


# **HARNESSING SERVICENOW TO ENHANCE DIGITAL RESILIENCY**

In this eBook, we discuss how organisations can enhance their digital resiliency efforts by unlocking value and harnessing ServiceNow to its full potential.



We are operating in unprecedented times where organisations are facing a complex set of challenges. Organisations are having to invest significant time, effort and money to manage:

- the growing digital risk and requirements to improve security postures
- the rising costs to remain compliant
- the increasing rate of change and transformation
- a heavier reliance on external vendors and partners
- the disconnection between people, processes, technology and line of business functions
- shadow IT
- the technical complexity driving poor user experience

With these challenges likely to increase beyond where we are today, there has never been a more critical time to embed strong foundations to be able to respond to these issues from an informed position. One way organisations are enhancing their digital resiliency is by investing heavily into the ServiceNow Platform.

In this eBook, we discuss how organisations can enhance their digital resiliency efforts by unlocking value and harnessing ServiceNow to its full potential.

## WHERE DO WE START? FOUNDATION DATA

---

The ServiceNow Platform maintains a core foundational data model that extends across all capabilities. The importance of laying a strong foundation cannot be underestimated, and AC3's Senior Business Analyst, Diana Gaskin, has detailed key details in another article that talks through the steps to get foundation data elements right. You can read the article [here](#).

When we talk about foundation data in the context of ServiceNow, we are focusing on key organisational information that is leveraged across the ServiceNow Platform – employees, teams, departments, cost centres, assignment groups, locations, reporting lines and manager details.

What is crucial to understand when establishing a strong base for foundation data, is that all capabilities in ServiceNow leverage these details in one way, shape or form. These pieces of information become pivotal elements that support driving maturity in ServiceNow capabilities and solutions that ultimately contribute to and underpin resilience efforts.

## AC3'S RECOMMENDATION

- Ensure integrated capabilities to ServiceNow that operate as a source of record, are managed, maintained and accurate.
- Ensure that as your business evolves, or changes, that foundation data is a key consideration when assessing impact.
- Where data is manually entered into ServiceNow from a foundation data perspective, ensure that it is someone's responsibility to keep this data maintained and accurate. Data Certification in ServiceNow can support this requirement with task-based workflows established to validate data on a defined schedule.

# SERVICE ASSET & CONFIGURATION MANAGEMENT

What is often under-appreciated in the context of ServiceNow is how important a robust and trusted Configuration Management Dataset is to digital resilience efforts, and the importance of effective Asset Lifecycle Management. In AC3's experience, maturity in the Configuration Management Database (CMDB), is often a tell-tail sign of the broader maturity of IT Service Management processes.

The CMDB in ServiceNow is the most critical capability in ServiceNow when considering the enhancement and maturity of digital resilience efforts. Without a mature CMDB dataset, investment in solutions that support risk mitigation, governance, operational stability, and user experience, will never truly hit the mark.

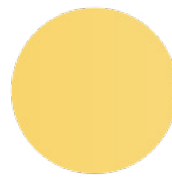
Over recent years, AC3 has delivered some significant transformations pertaining to the CMDB, and in most of these engagements, it has been a catalyst to support the next wave of delivery. It has been a pre-requisite to drive other outcomes.

So, why is the CMDB important to digital resilience efforts? Here's why:

- A trusted CMDB dataset allows for reporting on the broader technical environment. It enables granular insight to be obtained into where problems may lie, supports trend analysis, and also allows for the assessment of performance of delivery teams for the services or outcomes they are responsible for.
- The CMDB if established correctly, will map relationships between technical components. This allows for impact assessment for incidents, problems and changes to be assessed, and can facilitate notifications, approvals or communications based on impacted components in delivery.
- An accurate CMDB is a foundational element that can support automation efforts in ServiceNow. Whether this be through automated routing of incidents through 'Advanced Work Assignment', or

through the integration of monitoring capabilities like Datadog, Qualys, Splunk, Dynatrace, Azure Monitor, Akips, etc.

- An accurate CMDB supports impact assessment for Cyber Related incidents. In a time where cyber-attacks are prevalent, enabling the ability to assess and respond quickly is critical to protect the organisation and minimise impact. Recently one of our customers was able to assess the impact of the Log4J Cyber Security Vulnerabilities in the space of 4 hours due to our shared efforts in maturing the CMDB.
- The CMDB brings business context to technical data, through the mapping of technical components to Business Services.
- The CMDB is a pivotal reference point for Governance, Risk & Compliance capabilities in ServiceNow. Whether it be to support alignment of risks and issues to configuration items, or alignment of Business Continuity Plans to technical applications within the CMDB. The CMDB is often a key reference point to also meet compliance objectives.



