torix

experience. the difference.

RUN

YOUR ENTERPRISE

Zero Outage Protection

Approach for zero outage protection of mission critical systems

1. Introduction

A mission critical system is one which is essential to the survival of any business. When a mission critical system fails or is interrupted, business operations are significantly impacted. Every business no matter its size will have at least one system, which when lost, has a major impact on the business. Impact is variable and always relative to the size of the organisation. Outage may have a direct or indirect revenue impact. It may severely damage the reputation of the company. The bigger the organisation then the more likely its both. With regulatory issues more prevalent than ever, the bigger headlines are not hard to find.

All of us will have personally suffered the 'sorry the computer system is down' moment when we least need it. In November 2014 at a national hunt race in Cheltenham racecourse I was placing bets at Cheltenham racecourse via the Tote. The Tote links up meetings right across the country and sets market pricing according to the volume of bets placed. The last race was run but on the day no-one could collect their winnings after the Tote computer system went down. The same outage occurred back in June 2011. No fines that I know of, but loss of reputation certainly and no doubt lots of angst back at HQ.

In just over a year, the UK has seen two major service outages at our two largest airports Gatwick and Heathrow. In December 2013 Power problems at Gatwick North terminal caused by flooded electricity sub-stations led to the problems. All departures, apart from British Airways, were switched to the south terminal but flights were cancelled as systems struggled to cope. In December 2014 dozens of flights to and from Heathrow airport were delayed or cancelled due to a power outage at air traffic control. London airspace was briefly closed.

In November 2014, Royal Bank of Scotland (RBS) was fined by regulators after a 2012 software issue left millions of customers unable to access their accounts. RBS, NatWest, and Ulster Bank customers were all affected after problems with a software upgrade. The Financial Conduct Authority fined RBS £42m, and the Prudential Regulation Authority fined the bank £14m. It seems that no-one is foolproof.

For customers this is not good enough. If you are providing mission critical IT services, these headlines may give you one of those ‘there but for the grace of god …’ moments. Minimising all risks of an outage of mission critical systems relies upon you having in place (i) a zero outage culture, (ii) globally consistent controls, processes and standards (iii) a proactive attitude to risk management and assessment along with (iv) an enabling technology architecture and (v) an overarching Governance and control framework which delivers pre-emptive monitoring and capabilities by which the organisation can plan mitigation of potential failures. This is what TORI Global calls ‘Zero Outage Protection’.

Much of our acquired learning for Zero Outage Protection has been drawn from the hard earned experience of our associate workforce or through working closely with clients and technology partners. However as this is a relatively new field we have also drawn upon the research of others working in supply chain resilience and critical infrastructure protection. Please read on and learn how your organisation can benefit from the approach set out in this white paper.

2. The essential components of Zero Outage Protection

One fundamental assumption this white paper makes is that no IT service organisation is starting this journey anew. Organisations will already have some or all of the major components embedded within the critical service management and delivery framework. Most will have:-

- Comprehensively resilient technology architectures.
- Monitoring tools in place for most components
- Methodologies and tools for risk management
- Documented controls, processes and standards

When studied at arm's length it seems that the framework is already there for ensuring the mission critical systems never suffer an outage. But they still do – and to us the reason seems to be that organisations have not yet reached a level of maturity where zero outage protection is an integral part of an organisations culture, visible to everyone contributing to the services supply chain.

