3 Lines of Defence: Controls in IT Services

Introduction

2 years ago TORI published a white paper on Zero Outage Protection (https://www.toriglobal.com/sites/default/files/TORI_Zero_Outage_Protection.pdf). The paper considered which major factors were to be addressed to ensure continuous availability of mission critical systems.

The paper was developed from Financial Services client feedback, indicating the shortfall in satisfying regulatory demands by solutions based on higher resilience and orchestration strategies alone. Exponential expansions in client firms' governance, Risk & Control headcount, functions and processes were ensuring that firms' managers were 'doing the right things' [(1) (2)], but in IT Services where a simple technology gap, a human error or malicious act has a disproportionate impact there was an absence of innovative thought leadership that would help 'do things right' [(1) (2)].

The published TORI paper proposed a strategic approach for firms looking to mitigate risk in service provision of mission critical systems. At the time, response from clients and partners was mixed. Everyone understood the argument and accepted that the strategy was substantiated, based on detailed research and fundamentally solid. TORI sell-side partners were understandably supportive as the message was consistent with their own. From buy-side clients, most skepticism was reserved for the size of the challenge. There was little appetite for new programmes of work advanced from IT where material financial benefit was difficult to justify. Firms had already spent significant amounts on service continuity and the repercussions following the 2008 financial crisis were still very alive.

But a good idea does not disappear just because delivery is complex, large and of a lengthy duration. Populism often drives firms to follow the herd and focus on doing the right things. At TORI, we still believe our approach will ensure that firms do the right things and clients, and some of their supply chain partners, are now benefitting from following our advice. With our assistance the approach has been deployed across a number of different functions and organisations. This update on our white paper sets out what has happened since to justify our original position, why that is and why our approach may be as relevant to other industry sectors and not just Financial Services.

Acceptance of Change and Intolerance of Control

Mark Twain is credited with writing, "The only person who likes change is a wet baby". No-one would disagree too much with these words, but since he wrote it, speed of change has accelerated exponentially. Our acceptance of the speed of change has broken down our resistance and driven ever faster innovation cycles. With each major innovation comes another sprinkling of smaller innovation cycles that supports and spreads the innovation reach. Think of the computer chip and what it spawned; think internet; think iPhone and then think ahead to the next innovation in Financial Services: Blockchain. Blockchain will enable new business models and efficiencies for the economy, but it also introduces new risks and those risks need to be controlled.

Adoption of technology is now arguably at a speed that is far greater than most Financial Services firms can cope with. One reaction to this is to introduce into the supply chain - new partners that already have the right mix of cost technology and service expertise. Cost and service demands also drive new business models that make more effective use of technology. In consequence, the supply chains of Financial Services firms extend far beyond the physical and technological boundaries of the enterprise (Figure 1). With this increase in size and scope and service interdependency comes increased risk. A response to increased risk is increased control. Therein lays the paradox. Firms that innovate quickly and without controls make mistakes. Many mistakes have been and continue to be made, and the financial consequences for everyone have been close to catastrophic. The regulatory response has been uncompromising, yet still data breaches occur as a result of ineffective controls of data access; money

