fusion
GLOBAL BUSINESS SOLUTIONS

Fast Tracking COBIT 5 for Information Security and Auditing

White paper written by
Keyvan Shirnia: Chief Strategy Officer
Christina Kidd: Technology Evangelist

At Fusion Global Business Solutions, we help companies gain measurable business outcomes from their investments in Digital Services and Operations Management.

In this paper, we discuss how any organisation can achieve higher levels of information security maturity by focusing on Asset and Configuration Management. Our conversations and experiences with our partners indicate that deploying logical use cases for Asset and Configuration Management not only promotes information security holistically, but aligns you with compliance standards and frameworks.

Table of Contents

Information security: critical, yet challenging

Information security is a critical part of any business today. Without the right InfoSec protocols, you risk exposing your company to data breaches that can wreak havoc on your business and employees. It's not hard to imagine: infrastructure failures, disclosure of confidential financial information, network intrusions, intelligence and personnel leaks, and even espionage.

Of course, non-secure information can also result in major incidents, downtime, failed industry audits, and non-compliance with mandated governance such as the General Data Protection Regulation (GDPR) or Payment Card Industry Security Standards Council (PCI).

At Fusion, we specialize in helping companies gain measurable business outcomes from their investments in IT Service Management and operations. Drawing on our InfoSec experience, this whitepaper will provide:

- The most appropriate prescriptive framework to quantify and solve the gaps in your information security, by identifying and resolving capability gaps, improving the quality of asset data, and, most importantly, maturing the asset management governance and processes
- A "case study in brief", describing our recent partnership with a global brand who needed speedy InfoSec solutions
- A set of Fusion Pro-Tips to enhance your InfoSec journey.

The Importance of InfoSec

Digital transformation is effecting change in every part of your company. Two transformative areas stand out, for both their enormous potential and their enormous challenges: the exponential potential of cloud services, including sophisticated architecture like serverless applications and microservices, and the proliferation of connected devices and the Internet of Things (IoT). These major developments are key drivers of complexity, and the more complex your systems, the more significantly your risk level increases.

Information security often feels like checking the boxes of audits and compliance. But those are only outcomes of good information security. InfoSec is critical once it comes to reducing your risk in increasingly complex environments. InfoSec is a requirement for successful digital transformation. Without proper InfoSec, you cannot connect services for a zero-friction supply chain and you cannot move your services closer to your customers—both of which are agility requirements for successful businesses today. Delaying InfoSec improvements guarantees that your complexity, and hence risk, will become increasingly challenging.

The Challenge with InfoSec

InfoSec is comprehensive. It applies to every single part of your business. In an ideal world, everything your company owns would be visible, allowing you to secure each piece appropriately and continuously, minimizing risk by improving control.

However, as companies migrate data and workflows to the hybrid cloud, the visibility and control required by information security become more challenging to accomplish. IT must navigate various hardware, software, and third parties across the business supply chains in the attempt to protect and secure their information. Every asset must be tracked for security and value optimization.

Companies struggle to gain this visibility, even at the most elementary levels, because current tools, processes, and organisational structures are unable to cope with the increased threat of attacks. Companies defer to IT frameworks as a path towards governance and risk mitigation, but a variety of IT enterprise and InfoSec frameworks offer ways to achieve information security. Which one is best? We'll explore the most appropriate framework in the next section.

Case Study in Brief
Part 1

Last year, a global retailer contacted Fusion for help with its information security. The company operates 400+ stores worldwide and has revenues in excess of $4 billion USD per year. Despite this success, the Chief Information Security Officer, who reports to the Board of Directors, carried out an internal audit that highlighted multiple challenges:

- A limited view of their assets
- A siloed and incomplete set of asset management processes
- Limited ability to prevent, detect, and recover from security-related incidents
- Limited ability to report against the industry InfoSec standards, including PCI/DSS and GDPR, despite previous compliance
- Slow response time to InfoSec-related events.

This was a common prospect for us: how to get the retailer to understand their assets and proactively manage the asset lifecycles. With this control, the retailer could then deploy a set of information security controls and governance that would minimize risk and achieve their primary objective of full compliance with GDPR and PCI. Without this control, the risk is enormous—and each day that passed without the delivery of a solution would see the risk level increase. The company could inadvertently leak personal or proprietary data, resulting in reputation loss. They could unintentionally enable intrusions into financial networks. And in trying to remedy these situations, they could spend significant amounts on unplanned costs.

