Chartered Institute of Internal Auditors / Audit Leaders

Business resilience

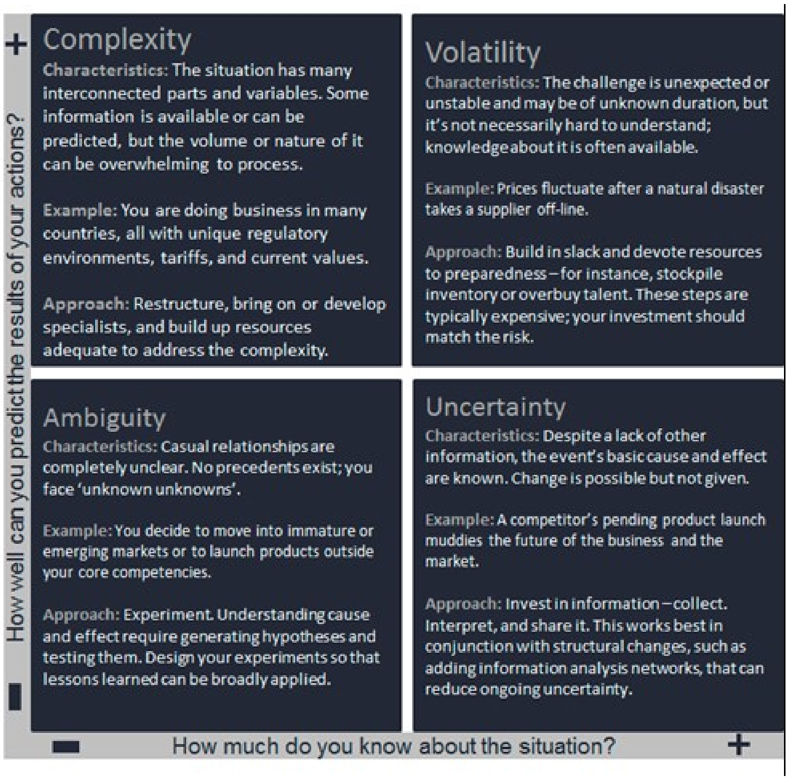
Disaster recovery assurance used to be a staple on the audit plan. Now the buzz is all about business resilience. But is this just consultant speak … and if so what happened to business continuity?

This piece looks at the evolution of managing significant disruptive events and asks whether internal audit is providing the assurance that matters to the board.

A changing world

Nothing is certain. Often the difference between organisational survival and failure can be their response when things go wrong. Organisations have a symbiotic relationship with their environment; impacted by natural disasters such as flood (Texas/Japan), drought (California/Australia/UK) or volcanic activity (Iceland) and those made by man from supply chain failures (CO2) to cyberattacks (NHS), terrorism and Brexit.

VUCA is a term often used to describe the world today; Volatile, Uncertain, Complex and Ambiguous. With so much disruption and the increasing potential for catastrophic events it's no surprise that business continuity has evolved to match the world in which it operates.



How well can you predict the results of your actions?
+
−
How much do you know about the situation?
−
+

Complexity

Characteristics: The situation has many interconnected parts and variables. Some information is available or can be predicted, but the volume or nature of it can be overwhelming to process.

Example: You are doing business in many countries, all with unique regulatory environments, tariffs, and current values.

Approach: Restructure, bring on or develop specialists, and build up resources adequate to address the complexity.

Volatility

Characteristics: The challenge is unexpected or unstable and may be of unknown duration, but it's not necessarily hard to understand; knowledge about it is often available.

Example: Prices fluctuate after a natural disaster takes a supplier off-line.

Approach: Build in slack and devote resources to preparedness – for instance, stockpile inventory or overbuy talent. These steps are typically expensive; your investment should match the risk.

Ambiguity

Characteristics: Casual relationships are completely unclear. No precedents exist; you face 'unknown unknowns'.

Example: You decide to move into immature or emerging markets or to launch products outside your core competencies.

Approach: Experiment. Understanding cause and effect require generating hypotheses and testing them. Design your experiments so that lessons learned can be broadly applied.