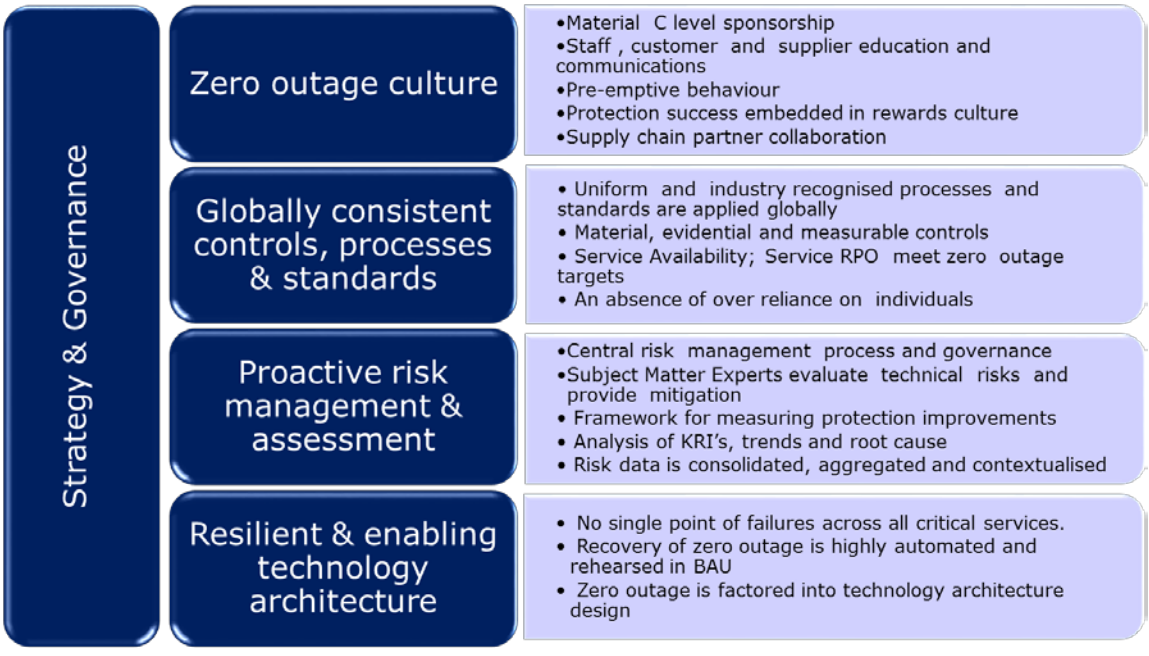

Figure 1 - 5 Components of Zero Outage Protection

Achievement of this level of maturity will never be the result of a one-off programme of activities. Instead it is the culmination of any organisation completing many cycles of activity that start with a mission and strategy. As the cycles of strategy review and delivery

complete the zero outage protection capabilities improve. In the most mature of organisations, capabilities cover the full E2E service supply chain network and become institutionalised in the organisations culture.

3. A framework for zero outage protection

The principle of plotting the journey by declaring the mission, strategies and objectives is well understood and once these are in place the framework starts in earnest with an Assessment & Analysis phase.

In the first cycle this phase requires a broad sweep of the enabling technology architecture. This ensures that nothing is left unconsidered for scope inclusion and kick starts collaboration with the business and service partners. As the programme of works gather momentum it is inevitable that this phase spawns many linked work packages as ensuing phases deliver better protection for each critical service identified.

Before the individual cycles of activity ramp up, then the governance, structure and capability measurement tooling has to be in place.

3.1. Risk assessment & analysis

3.1.1. Purpose

This purpose of this phase is to identify those components that are absolutely critical to the business service supply chain. Data will be gathered about the component vulnerabilities, upstream and downstream dependencies, and an agreed understanding about what requirements and capabilities the organisation needs to protect them.

Throughout the phase, be mindful that assessment and analysis is of the end to end service supply chain. Risks to disruption of the IT Service come in a huge variety of forms. They can appear at any point in the IT service supply chain from primary IT suppliers through to the end customers. They can interrupt the supply of parts, of software fixes, of skilled people. They can cause sudden peaks in demand; they can range in scope from a minor delay to a disaster. Their effects may be localised to one IT service or passed on to threaten your whole chain and that of your customers. A key feature of IT infrastructure service supply chains is that