More from our global retail partner case study in the next chapter!

FUSION TIPS:

Prioritize and narrow your focus. Avoid the mistake of managing every single asser perfectly from the outset. Instead, start with your top priority: your #1 problem becomes your use case.

Building Blocks for InfoSec Success:
Asset Management & Configuration Management

All security standards require assessing and understanding your assets and configuration. These frameworks aim to help companies answer two fundamental questions:

- What IT assets does your company use?
- What processes control these assets?

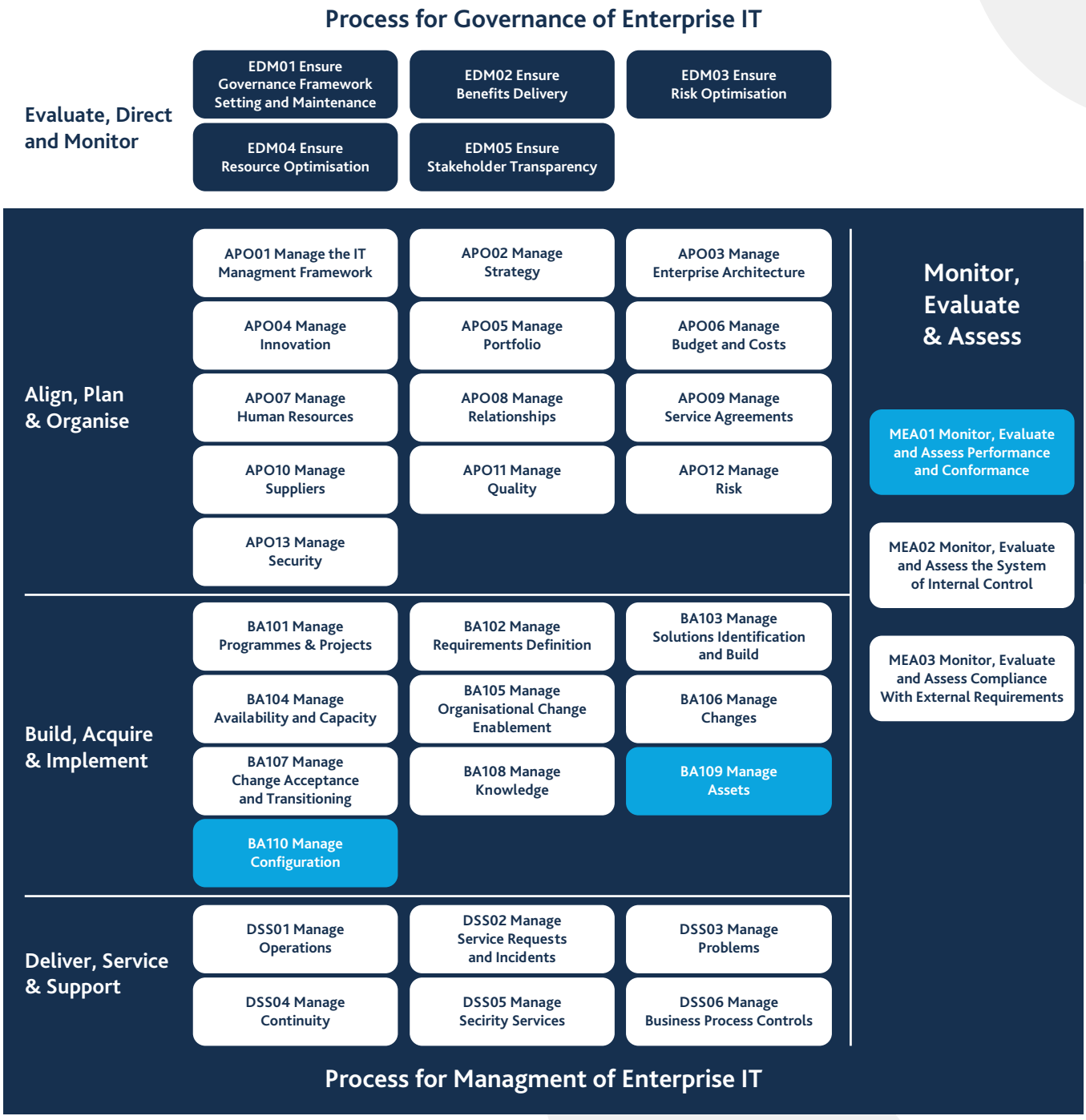
With this understanding, frameworks can guide your company towards a holistic IT asset management process that can secure your information. In our experience, the long-standing framework COBIT 5, most commonly used by auditors, provides the baseline for the vast majority of security standards frameworks (such as the ISO/IEC 27000 suite of information security management standards).

