Synechron

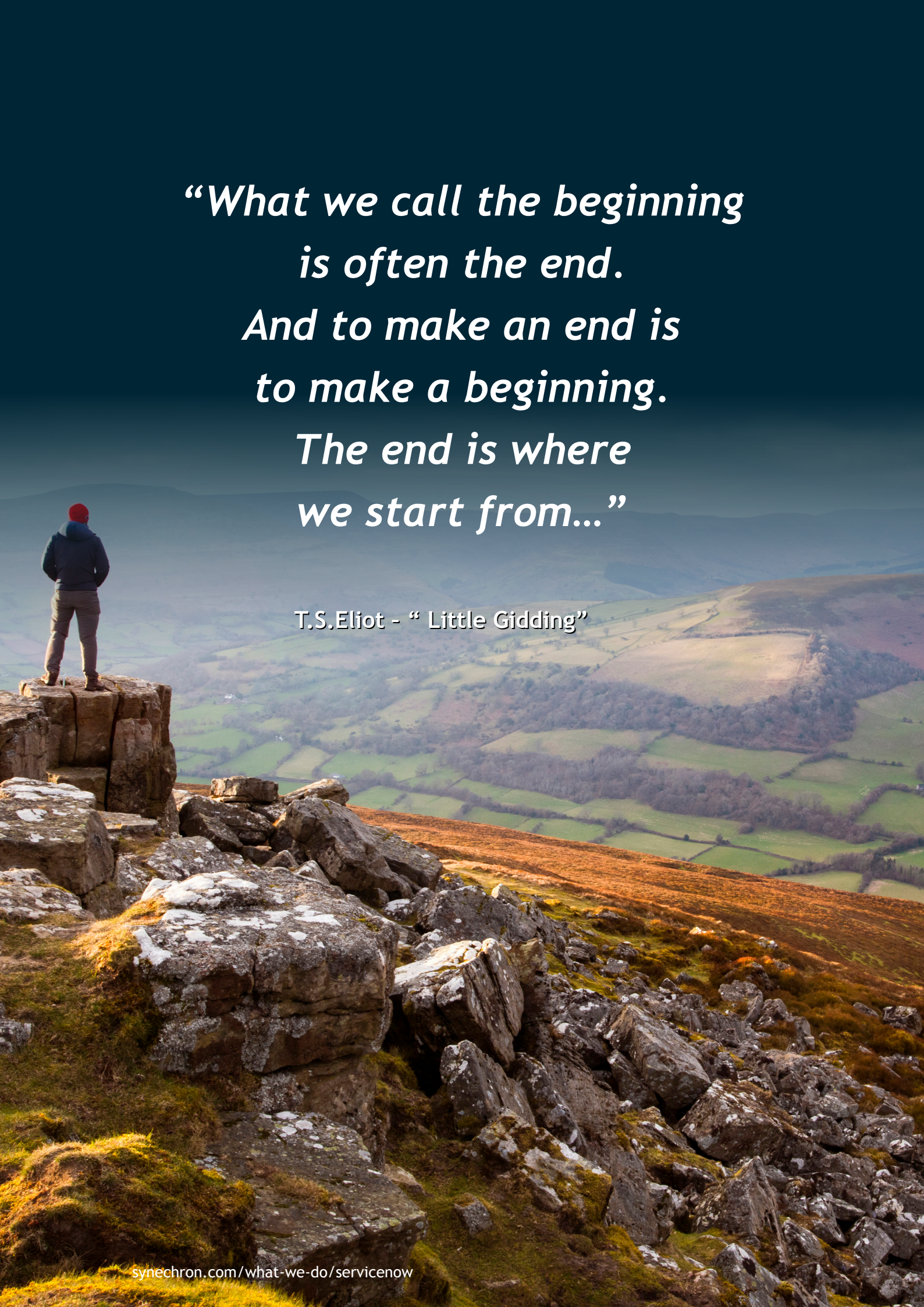
Whitepaper

The End is Where we Start From

How to move from transactional to value-based GRC.