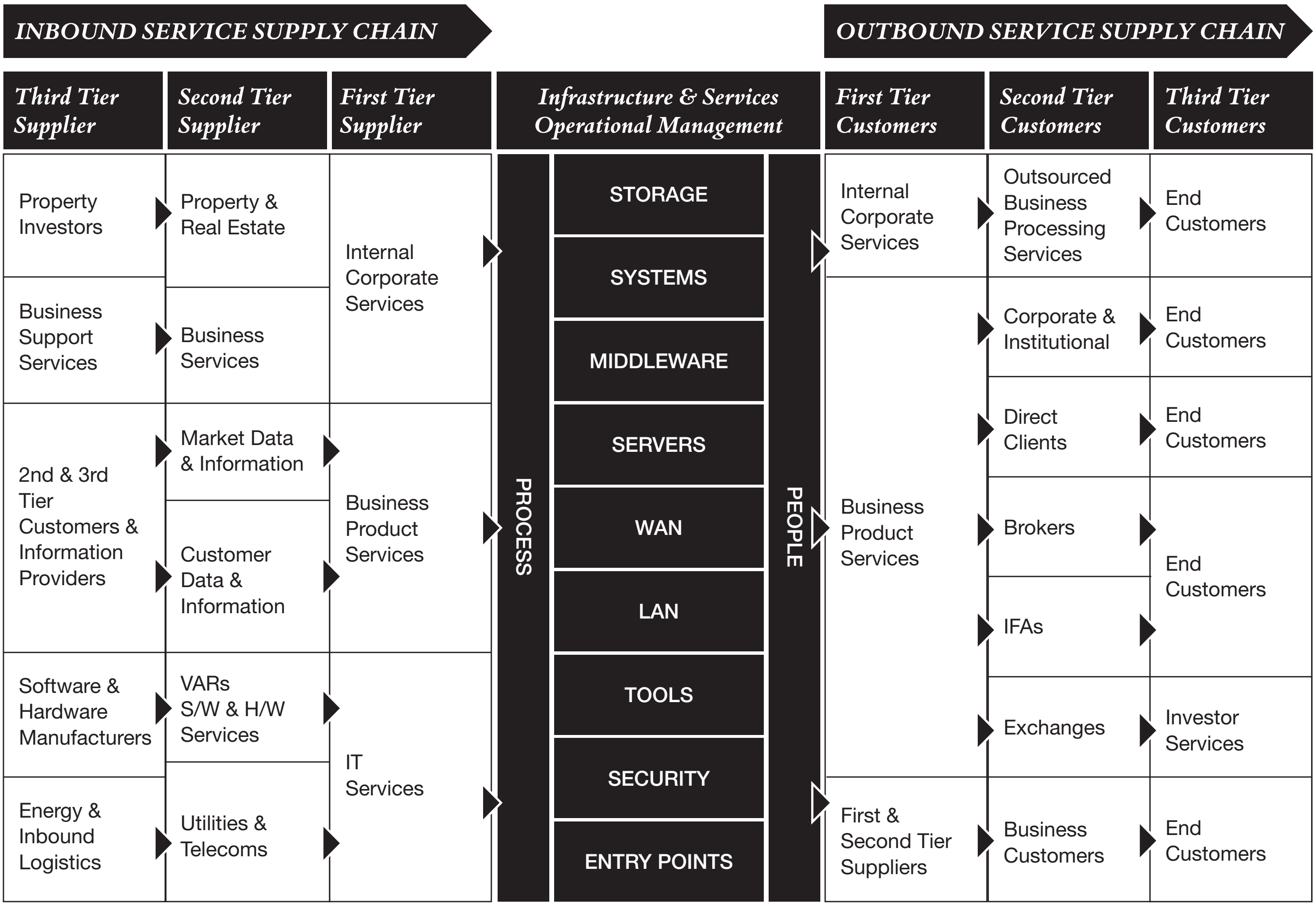

INBOUND SERVICE SUPPLY CHAIN
OUTBOUND SERVICE SUPPLY CHAIN
Third Tier Supplier
Second Tier Supplier
First Tier Supplier
Infrastructure & Services Operational Management
First Tier Customers
Second Tier Customers
Third Tier Customers
Property Investors
Business Support Services
2nd & 3rd Tier Customers & Information Providers
Software & Hardware Manufacturers
Energy & Inbound Logistics
Property & Real Estate
Business Services
Market Data & Information
Customer Data & Information
VARs S/W & H/W Services
Utilities & Telecoms
Internal Corporate Services
Business Product Services
IT Services
PROCESS
STORAGE
SYSTEMS
MIDDLEWARE
SERVERS
WAN
LAN
TOOLS
SECURITY
ENTRY POINTS
PEOPLE
Internal Corporate Services
Business Product Services
First & Second Tier Suppliers
Outsourced Business Processing Services
Corporate & Institutional
Direct Clients
Brokers
IFAs
Exchanges
Business Customers
End Customers
End Customers
End Customers
End Customers
Investor Services
End Customers

Figure 1 Extended enterprise services supply chains

laundering and fraud occurs as a result of inadequate monitoring of employee and client transactional activities; and back doors are left in systems applications due to the lack of depth and frequency of penetration testing. The list is long.

