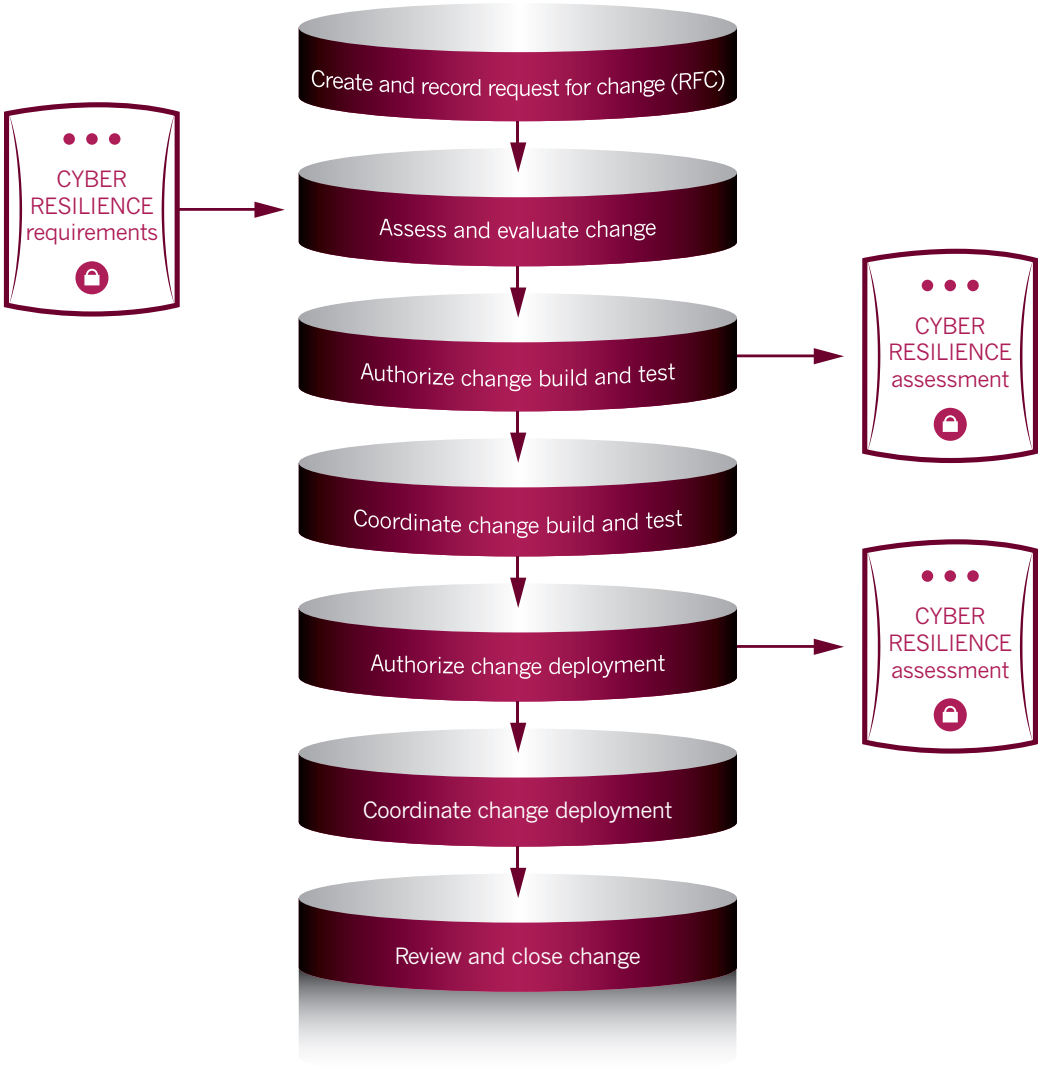

Figure 2.1 Change management activities

The RESILIA Foundation course in Cyber Resilience Best Practice seemed to be the perfect fit to give both management and IT the ideas, guidance and inspiration to evaluate, design and implement suitable processes to enable us to better control and monitor all changes within the business, no matter how large or small. The baseline ITIL processes within RESILIA enabled us to better understand our business requirements and how to achieve those through better policies, processes and procedures as well as how to better communicate those changes throughout the business.