Richard Taylor

Head of Resilience at
Synechron | ServiceNow


“What we call the beginning
is often the end.
And to make an end is
to make a beginning.
The end is where
we start from…”
T.S.Eliot - “ Little Gidding”
synechron.com/what-we-do/servicenow

We urgently need to focus on the positives!

When contemplating the notions of “GRC” or “Security,” what initially springs to mind? Perhaps terms like “Slick,” “Efficiency,” “Automation,” “Value-driving,” or “Integrated”? If you’re akin to the average individual within an organisation, it’s probable that terms such as “Expensive,” “Burden,” “Opaque,” “Scary,” and “Tedious” dominate your thoughts. But why is this the case? Why are the fundamental pillars of a safer, fairer, and superior world often associated with such negative connotations?

“The predicament commences at the very outset, rooted in how we frame and articulate the task at hand.”

The predicament commences at the very outset, rooted in how we frame and articulate the task at hand. Let’s delve into how these concepts have traditionally been defined and operationalised. GRC/IRM. What terminology serves as our gateway into this domain? We encounter phrases like Control Tests, Risk Assessments, and Audit Observations. When it comes to Security, terms such as Vulnerabilities, Security Incidents, and Threats prevail.

What do all these terms share in common? They all constitute transactional inputs. Are they significant? Undoubtedly, yes. However, they tend to steer our attention towards tactical, transactional, and input-driven approaches, often at the expense of a broader, more strategic outlook. This resembles the mentality employed by ineffectual politicians who boast about the magnitude of the “investment” they’re making to address a recently highlighted issue, lacking clarity regarding the allocation of funds and, more crucially, the tangible outcomes expected.

What's conspicuously absent, naturally, is the connection between transactional inputs and the ultimate value delivered by top-tier GRC practices. Fortunately, a solution to this quandary exists. Although seemingly straightforward, it necessitates a paradigm shift in mindset and embarks upon a three-stage journey.

Your three-stage journey; from transaction, to asset, to value.

A transactional start point for most organisations.

Many organisations find themselves, regrettably, stuck at the initial phase of their resilience journey, primarily fixated on executing tests or patching up existing systems—a perpetual cycle akin to running on a hamster wheel. While these organisations may be meeting the check boxes for Compliance, Risk, Audit, and Security, there exists a critical missing link where these transactions are tethered to their corresponding endpoints, containers, applications, and services. In essence, they constitute integral components of a more comprehensive and cohesive system of "Assets" (referred to technically as "Configuration Items" or "CIs") and their interrelations and functionalities, amalgamated to construct a Configuration Management Database or CMDB.

Considering the substantial investments in effort, time, and costs associated with monolithic CMDB implementations—where full design and deployment projects spanning over two years are commonplace among large enterprises—it's hardly surprising that this scenario persists. To facilitate progress and cultural change (moving to shared goals of risk management and business delivery (go faster, break less)) in this realm, we must advocate for a shift in perspective from one driven by burdens to one focused on benefits.

Consider the analogy of car insurance—while none of us relish the idea of paying for it, we understand its necessity. It provides us with the assurance that in the event of an unfortunate mishap, the necessary funds will be available to cover repairs, ensuring a swift restoration to normality, with minimal impact on both our lives and wallets.

Focusing on value driven outcomes, measuring these outcomes and making them transparent is a critical lever to moving away from point in time transactional measures, and is the starting point to positive cultural change towards audit, risk and controls.

As part of this, moving our CMDB implementations from monolithic to incremental and iterative where these benefits are delivered early and transparently and in a more agile fashion is essential.

In essence, this transition from burden to benefit underscores the need to ascend to the next echelon of maturity in this journey, namely the asset-focused stage.

Making the switch to an asset focus.

Once the pivotal decision to establish a Configuration Management Database (CMDB) is made, the incremental journey toward unlocking value commences. Our approach to this endeavour draws inspiration from the ancient Greek maxim – "Γνώθι σαυτόν" or "Know Thyself." Originating from the inscriptions at Delphi's forecourt, this wisdom advises individuals to understand themselves before consulting the Oracle Pythia, enabling them to pose high-quality questions and consequently receive high-quality answers.