The truth is that sometimes firms just don't learn from their past and apply that learning to the future. Firms, and all of us, carry on doing 'the right things' because of this – our corporate cultures don't always encourage bravery. We are certainly not thinking hard enough or long enough about how we do the right sort of things to control our complex supply chains and the systems and technologies that underpin them. In his seminal book 'The Fifth Discipline' [(3)], Peter Senge offered all of us some cautionary guidance that we would do well to remember. A few are selected below along with their relevance:

I. Today's problems come from yesterday's solutions – firms struggling already to manage legacy and technology debt need little reminder of this. Badly managed innovation and change adds to this risk inheritance. As firms struggle to get to grips with the problem and avoid the price tag that comes with the solution, they outsource the problems to third parties with wider broader experience. But the price tag never goes away and firms are inevitably left with the same issues – a mess for less.

II. The harder you push, the harder the system pushes back – for good reason the FCA/PRA has introduced stiff penalties and fines for firms that do not introduce the necessary due diligence and controls. Eye watering financial penalties and some high profile criminal cases supported by the codes of conduct of the senior manager's and certification regime are examples of how hard the system is pushing back. Within Financial Services firms behaviours have modified in response. TORI has material evidence in other clients of ours, including a leading UK law firm and a Platform Provider, where the requirements of the regulator are now impacting partners to Financial Services supply chains. EU statute in the form of GDPR manifests itself as effort to introduce controls and policies over data access and retention.

III. Behaviour grows better before it gets worse - no this is not the wrong way around! Measures of innovation benefit are usually short term. There is often a substantial time lag between the short term benefit and the long term disadvantages. Think of asbestos and its impact upon the underwriting community in the city of London; think thalidomide where 10,000 birth defects worldwide were caused after its introduction in 1957. As late as 1962 the required regulation was eventually introduced imposing guidelines for the process of drug approval. Far too late for the many thousands more that had taken the drug. Where is the parallel in IT? It's not too hard to spot the examples. In IT, risk analysis is often confined to a project development and delivery cycle. A cynical view maybe, but we all have experience of the risks from a project moving to the Corporate Risk register but without any real mitigation accountability. The risk analysis seldom focusses too long and earnestly enough on the long term maintenance and support activities. How many software development life cycle (SDLC) methodologies have you worked on where the deployment of controls is a feature of development… how many fingers do you have? As time moves on people move, accountability does not transfer and the inheritance remains for someone else.

IV. The easy way out usually leads back in – need I explain more? Read i- iii again.

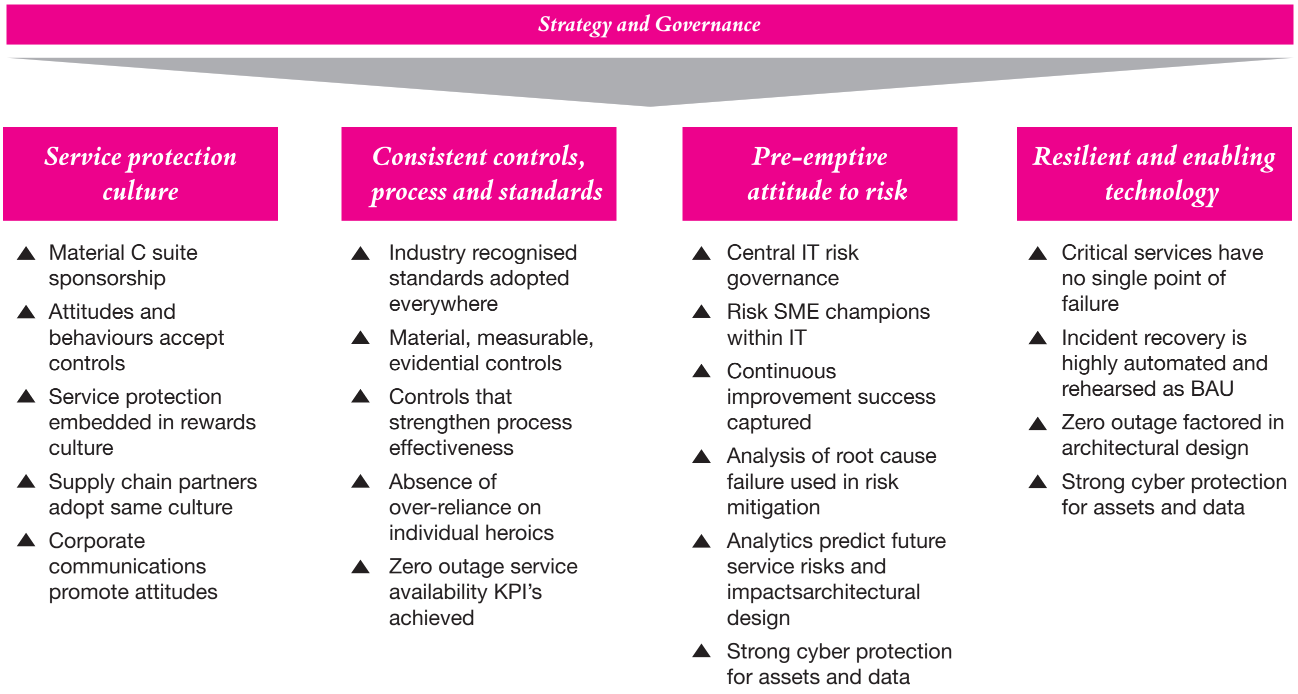
V. The cure can be worse than the disease – read i – iv again…