Understanding COBIT 5

Many companies already use the COBIT 5 framework for IT enterprise governance, either selectively or entirely. For companies with a mature IT configuration process, COBIT 5 can help define the requirements for a single source of truth for all IT assets. This is essential to InfoSec—and to the asset management processes governing the asset lifecycle, ownership, costs, and security controls.

COBIT 5 spans 37 control objectives within five domains:

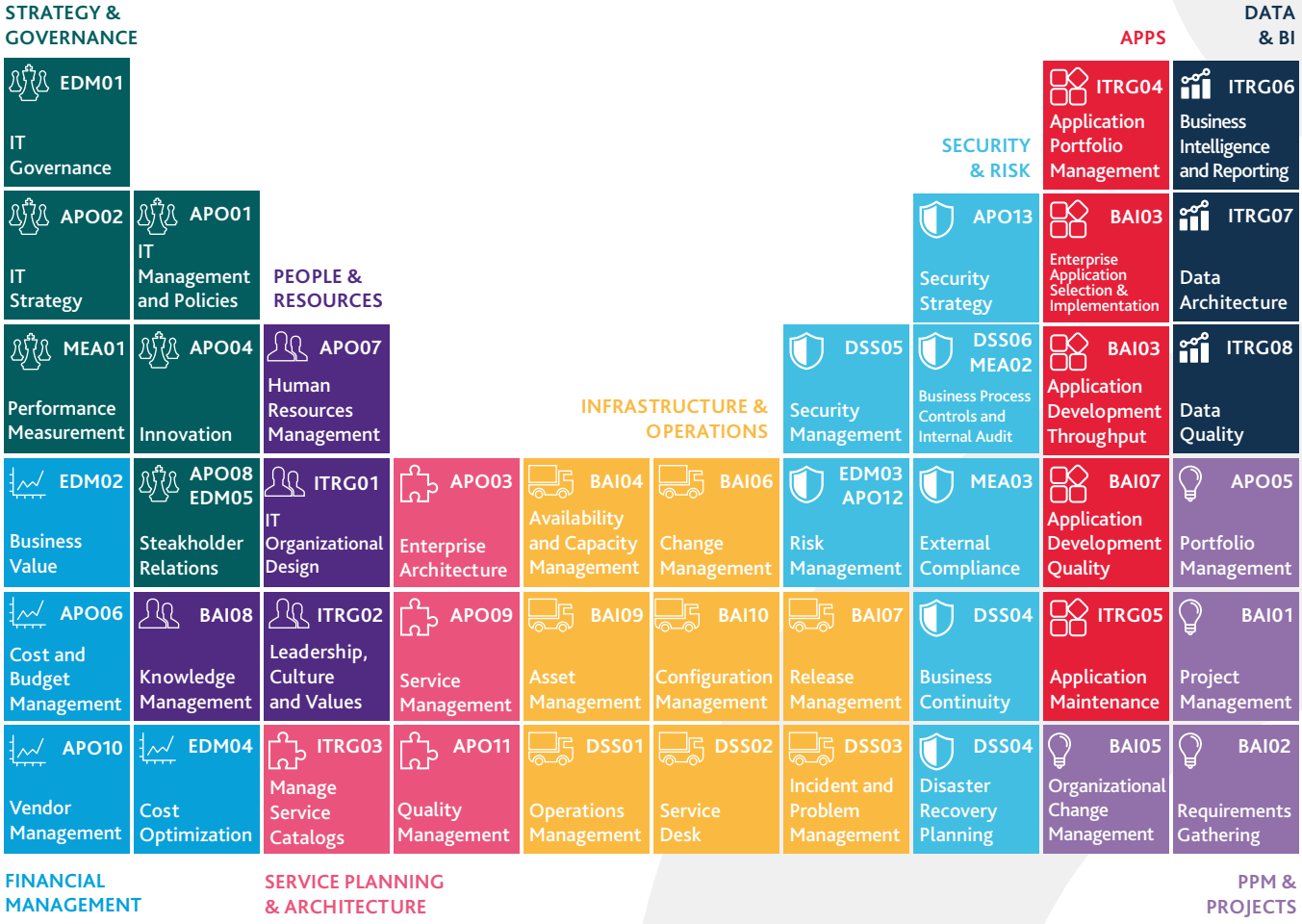
- Governance of Enterprise IT
  - Evaluate, Direct and Monitor (EDM) - 5 processes
- Management of Enterprise IT
  - Align, Plan and Organise (APO) - 13 processes
  - Build, Acquire and Implement (BAI) - 10 processes
  - Deliver, Service and Support (DSS) - 6 processes
  - Monitor, Evaluate and Assess (MEA) - 3 processes