To date, we're well on the way to implementing new policies, processes and procedures within our business to achieve the overview and control we require. Time will tell how effective these new policies will be, but the RESILIA course also promotes continual improvement as another vital piece of the cyber resilience jigsaw and we will continue to adapt and add to these new policies to achieve our current and future goals.

2.3.2 Risk management

Risk management is a key aspect of cyber resilience and we hoped to further our knowledge and understanding of this area in order to enable us to better implement risk management within the business. Whilst RESILIA covers aspects of cyber risk across all areas of the business (not just IT), we initially focused on IT security due to two recent breaches that had caught us somewhat off guard.

As with any typical small and medium sized enterprise, IT security is a fine balance between cost and the consequence of a 'realized' risk. Insufficient security puts the business at greater risk of attack and potential loss of productivity, yet too much investment in excessive security measures hits the bottom line unnecessarily. The RESILIA Best Practice approach helps to identify and evaluate key areas of risk, the impact of such risks, the probability of occurrence of those risks and, perhaps most importantly, it helps senior management identify which risks they consider to be acceptable and which are not. The appropriate level of security can then be designed, with the costs effectively pre-approved by management in order to meet their particular security requirements for the business. This mutual awareness across the organization allows the business and IT to work together to reach the agreed goals.

Our own IT department is now finalizing proposals for a number of improvements to IT security, using the experience of recent security breaches and the information and guidance provided by the RESILIA Foundation course and its associated resources.

One standout area of potential improvement is that of regular and continued staff awareness training and refresher workshops. RESILIA highlights people as potentially the biggest security vulnerability to a business and the course provides excellent guidance on appropriate staff awareness training and the importance of simple but effective staff procedures.

3 Implementing RESILIA

3.1 WHAT MEASURABLE CHANGES HAVE YOU SEEN SINCE COMPLETING THE TRAINING?

Since embracing RESILIA and cyber resilience within the business, we have implemented some changes which have already yielded positive results:

- More restrictive system policies have been implemented to further minimize the potential for staff to create incidents through lack of IT knowledge or understanding. Our internal helpdesk calls have reduced by approximately 25% as a result.
- We have reviewed and made changes to our anti-virus and anti-malware solutions. As a result, the number of security alerts that require manual investigation by the IT helpdesk has dropped by around 30%.
- Administrative access to IT systems has been reviewed and revoked for a number of non-essential technical staff that previously undertook some basic IT system maintenance within their specialist product areas. Whilst this has now increased dependency on the IT department to carry out this maintenance (15-20% increase in maintenance workload), the maintenance is now better planned and documented with the systems being more stable and reliable for end users as a result.
- Project management meetings with the board have become more formal and better structured, with all factors of the business being considered. Whilst no specific statistics are available, the overall benefit is a better organized short and long term plan for IT changes and cyber resilience in general.

- Staff awareness has been actively promoted; ensuring staff understand both the need for any new restrictions that have been implemented, but also their responsibility as part of the overall cyber resilience strategy to help safeguard the business. Staff response has generally been positive, realizing that less risk means less potential problems and less potential downtime for them and their team.

3.2 WHAT WAS THE BIGGEST CHALLENGE DURING THIS PERIOD?

The most difficult aspect of adopting cyber resilience was the underlying feeling that the business was not big enough and did not have sufficient resources to operate an effective cyber resilience strategy. Who was going to conduct all the continual improvement assessments, regular user training and risk assessments required? At the start it did look quite daunting, but as we tackled some of the simpler processes, we soon realized that many of the recommended practices were already being done, we'd just looked at them in a different way. Yes, some additional tasks and responsibilities have been unavoidable, but the impact so far has not been excessive and the anticipated benefits promise to be worth the effort and will help provide us with a better platform for our future success.

3.3 WHAT HAS BEEN THE SINGLE BIGGEST BENEFIT TO ADOPTING RESILIA?

The biggest benefit we have seen with the adoption of RESILIA Cyber Resilience Best Practice is improved communication and understanding between the business and IT, helping management and IT agree an overall strategy for the entire business. The RESILIA lifecycle, based on ITIL, has provided us with the tools to evaluate our business processes and identify not just IT technology issues and business process issues but also staff training and awareness concerns. Because we now realize that all our staff have a critical role to pay in our resilience it has become easier to get middle management on board with a cyber resilient ethos and to realize their responsibilities for both themselves and their team. This includes regular, compulsory training and refresher workshops. Plans are well underway to make changes to known problem areas and the effectiveness of those changes will be re-assessed as part of the continuous improvement process.