Uncertainty

Characteristics: Despite a lack of other information, the event's basic cause and effect are known. Change is possible but not given.

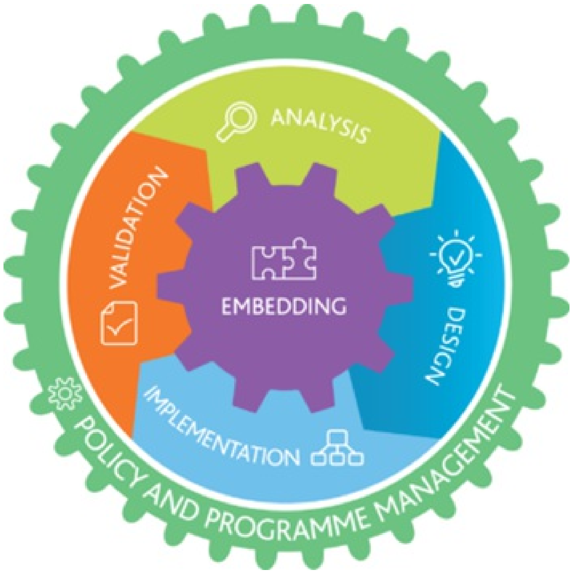
Example: A competitor's pending product launch muddies the future of the business and the market.

Approach: Invest in information – collect. Interpret, and share it. This works best in conjunction with structural changes, such as adding information analysis networks, that can reduce ongoing uncertainty.

Source: Harvard Business Review January-February 2014 Issue

Evolution

Initially organisations focused on prevention together with planning and documenting their approach to major disaster events such as losing a head office facility, a call centre or a major trade route such as the Suez Canal being closed; all high impact but relatively low likelihood events. Internal audit provided assurance that plans were relevant, updated and stored off-site but thankfully such plans were rarely tested.



Alongside this proactive organisations also set up crisis management structures and extended disaster recovery to detail business continuity plans for all functions. The creation, maintenance and co-ordination of so many disparate plans became an industry of itself.

The industry is business continuity management (BCM). According to the Business Continuity Institute it is a process (diagram opposite) that guides organisations in identifying threats, designing responses, implementing a plan and measuring effectiveness. It's an ongoing process to continually build and improve organisational resilience.

Whilst BCM is recognised as having value it has remained largely concerned with driving consistency and improving performance such as installing a dark site (technology only) for when critical systems fail or dual outsourcing of a call centre to overcome a single point of failure in a business model. Scenario workshops, testing call trees, crisis simulations are all typical endeavours that organisations engage in to prepare themselves for the worst.

All of the stages remain relevant; the evolution of BCM builds on the previous activities, it does not replace them like software updates.

However, the evolution now is about business resilience. The theory favours adaption rather than just recovery and continuity. A concept that is perhaps easier to accept in a VUCA environment than planning for events that may never happen when so much is already happening. It is holistic, beginning with strategy and culture rather than serving as a consequential afterthought.

- Crisis Management: a structured approach to dealing with emergency situations
- Disaster Recovery: a documented approach to get back to normal after a disruptive event
- Business Continuity Plans: detailed guides for temporary arrangements and recovery plans
- Business Continuity Management: process and framework to build resilience
- Business Resilience: ability to adapt to incremental change and respond positively to disruption

Organisational resilience

All organisations are different. Each is continually changing, either through its own actions or the environment it is operating within. Whilst there may be sector specific challenges an organisations culture, strategy and capabilities will make its response unique.

Resilience relies on adaption at all levels; strategic, operational and tactical.