Asset and Configuration Management comprise the core of COBIT 5. Therefore, we'll focus on its Build, Acquire and Implement (BAI) domain. BAI establishes how to identify, acquire and implement IT requirements and technology within your company's current business processes. Importantly, Manage Assets (control process BAI09) and Manage Configuration (BAI10) provide underlying IT asset information, that is then either directly or indirectly consumed by all other COBIT 5 processes.

This diagram visualizes the central roles of Asset Management and Configuration Management in COBIT 5. The closer a process is to this core, the more that process will rely on Asset and Configuration Management.

IT Management & Governance Framework



Asset Management

Asset Management is the strategy of procedures and actions, all documented and communicated to stakeholders, that track and configure your myriad assets. Assets comprise any hardware, software, information, or other items your company uses to conduct business. All assets have financial and strategic value to the enterprise.

The goal is clear: proper accounting of assets means you can begin to secure and protect those assets (the primary goal of InfoSec) and then optimize the value each asset provides. Asset Management involves a variety of activities and procedures throughout asset lifecycles: accurate planning, procurement, protection, maintenance, upgrading, replacement, and retirement and disposal.

To achieve these Asset Management capabilities, COBIT 5 defines five critical tasks:

1. Identifying and recording current assets
2. Managing critical assets
3. Managing the asset lifecycle
4. Optimizing asset costs
5. Managing licenses

Configuration Management

COBIT 5 defines Configuration Management as the process of providing sufficient information about service assets to enable the management of the service, the handling of service incidents, and the assessment of service changes' impact. By providing accurate configuration information, IT service management can efficiently and effectively support other processes, including InfoSec.

Configuration Management involves a variety of activities such as identifying, recording, controlling, reporting, auditing, and verifying service assets and configuration items (CIs). These assets and CIs could include baselines, versions, constituent components and attributes, and relationships.

COBIT 5 identifies five tasks for building a mature configuration management process:

1. Establish and maintain a configuration model
2. Establish and maintain a configuration repository and baseline
3. Maintain and control configuration items
4. Produce status and configuration reports
5. Verify and review integrity of the configuration repository

Let's explore how the asset and configuration management processes come to life.

Case Study in Brief, Part 2

After understanding our partner's challenges, we implemented the first step: providing the data and processes required to support InfoSec outcomes. Having chosen a very narrow use case—addressing the InfoSec internal audit requirements—we needed to achieve and show control over our assets. In doing so, our partner would also pass their audits, which are indicators of successful and controlled asset management.

This was particularly challenging. Their InfoSec use case required a large dataset that spanned all assets (data centre, AWS and Azure clouds, desktops, mobile devices, and software), held in one central repository, per BAI10.

This highlighted many questions:

1. What specific outcomes must I achieve in order to pass security audits?
2. What data does InfoSec reporting require?
3. What is the quality of the required data? How much information is required for each asset? How often must this data be refreshed? How accurate must the data be to achieve control?
4. Where and how is the data obtained and maintained?
5. How do I combine various data sources to gain complete lifecycle visibility into every asset?