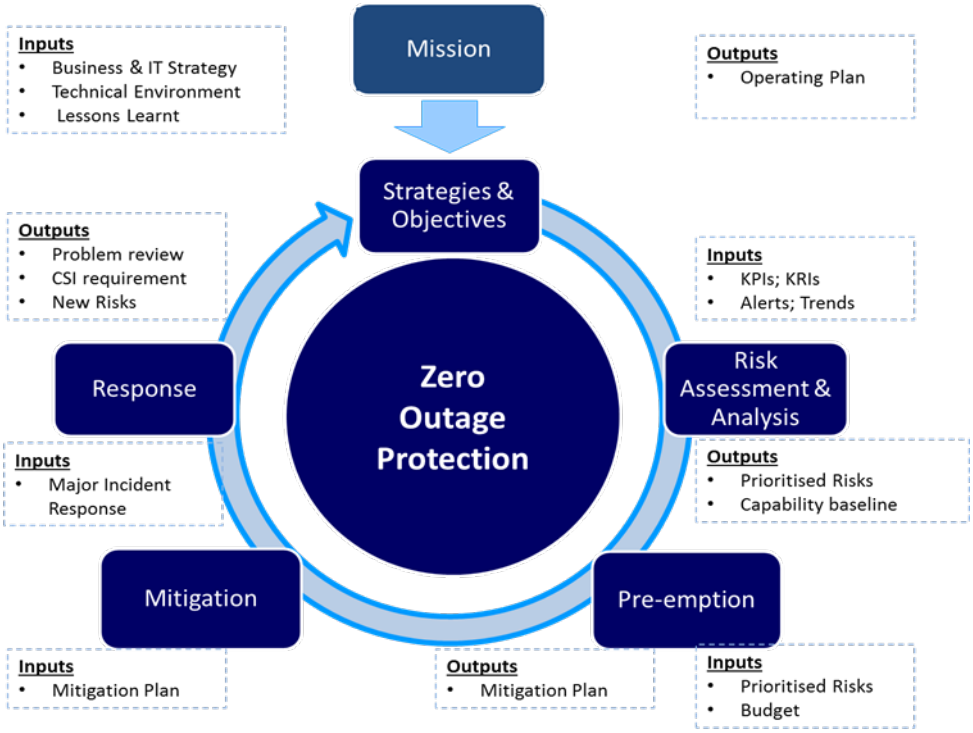

Figure 2 - The framework for zero outage protection

mostly all the components are interlinked at some point. A risk to one component is automatically transferred to all of the others.

The IT services in scope will be agreed with the business so its necessary to agree early on the criteria for defining what is mission critical. Traditional analytical tools such as SWOT (Strengths/Weaknesses/Opportunities/Threats) can be harnessed to good effect here alongside semi-structured interviews and on-line questionnaires. Here at TORI Global we have developed a web-based tool (TECAM) to support you through these four stages, tracking risk mitigation tasks, their allocation and measuring results. TECAM disrupts the traditional approach to risk – simply ignoring it. Managers base risk mitigation on normal conditions. As long as things work normally there are no disruptions and therefore no problems. Managers argue that planning for events that are unlikely to happen is a waste of time as long as there are response mechanisms in place to mitigate the effects. The problem with this approach is that considerable damage is being done before the response takes effect. By making the risk analysis, assessment and actions visible to the

organisation, IT managers can propagate a culture of zero outage protection that addresses risks before they occur.

Key Performance Indicators that determine how well the organisation is protecting its mission critical infrastructure and Key Risk Indicators are Inputs to this phase. The framework objectives include elevating the organisations capabilities to deliver in a manner whereby they can be measured and recalibrated over time with incremental improvement targets set. In mature organisations this recurring cycle manifests as a continuous improvement programme, linked inextricably to business & IT strategy, corporate risk Management and operational planning.