## Why is Asset Lifecycle Management so important to digital resilience efforts?

Understanding the hardware and software assets deployed in your environment, enables you to make informed decisions on future investments, and also helps to manage the risk and security posture across your organisation. In times where the economy is on shaky ground, and organisations may be forced to make tough decisions pertaining to people, process and technology to better manage costs, it is imperative to know what you have deployed in the technical environment, who has custody of hardware assets, where assets are located, and who is consuming software licenses. This isn't just critical to help manage costs, but also to support the reclaiming of assets if employees are offboarded from your organisation.

For many organisations, the concept of lifecycle management doesn't exist. Spreadsheets still reign supreme, which is unfortunate, but it doesn't have to be this way. The concept of Asset Lifecycle Management is to ensure that from procurement to retirement, the asset is managed effectively within your IT Ecosystem.

ServiceNow can play a key role in supporting lifecycle management in your environment, and due to the existing solutions available, there are modules available to support the differing levels of maturity for your organisation.

Within the core IT Service Management suite, each customer has access to basic Asset Management capabilities. This allows organisations to integrate solutions like SCCM, InTune, SNOW Asset Management, or other COTS (Commercial off the Shelf) Products into ServiceNow. For those still operating from spreadsheets, ServiceNow also supports the ability to conduct data loads into the platform.

If you're operating from a higher level of maturity, the ITAM Products Hardware Asset Management (HAM) and Software Asset Management (SAM) which are licensed together or separately, may be a better fit to support evolution of your Asset Management Practices.

Improving digital resilience in IT Asset Management provides the transparency you didn't know you needed. It is an enabler for helping to make informed decisions on sweating assets when times are tough, it helps to provide clarity on volumes deployed across your environment, it reduces the investments you need to make due to being able to reclaim assets effectively, and also helps to understand the risk profile of your IT Assets.

- Leverage the ServiceNow ITOM Suite to maximise the accuracy and auto-map relationships between technical components.
- Assign a Configuration Management Process Owner. If the process is not managed, governed, and internal teams are not constantly reminded of why the CMDB is important, this will likely lead to the CMDB not being seen as a trusted and reliable data source. Leverage CMDB Health Dashboards to drive action to maintain the CMDB.
- Recognise that in a fast-paced environment where digital transformation is constant, that the CMDB requires ongoing maintenance. Ensure a support arrangement is in place with a ServiceNow Partner like AC3, to ensure the CMDB related solutions are continually optimised.
- Focus on populating the CMDB with technical components first, before proceeding to the mapping of business services. This will ensure the right context is obtained when looking bottom up, or top down in the context of a business service.
- Assign an IT Asset Manager to drive governance and process ownership of your IT real estate.
- Work to understand the importance of effective IT Asset lifecycle management as a key mechanism to help control IT spend. You will be surprised what you discover once all of your Assets are represented in ServiceNow.
- Integrate where possible to support Lifecycle Management. This will remove the need to manage your IT Asset Management processes manually. There are many pre-built integrations available for Asset Management systems of record.
- Understand what an employee has in the way of hardware and software, limits your risk when an employee moves to a new role, or is offboarded from the company.
- Hardware Assets Management in ServiceNow within the ITAM suite is best deployed on the back of an ITOM Discovery implementation with the IP Ranges and subnets already defined.
- To build further maturity if you implement Software Asset Management, leverage Client Software Distribution, which enables auto deployment of software from the Service Catalogue, post approval. This is a key mechanism to remove the human glue in delivery and leverages supporting platforms in place within your organisation.

## RECOMMENDATION

### AC3'S RECOMMENDATIONS

- Recognise the importance of the CMDB, and invest the right technologies, processes, and supporting teams to ensure the CMDB is managed and maintained.

## ITOM - EVENT MANAGEMENT & MONITORING

With a mature CMDB, the ability to build resilience in operations is imperative to not only moving to a proactive mode of operational delivery, but also improving operational stability. In times where resourcing costs are soaring, interest rates are on the rise, and cost of doing business continue to increase, harnessing smart technology solutions to help support robust and proactive delivery has never been more critical.

A mature CMDB in many respects is a pre-requisite to integrating monitoring solutions to ServiceNow to support the flow of alerts/events from monitoring toolsets based on pre-defined monitoring rules. The reason the CMDB is so pivotal, is that when alerts and events are generated from monitoring solutions, when they hit ServiceNow, ideally they will correlate to the existing configuration item (CI) in the CMDB. When an event or alert does not correlate to an existing CI, the event will only have context generated from the source system but will not be enriched by any supporting data from the CMDB. This does still occur on occasion when there is a mature CMDB dataset, and business rules can be established to create a CI record into the CMDB with the context provided from the source monitoring tool. At this point in time, review and analysis should be undertaken to either uplift the CI or understand why ITOM is not picking up the CI from scanning across the environment.