In summary ,we have become conditioned to accepting the speed of change and in many ways our behaviour and its outcomes of economic growth and higher living standards illustrate that we are doing many things right. Change is popular and as we accept it and see that others feel it's a good thing we do more of it and the cycle gets bigger and faster. But we have also explained why it is that in Financial Services IT change has to be controlled. Rather than being intolerant and frustrated by control we more readily need to accept controls as being essential and good. This is in so many ways counter cultural to social attitudes, and in IT we often compromise with bi-modal IT, where we make use of both agile and waterfall depending on the levels of risk involved. At the same time, we encounter difficulty in finding the right balance between DevOps and the traditional segregation of responsibilities across teams and functions. Yet without controls we will continue to make mistakes. At TORI we believe controls are not a necessary evil but a mandatory good. So in our IT Services world how can we do that and what has TORI been doing to help firms do things right?

The TORI approach to Control of IT Service Risk

Our earlier paper advocated an approach (Figure 2) leveraged by pre-emptive risk management and assessment, in turn underpinned by 2 Lines of Control defences. Technology provides the risk mitigation or the knowledge that allows a firm to identify and deliver the act of mitigation tasks. We advocated a separate governance model for service protection, until at least the new operational norms and behaviours are established.

The acceptance of our approach has resulted in demand for our advisory services to help firms build 1st & 2nd lines of Control defences for IT services. The regulators push for firms to evidence compliance is stimulating their adoption of the 3 Lines of Defence model (3LoD).



Strategy and Governance

Service protection culture

- ▲ Material C suite sponsorship
- ▲ Attitudes and behaviours accept controls
- ▲ Service protection embedded in rewards culture
- ▲ Supply chain partners adopt same culture
- ▲ Corporate communications promote attitudes

Consistent controls, process and standards

- ▲ Industry recognised standards adopted everywhere
- ▲ Material, measurable, evidential controls
- ▲ Controls that strengthen process effectiveness
- ▲ Absence of over-reliance on individual heroics
- ▲ Zero outage service availability KPI's achieved

Pre-emptive attitude to risk

- ▲ Central IT risk governance
- ▲ Risk SME champions within IT
- ▲ Continuous improvement success captured
- ▲ Analysis of root cause failure used in risk mitigation
- ▲ Analytics predict future service risks and impactsarchitectural design
- ▲ Strong cyber protection for assets and data

Resilient and enabling technology

- ▲ Critical services have no single point of failure
- ▲ Incident recovery is highly automated and rehearsed as BAU
- ▲ Zero outage factored in architectural design
- ▲ Strong cyber protection for assets and data

Figure 2 IT Service Protection approach

Generally, demand for our services has been driven by the global banking community, but of late we are seeing increasing activity in the larger insurers and the Financial Services community supply chain. To back up our earlier point about supply chain impact, the service buyers (Banks & Insurers) are pushing their service supply chain partners to evidence their own compliance. In consequence, the impact of the regulations is extending beyond Financial Services. Platform providers, outsourcing firms and legal advisory partners are all examples of the firms that have sought advice from TORI. Our advisory services help our clients design a risk assurance framework that integrates the 3 Lines of defence Controls with ITIL version 3 and other best practices such as Cobit4/5.

3LoD model in an IT Services setting

In the standard 3LoD model (Figure 3), business owned control is the first line of defence in risk management. The various oversight functions (risk/compliance) established by management are the second line of defence, and independent assurance audit is the third. Each of these three "lines" plays a distinct role within the organisation's wider governance framework.