Zero outage KPIs will set targets for service availability and component uptime. KPIs may also set targets for the completion of any number of business continuity tests or component role swapping over a given period of time. These are just two examples however. A full E2E assessment and analysis should consider all the processes, technology and people that interact together to deliver the supply chain to a customer. It therefore follows that the KPIs should not just focus on the service levels being delivered as this is a retrospective activity, but on the underlying capabilities that ensure zero outage protection is being delivered for the future.

3.2. Pre-emption

The Pre-emption phase involves taking the preventive measures and actions needed to avoid service events that may cause an outage or compromise the service supply chain.

Pre-emptive actions may take many forms. Examples include education and awareness, operational process or procedural changes or system configuration and component changes. Inputs to the mitigation plan are the KRI's, KPIs, recurring alerts and trend data. Capability measures of vulnerabilities and risks exposed in the earlier Assessment & Analysis phase. Service supply chain intelligence of risks and pending threats will be exposed continually by alerts and trends drawn from monitoring tools, incident and problem tickets, supplier communications, news and media and sometimes from word of mouth.

Continuous monitoring will determine if there are potential event indications to report. Indications have to be routed correctly to ensure that any warnings which may indicate

whether an infrastructure event is likely to occur or is planned. Routing ensures that accountable owners are warned as to the potential of a service threat thereby allowing them to prioritise the precautionary activities for inclusion in this phases key output – the Mitigation plan.

3.3. Mitigation

The Mitigation phase comprises of the actions that may be taken before or during an event in response to warnings, incidents or a prioritised action arising from the Mitigation plan. Service, infrastructure or delegated business owners accept these actions to minimize the operational impact of a critical service (or asset) outage or debilitation. If Investment is necessary, the cost of failure may often be disproportionate to the mitigation required. Risk analysis from earlier in the cycle will have proven the investment necessity.

Mitigation may well extend beyond the organisation. Dependence on key suppliers may well require an audit and report requesting evidence of the supplier's contracted obligation to support outage of a mission critical asset or service. Collaboration with key suppliers is essential to end to end mitigation. The IT service supply chain is a complex network of interconnected people, processes and technology.

Dress rehearsals that test the organisations responsiveness and agility during a critical service outage should be supported by active participation of service supply chain partners within and external to the organisation. Completing successful dress rehearsals should be a KPI measure for the organisation.

3.4. Response

Zero outage protection objectives should include a KPI which collects the number of major incident responses required in a measurement period. From an IT Service Management perspective a major incident review is one where service stakeholders meet in reaction to a critical service outage and determine what actions are required

Whilst the success of zero outage protection is gauged by the number of major incident reviews, this is reactive and addresses the symptoms. Zero outage protection is more concerned with root cause analysis and resolution which are fed back into the cycle as lessons learnt. A successful zero outage protection programme will have the framework in

place to allocate responsibility for actions via channels such as Problem Management, Change management or through a linked continual service improvement initiative.

4. Maturing towards E2E zero outage protection

Service, Infrastructure owners and IT executive heads all strive to achieve the ideals of an end to end fully integrated, service supply chain which runs continuously and without any disruption. A modern commercial service supply chain is no longer the preserve of the organisation. No service can operate as an island and IT services are nowadays dynamic networks of interconnected people, processes, technologies and organisations. For financial services firms the inbound and outbound logistics of the service supply chain straddling upstream and downstream operations are numerous and complex (Figure 3) introducing a level of risk that can overwhelm if not managed well. For decades now, the drivers behind these logistics have been effectiveness and efficiencies with the objective of driving down cost and increasing quality.