In the context of Event Management, digital resilience is improved when the mode of operational delivery moves towards proactive issue resolution before the business or external customers raise an incident due to service/performance degradation. It is a means to deflect calls to allow teams to focus on items that require attention, improves the overall stability of the technical environment, and improves the perception of IT who underpin business services.

## RECOMMENDATIONS

- Start with a single monitoring capability first to establish a repeatable process for onboarding new alert and event rules.
- Focus on critical alerts first which have the highest risk of impacting business services.
- Implement auto incident creation logic to remove manual touchpoints when certain alerts/incidents are known to cause impact. This will mobilise Major Incident Management Processes sooner.
- Leverage ServiceNow's Service Graph Connectors to increase the speed at which monitoring sources can be onboarded.
- Ensure Platform Teams have the required reporting and dashboards enabled to ensure real time visibility can be maintained to underpin delivery.
- Establish an ongoing operational process for fine-tuning event management rules as platforms mature and evolve.
- Continue to move further down the priority list (P1 > P2 > P3 > etc) as Event Management Processes mature.
- Activate Health Log Analytics to support prediction and prevention of outages. Leverage this capability to shorten mean-time-to-resolve by gaining insight and data-driven advice on how to fix an issue.
- Automate where you can support remediation efforts to remove the manual overhead on platform teams.

## GOVERNANCE, RISK & COMPLIANCE

The Integrated Risk Management (IRM) Suite of applications, or otherwise known as Governance, Risk and Compliance (GRC), is a suite of applications that help to support the effective management of risk and compliance for the organisation. It supports both internal and external needs, to support alignment to regulations, compliance frameworks, policies, and standards set both at an organisational level, industry level, or put in place by the government or regulatory bodies (I.e., APRA, ASIC).

When we consider GRC within an organisation and in the context of ServiceNow, we need to assess the challenges that face organisations today. We need to have a close affinity with these challenges to help guide investment into the right tooling to best support the organisational processes, and how we respond to these challenges.

The IRM suite of applications in ServiceNow, help to break down the siloes that exist in organisation and help to bring context to the risk and compliance posture. The IRM capabilities centralise activities that may have previously been captured in spreadsheets or disparate tooling. It is an enabler to bring a risk-based approach across the organisation which has never been more critical.

Applications	Descriptions
Risk Management	<ul style="list-style-type: none"> <li>Use Risk Management application to <b>continuously monitor</b>, to identify high-impact risks, <b>improve your risk-based decision-making</b>, and reduce reaction time effectively.</li> <li>The application also provides structured workflows for the management of risk assessments, risk indicators, and risk issues.</li> </ul>
Regulatory Change Management	<ul style="list-style-type: none"> <li>The Regulatory Change Management application enables customers to <b>check upcoming regulatory changes, assess their impact, and implement risk and compliance-related changes</b>, ensuring overall regulatory compliance.</li> </ul>
Policy and Compliance Management	<ul style="list-style-type: none"> <li>The Policy and Compliance Management product provides a <b>centralised process for creating and managing policies</b>, standards, and internal control procedures that are <b>cross-mapped to external regulations</b> and best practices. Additionally, the application provides structured workflows for the identification, assessment, and <b>continuous monitoring of control</b> activities.</li> </ul>
Audit Management	<ul style="list-style-type: none"> <li>The Audit Management application involves a set of activities related to planning audit engagements, <b>executing engagements, and reporting findings</b> to the audit committee and executive board. Actions from audits are then assigned to teams to remediate and action.</li> </ul>
Vendor Risk Management	<ul style="list-style-type: none"> <li>The Vendor Risk Management application provides a centralised process for <b>managing your vendor portfolio, assessing vendor risk</b> and tiering, and for completing the remediation life cycle.</li> </ul>
Business Continuity Management	<ul style="list-style-type: none"> <li>The Business Continuity Management (BCM) application gives your organisation the capability to <b>continue to deliver products and services</b> at an acceptable level <b>following a disruptive incident</b>.</li> <li>It allows for the definition and testing of Business Continuity and Disaster Recovery Plans to provide structure, and supports the organisation in a time of crisis.</li> </ul>

Now, when considering and implementing the broader IRM suite of applications, it can seem like a daunting task at first. AC3 see the most success within our customers when they execute an incremental maturity journey – Crawl, Walk, Run. An example approach to enabling the IRM suite is detailed below.



One of the most critical foundational elements for enabling the GRC capabilities in ServiceNow, is in defining the Entity structure. Entities are people, places, objects, or things that need to be monitored in order to manage risks, track control compliance, or review as part of audit engagements. They are logical groupings that help to provide insight across all GRC capabilities deployed.