Strategic resilience involves:

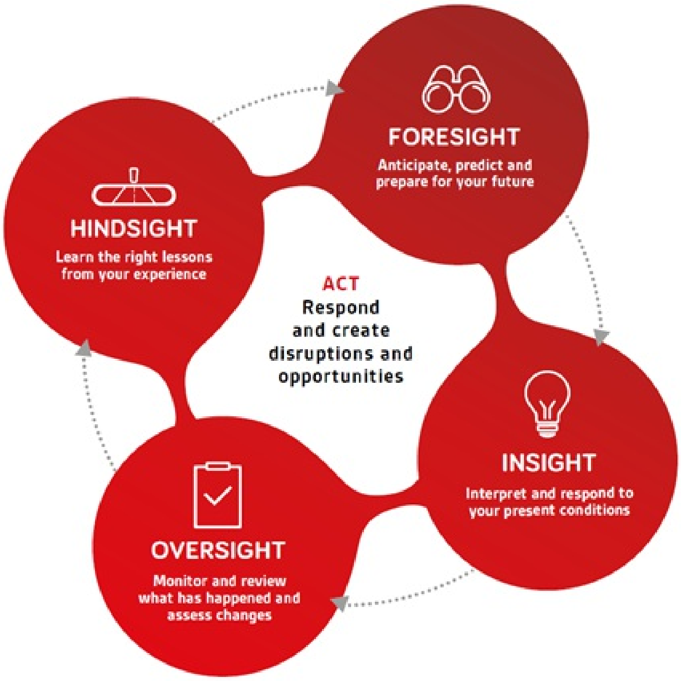
- meaningful and transparent values shared within and outside the organisation
- effective corporate governance particularly clear accountabilities
- cultivating a resilient culture, focusing on purpose, values, future and engagement
- identifying emerging risks and issues
- anticipating events and change
- encouraging disruptive thinking
- seeking out disconfirming evidence and alternative opinions
- assessing vulnerabilities
- planning for a range of scenarios/outcomes

Operational resilience involves:

- developing a culture of personal and team resilience
- leaders managing and developing resilience as a core skill for themselves and others
- including questions on personal resilience, stress/well-being during interview
- monitoring activities for pressure points to deal with them quickly, key risk indicators
- maintaining business continuity plans
- being proactive

Tactical resilience involves:

- genuine empowerment at all levels of the organisation
- embracing a culture of learning and freedom to experiment
- embedded risk management, individual accountability for risk
- rapid escalation protocols for issues/concerns
- creating a library of external statements for different scenarios
- quickly making informed decisions
- agile mind-sets/ways of working


FORESIGHT
Anticipate, predict and prepare for your future
INSIGHT
Interpret and respond to your present conditions
OVERSIGHT
Monitor and review what has happened and assess changes
HINDSIGHT
Learn the right lessons from your experience
ACT
Respond and create disruptions and opportunities

Where is assurance needed?

Research at Cranfield University also followed the evolution of BCM identifying that an organisation needs balance across two sets of tensions; defensive and progressive plus consistency and flexibility. Part of this is a new BSI methodology for organisational resilience, 4Sight; the outline of oversight on page 21 could be a charter for internal audit!

Recognising the role of culture and strategy, oversight also references risk appetite, operational effectiveness, risk management and compliance.

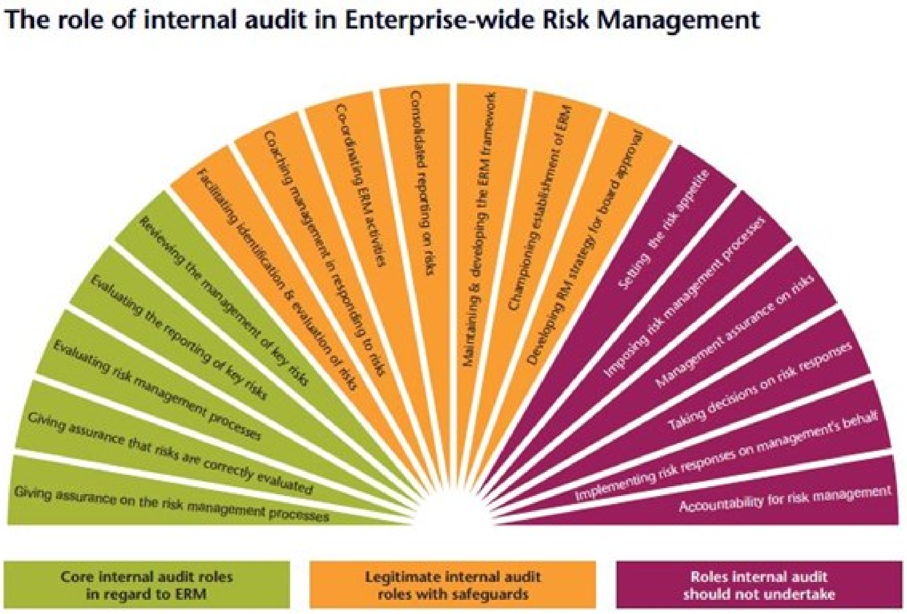
Of the two aspects to resilience, assurance over preparations and adaptability regarding disruptive events is relatively straightforward; environmental awareness, effective risk management, crisis management and recovery planning. The more challenging aspect is providing assurance of the organisations ability to adapt to incremental change.