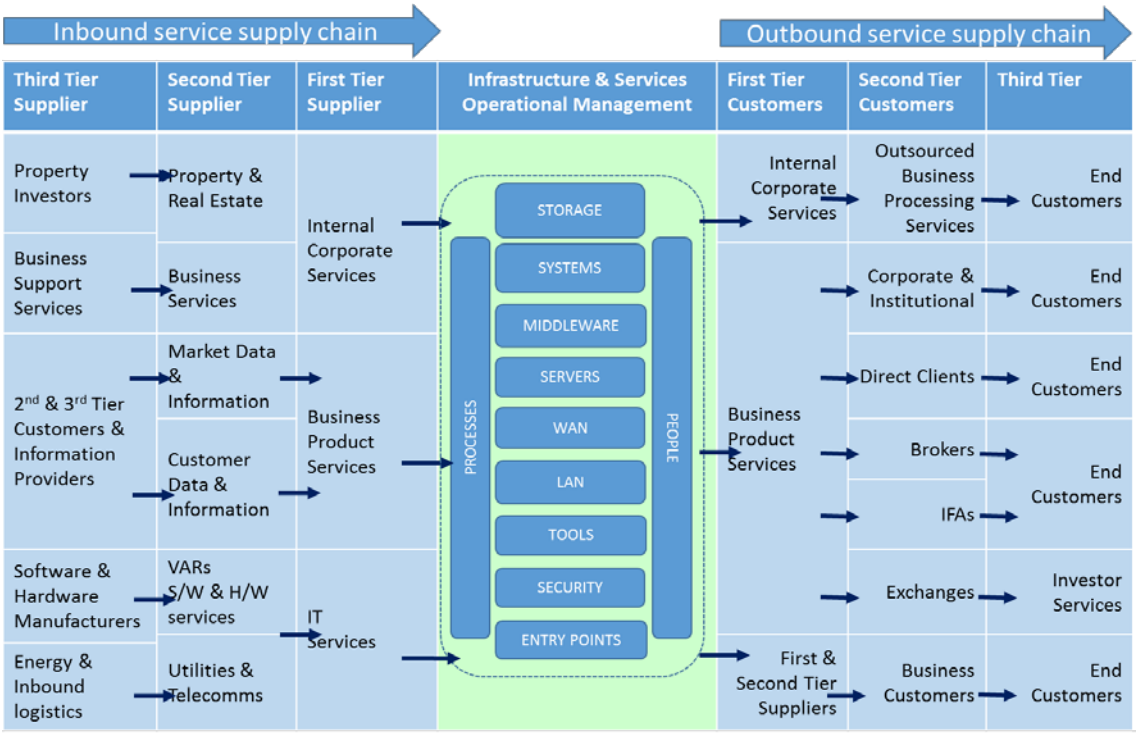

Figure 3 - IT Services Inbound and Outbound supply chain

Ironically, the very factors that propagated effectiveness and efficiencies such as Outsourcing, Data centre and supplier consolidation, software rationalisation, agile demand management and cloud computing now contribute to increased service supply

chain risk as a result of increased dependency. The paradox is that the new drivers of flexibility and agility are hindered by the many layers of interdependency and sometimes bureaucracy that though well intentioned and necessary obstruct them. Removing these is the very thing that results in isolated response to zero outage protection.

Isolated responses will help, but and some may be very effective. But to be wholly successful at zero outage protection, organisations needs to mature into collaborative networks where all the supply chain partners are aligned to deliver zero outage protection. This white papers proposes 4 levels of maturity that can be measured to calculate how capable an organisation is at delivering zero outage protection.