4 About RESILIA

RESILIA™ is a portfolio of Cyber Resilience Best Practice publications, certified training, all staff awareness learning and leadership engagement tools designed to put people at the centre of an organization's cyber resilience strategy, enabling them to effectively recognize, respond to and recover from cyber-attacks.

Effective cyber resilience is all about people and behaviours, from the boardroom to the frontline. Everyone has a vital part to play in protecting their organization's most precious information. It requires a balanced and collaborative approach across the entire organization: embedding awareness, insight and skills that will make you more effective in keeping your most precious information and systems safe.

RESILIA Best Practice (based on ITIL®, the proven IT Service Management Best Practice) takes a holistic management system view to help integrate information security into everything an organization does. It considers how security controls fit with IT service management and with an organization's wider management system to provide the right balance of controls to prevent, detect, respond and recover from cyber breaches.

The RESILIA Portfolio

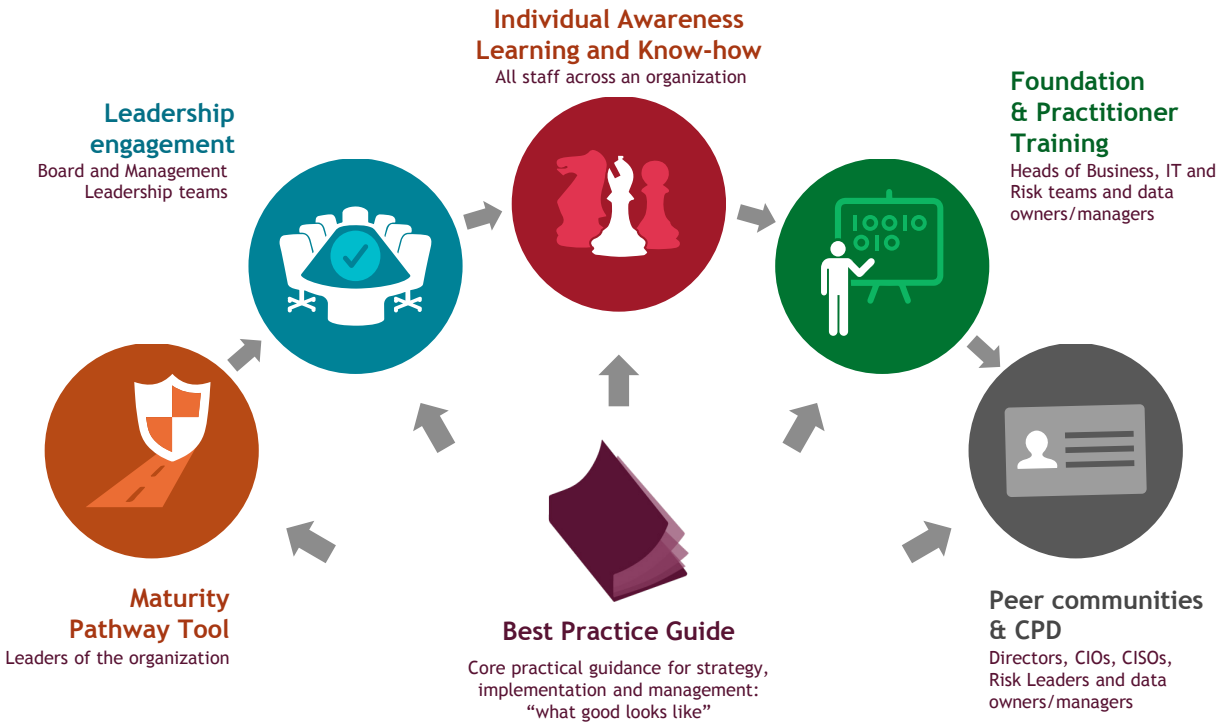

Figure 4.1 The RESILIA Portfolio

5 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 an already enviable track record and an unmatched portfolio of products, including ITIL®, PRINCE2® and RESILIA™. RESILIA is 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 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 for practitioners, fully aligned with AXELOS Global Best Practice.

6 Trade marks and statements

Sourced and published on www.AXELOS.com.