Thus, the initial stride in self-awareness entails inventorying, defining, and subsequently managing/controlling Configuration Items (CIs) and their relationships with applications, services, and associated personae, effectively constructing a comprehensive depiction of organisational "Assets." While "Asset" may not be particularly technical, it emerges as the chosen term in English.

"...And every phrase
And sentence that is right (where every word is at home),
Taking its place to support the others,
The word neither diffident nor ostentatious,
An easy commerce of the old and the new,
The common word exact without vulgarity,
The formal word precise but not pedantic,
The complete consort dancing together),
Every phrase and every sentence is an end and a beginning…"

T.S.Eliot – " Little Gidding"

Armed with this new-found, refined, and comprehensive organisational profile (which can/should of course be delivered in a business objective prioritised, incremental fashion as previously alluded to), the subsequent phase involves comprehending how (and to what extent) any transient risk-bearing event (e.g., Emerging Threats, Zero-day Vulnerabilities, Data Breaches, Control Test Failures, Key Risk Indicator Failures, Failed Changes, etc.) would impact these assets.

This marks a notable shift. Essentially, we've reversed the dynamic, making the assets come to you rather than vice versa. In other words, the Asset Owner (e.g., Service Owner) now possesses a clear overview of all pertinent Risks, Controls, Audit Actions, Threats, Vulnerabilities, Security Incidents, Continuity Items, and Third-Party Events. They are no longer compelled to adopt a reactive stance, constantly chasing after issues; the focus has pivoted from transactions to assets.

synechron.com/what-we-do/servicenow

The implementation of the RACI model (Responsible, Accountable, Consulted, Informed) for each asset encourages the respective personae to assume ownership over their designated aspect of the asset, particularly when bolstered and enforced by relevant Frameworks, Policies, Standards, Procedures, and Metrics that dictate their obligations based on their roles. Consequently, the concept of Resilience becomes ingrained within the organisational fabric, changing “Have to” to “Want To.” And as the necessary tools, support and shared goals have been provided to change the culture of the delivery organisation to be risk and control focused, we then have shared delivery goals within the control organisation. People are doing controls because it’s the right thing, not because they are told to. It’s what within DevOps is referred to as “Controls as Products” and can also be facilitated by “Policy As Code Engines” (PACE)

It’s imperative that these Governance, Risk, and Compliance (GRC) artifacts persistently maintain and sustain this organisational self-description—falling into the trap of viewing this as a one-time task is all too easy. The data swiftly grows stale, diminishing in value accordingly.

In scenarios of extreme volume, an enterprise-grade CMDB experiences thousands (potentially tens or hundreds of thousands) of updates daily. This demands concerted effort, necessitating a clear understanding of how these efforts yield benefits—ranging from reducing organisational friction and errors to enhancing regulatory compliance (e.g., NIST CSF, DORA), enabling automation, and facilitating AI integration. While the benefits are manifold, it’s essential to ponder, “what purpose does an asset serve”?

By definition, an asset is “a person or thing that is valuable or useful to somebody/something.” Hence, assets are utilised to achieve outcomes or provide value to an organisation. The critical question then arises: where are these outcomes or values defined?

"…We shall not cease from exploration
And the end of all our exploring
Will be to arrive where we started
And know the place for the first time."

Reaching our value destination

At last, we catch a glimpse of our radiant destination on the horizon—Value—the quintessential raison d'être behind our pursuit of Governance, Risk, and Compliance (GRC), Information Risk Management (IRM) and Security endeavours. Furthermore, we find ourselves embarking on the evolution of the Configuration Management Database (CMDB) into a broader, more expansive, and outcome-centric concept—a "Digital Twin"!

Originally coined in the manufacturing realm, the term "Digital Twin" becoming relevant for any enterprise striving to harness the advantages of advanced automation and AI capabilities, enabling them to outpace competitors and navigate a landscape where every passing minute holds significance.