In TORI IT Services adaptation of the model, risk control self-assessment propagates the control objectives for operational processes that are monitored and evidenced to the second line onwards. The firms risk appetite and adherence to prevailing regulation will ultimately determine which processes require the controls. Internal and external auditors will also shape the scope and extent of the operational effort required. Processes may be a mixture of cross-functional ITIL process such as Access management; Major Incident or even Change categories such as Major and Emergency change. They can also include vertical functional processes like Acceptance Testing and Patch Management.

Firms that need to develop and deploy IT Service Controls need to follow a 6 step process (Figure 4):

I. Assessment of the existing processes and controls that constitute the 1LoD. Strengths, weaknesses, opportunities and threats are analysed to draw out the major risks to service.

II. Analysis provides the basis for linking the outputs to 2nd level IT and business risks, risk controls self-assessments, audit points and non-compliance with or gaps in policies.

III. Step 3 requires a benchmark of how the firm is currently applying its controls when contrasted with best practices. Capability Maturity Model Integration (CMMI) for services, COBIT4/5 are adapted to perform the assessment which leads to recommended strategies for the identified processes.

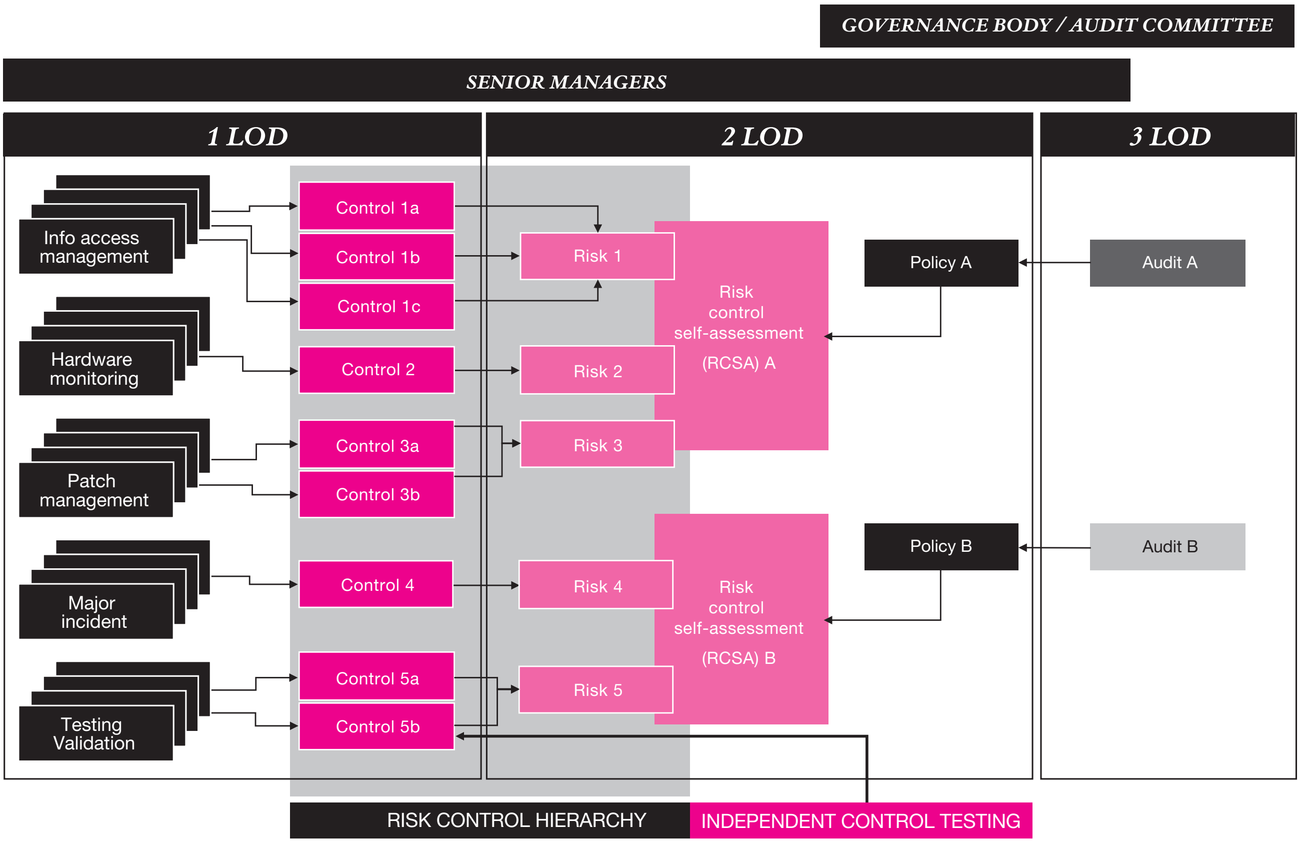


Figure 3 The 3LoD set in IT Services

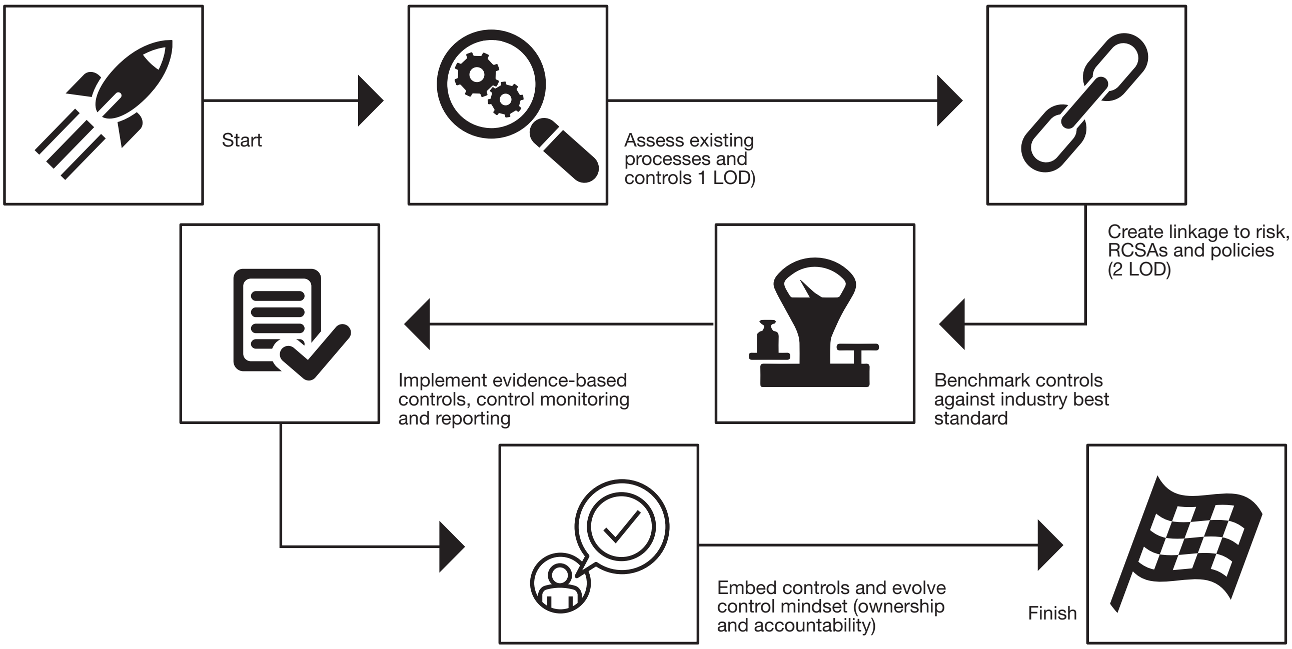

Start
Assess existing processes and controls 1 LOD)
Create linkage to risk, RCSAs and policies (2 LOD)
Benchmark controls against industry best standard
Implement evidence-based controls, control monitoring and reporting
Embed controls and evolve control mindset (ownership and accountability)
Finish

Figure 4 TORI methodology for Controls deployment

IV. Controls are implemented that allocate responsibility and accountability across the first 3 lines of defence. Workshops identify missing controls and gaps within them that in turn create risk. Control point objectives are set and control points are inserted into the process and allocated to accountable owners. Here the emphasis lies in ensuring the control points are actioned and that evidence-based assessments are occurring in accordance with the defined frequency. Controls may be daily, weekly, monthly or annually.

V. Finally, the real success of the deployment requires the firm to embed the controls and evolve the culture into one where controls are accepted as the norm.

Reporting and evidencing control status at a given point in time is a separate challenge. It may be possible to accommodate controls reporting within IT Service management systems such as Service Now, Remedy and other tools of this genre. Operational Risk Management systems are often used to do this, but there are known risks in trying to stretch the capabilities of systems designed for an entirely different purpose. TORI ControlNet software was designed specifically for controls monitoring and reporting and its open design means that it can be integrated with ITSM systems.