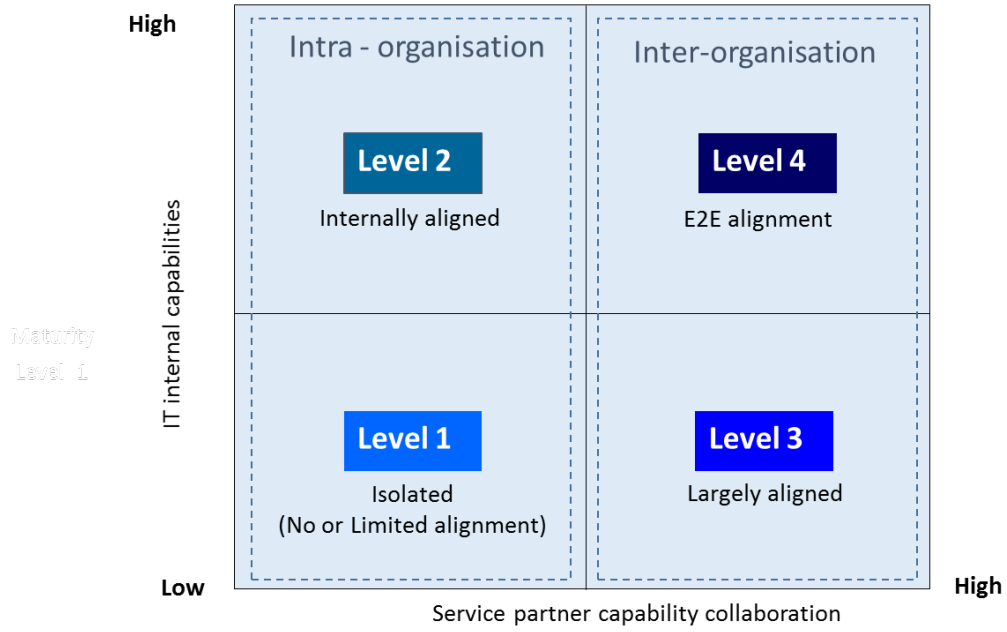

Figure 4 Zero Protection Maturity model

4.1. Isolated

The organisation has pockets of protection but efforts to measure them and improve are rudimentary or non-existent. Resiliency will be built into the production architecture. Highly skilled people may well be in place to manage service and its' change. Processes may be documented and updated as change is introduced.

However other than through scheduled events such as business continuity tests, there is no formal governance that is Accountable aligning all the responsibilities for zero outage capability into a framework that will set targets against which progress can be measured.

At this level of maturity, Managers may follow processes and best practice (e.g. ITIL & ISO27000) that will help to reduce the risk of service outage but they are not specifically focussed on the objective. Incentives for protection against zero outage are not evident in the corporate rewards systems.

There is no visible accountability nor singular focus on implementing zero outrage best practices. Consequently effort is often reactive in response to a new risk, a service outage experience or as result of an isolated managerial initiative. Collaboration is spasmodic and characterised by arm's length, bureaucratic and sometimes even adversarial relationships between the key players.

4.2. Internally aligned

This level of maturity is achieved when the organisation introduces accountability and governance that is able to preside over the framework TORI described earlier in Section 3.

The framework supports the setting for mission, strategy and the delivery of zero outage protection objectives. Individuals are appointed to operational roles that allow the framework to function and deliver improvements. Achievement of objectives and actions that deliver zero outage protection is recognized by the corporate rewards systems.

Zero outage protection capabilities are daisy chained across internal and interdependent services and infrastructures. Zero protection comes under the annual operational planning umbrella with budgets agreed and priorities set. Participation in the planning process sets a base for higher levels of collaborative working across the internal service supply chain.

The setting of mutual targets, measurement by mutually agreed tools and the exchange of information all help to reduce risk and facilitates better supply chain cohesion. This level of maturity will have raised the visibility of zero protection objectives and played a significant part in embedding the required culture and behaviours into the organisation. With this improved visibility the organisation is better positioned to improve incrementally the resilience for the many external nodes of the service supply chain.

4.3. Largely aligned

Here, lessons learnt from the internal alignment are applied to the wider external network. Trends towards the creation of increasingly complex networks of interdependent services, suppliers and trading partners – through strategies of out-sourcing and consolidation in particular – have all heightened the need for inter-organisation collaboration.

Zero outage resilience requires more than just flexibility. True zero outage capabilities must have the capability of introducing resources. It requires an organisation to have the assurance that it and its suppliers have a committed ability to immediately introduce contingency resources where an outage threatens (or) to respond in align to any new major outage risks that have been identified.