With our Digital Twin in tow, we can now delineate (and ideally quantify) our Objectives and Outcomes—referred to as "value-based use cases"—alongside all the underlying components that bolster these objectives, down to the minutest detail, such as individual network cards or containers.

Consequently, any transient risk-bearing event can promptly and visually reveal its impact on our objectives. For instance, questions like, "Can we launch a new mortgage product/drug/car/foodstuff/aeroplane next month, considering the real-time risk landscape?" become readily answerable.

What ensues is the ability to furnish the C-Suite with a comprehensive overview, articulated in their language, detailing precisely where their

investments have been allocated and how they contribute to safeguarding and advancing organisational value in near real-time—a paradigm shift that's revolutionary yet undeniably logical.

Consider a hypothetical scenario: the Cyber Threat Intelligence team uncovers the emergence of Log4J mark 2 as a near zero-day Vulnerability. The immediate query from the board is, "What is impacted?" In a previous experience with a manufacturing client, it took a staggering 10 weeks to address this question when mark 1 surfaced—a potentially calamitous delay.

However, armed with a well-structured digital twin, complete with a Software Bill of Materials, addressing such inquiries becomes swift and efficient. This includes assessing potential impacts on clients/suppliers—a capability that should be standard practice rather than an exceptional feat.

As is customary in any argument, when seeking to comprehend a phenomenon, it's instructive to reverse or invert it. Thus, let's ponder, "Is it acceptable for it to take 10 weeks to ascertain threat impact mapping?" At Synechron, we assertively argue otherwise, especially considering that your job, your company's welfare, and even your country's prosperity could hinge on it.

Value, therefore, manifests as follows:
The board gains insight into the allocation and trajectory of investments, along with the impact of real-world events on their objectives and outcomes, articulated in a language they comprehend.

Technologists discern the infrastructure implications of incoming threats and risks, enabling alignment with business priorities and reinforcing the significance of their contributions.

Security professionals leverage real-world business impact modelling to harmonise posture and prioritise responses, thereby enhancing organisational resilience and fortifying defences against emerging threats.

Turn your Negatives to Positives

Just as electricity flows from negative to positive, we need to start flowing towards a more positive view of the world of Resilience and its business enabling, culture changing potential.

The days of tactical, adhoc Governance, Risk and Compliance are nearing an end – the digitisation of the world is ensuring that transparency of state will be present whether organisations like it or not. AI will only seek to exacerbate the necessity to be proactive rather than on the (penalty afflicted, margin impacting) back foot.

This paper seeks to set the basis for a transformation journey that will lever existing investment, draw out new patterns of information and knowledge and provide value and resilience to customers implementing it. Key to this is demonstrating to all stakeholders clear, consistent and continuing value at every stage of the way.

Not only that but the tenets of the roadmap laid out here will provide benefits across the realms of ITSM, ITOM, ITAM, Business Workflows and many more areas.

It provides the basis for future acceleration, agility and growth whilst simultaneously delivering better governance, risk, compliance and security.

As for how this is achieved in an agile, early value, low risk, standards aligned, cost effective way, Synechron would love to have a conversation on exactly this subject and how we've done it before and brought benefits to customers just like you.

"The end is where we start from."

Synechron

Capture your future faster.

Synechron is an elite ServiceNow partner, experienced in delivering major transformations at scale for clients operating in complex and highly regulated environments - all delivered by our world-class team.

- Transform at scale
- Engineer expertly
- Build in resilience
- Accelerate with AI

servicenow
PREMIER
Partner
Consulting & Implementation

Richard Taylor

Head of Resilience, Synechron | ServiceNow

Richard is a highly experienced ServiceNow veteran and well known in GRC/IRM circles. He has a real passion for embedding resilience early and effectively into the heart of every organisation.

Contact us:

Synechron Limited, 95 Gresham Street,
London - EC2V 7NA, United Kingdom

servicenow@synechron.com