Embedding Controls and changing behaviours

As with all deployment, transition into operations is a matter for the project. As we mentioned earlier, the biggest risk is in the focus on the short term benefit and not the long term. Embedding the controls and evolving the control mind-set into a different form of behaviour is a complex challenge that TORI has met with a unique solution.

At TORI we offer a proprietary level 1 control technology tool called ControlNet (www.toriglobal.com/services/risk-control/control-technology). It allows you to identify your control requirements, then manage, monitor, escalate and provide evidence of your control status on a near real-time basis.

Summary and applicability to other industry sectors

Our prior paper was intended as an act of thought leadership. Written 2 years ago, those thoughts have stood the test of time and led to a number of successful TORI engagements. We know there will be more to come particularly as the radar moves from the larger global banks to the second tier, insurers, brokers and other players in the Financial Services community. There we have already seen penetration further down the supply chain as leading Banks and Insurers test the due diligence and risk controls evidenced in their respective partners. GDPR is another regulatory driver of controls over data that will increase demand and deployment for services. But could the model be applied for the same benefit in other sectors?

The 3 LoD model is known to most but certainly not all throughout the Financial Services economic cluster. Based on Rogers's innovation diffusion theory [(4)] its adoption curve suggests it is arguably at early critical mass. There is no doubt that 3LoD will cross into other sectors via supply chain penetration. Telecommunications providers will need to evidence controls to their customers in Financial Services; from experience we see the early evidence that the same is already true of legal advisory firms. BPO firms processing data will need to do the same as a result of customer demands and the GDPR legislation. We anticipate those regulatory demands in other sectors such as Utilities; Health; Environment and Transport will fuel the adoption of the same.

Yet even without these demands and pressures, TORI has set out the case for controls being a mandatory good thing with the 3 LoD a best practice worthy of much wider adoption. Best practices such as CMMI, Cobit4/5, ITIL and TOGAF accentuate their adoption as a route in the organisations journey towards a higher level of quality and maturity. The 3LoD ensures that the change journey is controlled and that the risk and impacts of operational change (in business and IT) is assessed while the journey continues its route.

Bibliography

[1.] Drucker, Peter F. Management, the Individual & Society. s.l. : Routledge, 2001.

[2.] Bennis, Warren and Nanus, Burt. Leaders: The strategies for taking charge. s.l. : Harper Collins, 1985.

[3.] Senge, Peter M. The Fifth Discipline. s.l. : Century Business, 1993.

[4.] Rogers, Everett. Diffusion of Innovations. s.l. : Free press, 2003.

About TORI

It takes courage to embrace change and transform your business. We know. We've been there. That's why we set up TORI Global. To be a credible alternative to the 'big four' within Financial Services – by putting real industry experience at the heart of consultancy. So our clients get the best independent advice and specialist expertise for the success they deserve.

We are truly global. Headquartered in London, with offices in New York and Dubai and recent expansions into Bangalore and Singapore, there is a TORI network across the globe with aggressive growth plans.

At TORI Global we believe that delivering success for customers relies on successful partnerships, and that successful partnerships are founded on the values of Trust, Openness, Respect and Integrity.

Why our clients work with us

We're experienced. The TORI team have held C-level and senior roles in global organisations. We understand their business needs and the challenging sectors they work in.

We're outcome based. We complete every project with speed, agility and a clear return on investment. We don't just deliver value, we prove it.

We're agile. Our extensive network of Associates and partners means we can scale up and down quickly. We can put the right people on the job to deliver the best solutions.

We're flexible. Our flexible pricing model allows us to tailor projects to our clients' specific needs. We will always find the right balance between quality, cost and risk.

We have no external investors. We believe this brings greater integrity and personal commitment to our client engagements.

We have a strong track record. Our long-standing client relationships are testament to our collaborative approach. We have achieved success together time and time again.

We have a no-nonsense attitude. Shying away from hard truths is not our style. Bringing a candid pragmatism to any problem is. Sometimes we may have to tell our clients what's needed, not what they want to hear. We believe they'll thank us in the end.

TORI London	*+44 (0) 20 7025 5555*
TORI New York	*+1 212 461 2145*
TORI Dubai	*+971 4 558 8798*
TORI Singapore	*+012 3 456 7890*
TORI Bangalore	*+9180 4647 1302*

toriglobal.com
info@toriglobal.com

TORI
Experience. The difference.