Achieving this requires the organisation and its service supply chain partners to invest more time and effort in:-

i) Understanding the service supply critical path and the service supply partners interactions
ii) Analyzing the risks that may cause an outage and providing proactive and reactive mitigation.
iii) Mitigation may require investment and all partners need to consider the limitations of what they are allowed to do.
iv) Mitigation should be tested within a schedule that provides reassurance that the partners have done all they can with resources available to confirm satisfactory protection
v) Committing time and resource to the framework governance

Supplier selection is for most organisations now, a comprehensive mix with many criteria. A demonstration of the suppliers will to collaborate and its own capability at delivering zero outage is another criteria which needs to be added to the mix.

4.4. E2E alignment

This is the desired end state of all zero outage efforts. It is one where all the component parts of the service supply chain unify to plan and deliver resilience. Response is quick as the flexibility and agility required is inbuilt due to the maturity acquired through a prolonged

and detailed collaboration experience. Risks to zero outage protection are managed continuously throughout all the extended service supply chain nodes. This is supported by service supply chain monitoring; awareness that produces intelligence and heighted visibility amongst all the players.

The journey to this end point will not be quick. For most, this will be the culmination of many years of efforts. However once this level of maturity is maintained a certain level of delegation can take place. Self-regulation (allocated to Service Owners) becomes the new norm as the culture, governance framework and enhanced resilience become institutionalised, but always retaining the desired flexibility and agility to cope with change.

5. Summary

Ultimately, Zero Outage performance is the easiest component to measure for IT Infrastructure and Services. Unfortunately achieving the target remains out of reach for many. Isolated initiatives do make headway into the target, but too often they rely on individuals and do not permeate into the subconscious of the organisation. Consequently a key part of the business supply chain to the end customer (i.e. the enabling technology architecture) is underperforming. In the significant majority of organisations this underperformance is accepted as the norm when it need not be.

Within this white paper TORI has set out the five key components of zero outage protection. Together the components provide a framework by which zero outage protection can be delivered and progress can be measured. The approach draws upon proven best practices from Critical infrastructure protection, Supply chain resilience, IT Service Management process and Continuous service improvement along with the learned experience of TORI's extensive pool of practitioners.

This is a fit for purpose framework capable of delivery for in-house, outsourced and SIAM operating models. Organisations considering moving to a SIAM model may be particularly interested in adopting the framework as a methodology for transformation of service availability across key suppliers. In all likelihood, best results will be obtained where the framework is adopted and sponsored by C level executives. However where this is not evident IT executives should consider using the framework as a starting point for a wider business initiative leading to greater supply chain resilience.

If you would like to learn more about the assistance we can offer to help you achieve Zero Outage Protection, contact us by calling **+44 (0)20 7025 5555** or via **info@toriglobal.com**

6. About TORI Global

TORI specialises primarily in providing solutions to industry leaders within global Financial Services organisations. The solutions we offer are innovative, realisable and sustainable with benefits that have real impact. We have a hard earned reputation for experience, quality and professionalism and have built long standing relationships with clients who set the most exacting standards. We are made up of practitioners who, prior to joining TORI, have enjoyed successful careers running business and support functions for many of the global institutions we now count as our clients. Since its inception in 2002, TORI has worked almost exclusively in the Financial Services sector and we have developed a flexible resource pool of highly qualified, usually personally recommended individuals who now work for us regularly and repeatedly.

Our Financial Services domain knowledge, coupled with the expertise of our select group of niche Alliance Partners and extensive Associate bench, allows us to deliver innovative solutions to our clients to meet their most critical requirements. We are driven towards areas of high complexity, high risk and high impact as that is where our clients need solutions delivered.

We support our clients through the delivery of sustainable change programmes in the areas of our core practices. As major business change impacts People, Process and Technology, our key offerings to clients are underpinned by a number of core practices in or across those areas

TORI London
33 Cavendish Square
London
W1G 0PW
+44 20 7025 5555

TORI New York
44 Wall Street
12th Floor
New York NY 10005
+1 212 461 2145