It is useful to think about the 3 lines of defence in relation to assurance. What are the first and second lines doing in the resilience space? To aid board understanding, could internal audit facilitate the creation of an assurance map specific to resilience?

Risk Management

Organisations that have not reached risk maturity (effective and embedded risk management) will likely struggle to achieve organisational resilience; the concepts are interdependent and share so many similarities that they could be one and the same. Without the capability to identify emerging risks (think PESTLE) and vulnerabilities the organisation will remain reactive, unable to anticipate and adapt.

What role does internal audit have not only in providing assurance to the board on the effectiveness and efficiency of what is in place but in supporting the organisation to improve? There are legitimate roles that internal auditors have in risk management, relevant for all functions not just those with joint audit and risk functions; facilitating, educating, advising, coaching, co-ordinating and reporting.


The role of internal audit in Enterprise-wide Risk Management
Giving assurance on the risk management processes
Giving assurance that risks are correctly evaluated
Evaluating risk management processes
Evaluating the reporting of key risks
Reviewing the management of key risks
Facilitating identification & evaluation of risks
Coaching management in responding to risks
Co-ordinating ERM activities
Consolidated reporting on risks
Maintaining & developing the ERM framework
Championing establishment of ERM
Developing RM strategy for board approval
Setting the risk appetite
Imposing risk management processes
Management assurance on risks
Taking decisions on risk responses
Implementing risk responses on management's behalf
Accountability for risk management
Core internal audit roles in regard to ERM
Legitimate internal audit roles with safeguards
Roles internal audit should not undertake

Risk-based audit planning should already ensure that assurance is provided over the management of individual risks critical to resilience. An additional area to consider is the extended risk enterprise, a more advanced approach to supply chain management, thinking about all relationships and dependencies impacting operations and reputation.

Culture
All organic life has its own unique DNA and an organisations culture is exactly that, threading through governance structures, conversations at the coffee machine and everything in-between.

The cultural enablers of a resilient organisation take time to develop and maintain. How is your organisation addressing this? Are there disparate activities or a formal programme? Does the board understanding its responsibilities in respect of the culture?

Auditing culture has been a focus of the Institute for some time as it is the root cause of many control failings and weaknesses. Prevention is always better than cure and DNA carries the antibodies and resistance required for robust resilience.

Back to Basics
Organisational resilience has firm foundations in the internal control environment. A key learning point highlighted by the 4Sight methodology is the need for multiple layers of protection for all critical assets (e.g. people, products, property, information etc.) and compliance with procedures, processes, values etc.

Internal audit should already be providing assurance of this nature. However, repackaging it with new language could be beneficial to assist the board in their understanding of resilience. It may also be useful for chief audit executives needing to reinvigorate the value and relevance of their function.

Closing Thoughts

Shift happens…whether the board is ready for it or not. There are a litany of organisations that have not been prepared; Pan Am, Kodak, ToysRUs, Lehman Brothers to name but a few. Organisational resilience is not an optional competency for the volatile, uncertain, complex and ambiguous landscape of today. Insurance premiums cannot protect against reputation damage and lost customer confidence but resilience can. Do your audit results evidence that genuine resilience assurance has been provided to the board for them to act upon or if the organisation collapsed would questions over the role of internal audit be justified?

> *In the business world, the rear-view mirror is always clearer than the windshield (eng. windscreen)*

> *Warren Buffett*