Entity Type	Example Entity	Entity Type	Example Entity
Business unit	Shared Services	Utilities	Air Conditioning
Department	Facilities	Business Applications	ServiceNow
Region	APAC	Services	Service Desk
Country	Australia	Suppliers	ServiceNow
Location	Sydney	Customers	Employees
Building	Head office	Processes	Desk Relocation

The entity design underpins the entire IRM suite and helps to provide granular insight through reporting to help focus efforts.

The IRM suite enables organisations to subscribe and integrate to the Unified Compliance Framework (UCF), to allow organisations to ingest controls and authority documents aligned to compliance frameworks into their instance of ServiceNow that are relevant to them. I.e., ISO9001, ISO27001. The integration leverages the Common Controls Hub and reduces time in populating ServiceNow, assists in extracting value from the Policy & Compliance capabilities, and enables the Audit Management capabilities to aid in assessing compliance against deployed frameworks.

## RECOMMENDATION AC3'S RECOMMENDATIONS

- Invest a lot of time in defining the right Entity Design structure to underpin the IRM portfolio of applications. This maps out the structure of activities, services and functions performed across the organisation to bring context to GRC activities.
- Start small and iterate. Crawl, Walk, Run. We recommend spending time to nail the entity design, and then loading your risk register(s) into ServiceNow as a start.
- Leverage the CMDB where possible to enrich the GRC applications with broader context and to aid in impact assessment.
- Integrate to the Common Controls Hub via the Unified Compliance Framework. Identify 1-2 compliance frameworks to commence mapping the most critical elements for your organisation.
- Invest in ongoing training and education to support GRC activities, as these processes continue to gain traction and buy in across the organisation.
- If your organisation is starting from a low level of maturity or moving away from spreadsheets, adopt the lowest tier of licensing and start there. You can always uplift licensing to activate more products when your organisation is ready to take the next step in the maturity curve.

## SECURITY OPERATIONS

In a time where digital innovation and technology evolution continues to move forward at light speed, it is becoming increasingly necessary for organisations to improve their cyber resilience and security posture. As organisations continue to invest in technology to improve ways of working and drive efficiencies, platforms like ServiceNow, are helping to connect a complex ecosystem of cyber security toolsets to support effective management of vulnerabilities and security incidents.

The two most prevalent capabilities in ServiceNow that are seeing increasing adoption in the market, are the Vulnerability Response & Security Incident Response Applications. These capabilities integrate with a variety of enterprise capabilities (Qualys, Tenable, Rapid7, etc) to help track, manage, respond and remediate vulnerabilities and cyber security incidents within pre-defined workflows within ServiceNow.

The Cyber Security capabilities in ServiceNow have a heavy reliance on a mature CMDB to help enrich and provide context to vulnerabilities and cyber incidents, helping to drive improved context and mean-time-to-resolve. For one of AC3's ServiceNow customers, when the Log4J vulnerability was detected in December 2021, the customer was able to assess the scale and impact within 4 hours, at 96% accuracy. As this scenario played out, as a whole it provided a great deal of confidence and validation for the investment in maturing and maintaining a robust CMDB, due to how beneficial it was to assess risk and impact of the vulnerability. A true sign of how ServiceNow was at the centre of helping to maintain and underpin digital resilience.

Some of the key benefits of bringing in delivery components associated with Cyber Security into ServiceNow within the Security Operations suite, is the ease in which delivery teams can be engaged to participate in remediation and the associated reporting that helps to govern the underlying processes. The capabilities help to break down siloes and when coupled with core ITSM and GRC capabilities, helps to provide a holistic view of risks, issues, security posture, associated impacts and performance pertaining to Cyber Security.

## RECOMMENDATIONS

- Ensure a mature CMDB dataset is in place before investing in Security Operations.
- Integrate the security stack where possible and where it makes sense, to help provide a consolidated view across the technology ecosystem for Cyber Security.
- Integrate process capabilities on-platform to help provide more holistic reporting through related lists and to aid in broader transparency across the cyber technology stack.
- Support Cyber Security Processes with seamless integration at a process level
- between Major Incident Management, Incident Management, Security Operations, and Change Management. The tooling will guide how a process works, but there are people related elements and hand-offs that require definition.
- Be prepared for a significant volume of vulnerabilities to be identified upon enablement of the Vulnerability Response application.
- Define a plan prior to launch, for what will be treated and in what order.
- Ensure platform teams and process personnel outside of Cyber Security are taken on the journey to compliment the solutions being

## SUMMARY

In summary, it is evident that ServiceNow can play a pivotal role in underpinning the digital resilience efforts of an organisation through a broad set of capabilities. As organisations continue to implement strategies to improve their risk and security posture, a broader conversation on the capabilities that can help underpin this vision is critical. An uplift in maturity across service operations, governance risk and compliance, and cyber security, is necessary to help deliver on the holistic outcome. Each capability compliments one another, and there are dependencies and relationships across the platform that can be leveraged in unison to provide a more holistic and reliable outcome.