FUSION TIPS:

Define who manages and maintains each asset. security standards require that all assets have an owner. without ownership, an asset cannot be managed and maintained effectively. Asset ownership provides additional governance by aligning it with business spending.

We answered these questions through a series of workshops with our partner. Then we delivered the first solution: an outcomes-based service that aligns with data quality targets set by the InfoSec audit team. The goal of this service is to operate the solution and continuously deploy improvements in data quality. This is complicated by having a combination of data that is discoverable, such as a service, and non-discoverable data, such as who owns that server.

Our resulting service provided InfoSec with three sets of capabilities:

- **A comprehensive, end-to-end Asset Management process (BAI09) that:**
  - Defines our partner's unique end-to-end IT Asset Management (comprising 150+ steps), based on a detailed gap-analysis study
  - Spans all servers, including on-premise and cloud, networks, software, and mobile devices
- **A Configuration Management process (BAI10) that:**
  - Provides a single source of truth for all assets stored in the new CMDB
  - Discovers all hardware and software assets in data centers, including on AWS and Microsoft Azure
  - Integrates hardware across desktop, laptop, and mobile with CMDB software inventory
- **Exploitation & Data Quality Management that:**
  - Provides a continuous data quality improvement programme that complies with data SLAs and Key Performance Indicators
  - Establishes a daily management discipline to proactively explore for bad data and provide remediation plans
  - Delivers business outcomes aligned with the company's use case and our Managed Service Operations

Our global retailer had their first real solutions, but they hadn't accomplished their use case goals yet.

Outcomes and Benefits:
Managing and Maturing Data Quality

Because asset and configuration data underpin every COBIT 5 control objective, data quality is essential. Without accurate, high-quality data, all effort spent on InfoSec and other consuming use cases becomes pointless. Unfortunately, managing and improving data quality is the most difficult part of your InfoSec journey. Enterprises will inevitability run into hard-to-answer questions about who owns what data, where the boundaries lie, how to determine whether data is wrong—and how to rectify it when it is.

Companies often approach data governance with a bottom-up perspective, hoping to ensure all data is good quality. This is the wrong approach for two reasons.

First, the nature of data required for InfoSec reporting is different from the data that is needed for other use cases, such as cloud migration or change management. Second, from a more holistic perspective, correcting all enterprise data without a proper focus is impossible. You can't grasp something that is constantly changing and growing. (Companies who try this get stuck on a years-long plan with no short-term solutions or outcomes.) With exponential data growth, you will fail to ensure quality on any data subset unless you have one specific goal (use case) per iteration. When data quality suffers, it affects all business units, and your employees and customers will begin to question the data.

Our experience underscores the top-down approach. By choosing a single use case (outcome) per iteration, you'll harness speed and agility for significant, quick-to-implement solutions. This approach offers a number of benefits:

- The dataset and related data quality SLAs are confined within a smaller, more manageable scope
- One use case provides actionable information quickly and full solutions in mere months. These short-cycle iterations can then be showcased for wider business approval to increased adoption
- As you move onto additional use cases, your data quality improves iteratively
- Short cycles that provide use case solutions and data quality maturation means the data becomes more and more trustworthy.

Assessing and Improving Data Quality

Fusion has developed these five key principles for assessing and improving data quality within Asset and Configuration Management:

Case Study in Brief, Part 3

Once we established the first use case (passing the internal InfoSec audit) and narrowed down the necessary processes and data necessary, we moved onto improving the data quality.

Our goal for every company is to achieve valuable business outcomes. Within only four months of implementing DEaaS, our global retail partner:

- Passed an internal information security audit
- Developed a comprehensive asset management process incorporating software, network, servers, and end-user computing
- Achieved 95% asset discovery across data centre, cloud, and end-user computing as part of Configuration Management
- Established central repository (CMDB) for all IT assets, which refreshes every 24 hours
- Integrated their service desk with the CMDB to improve incident handling and change the management decision-making process using the most up-to-date information.

Our global retail partner could stop here—they've got the tools and processes to achieve their first goal. But they'd be missing the best part!

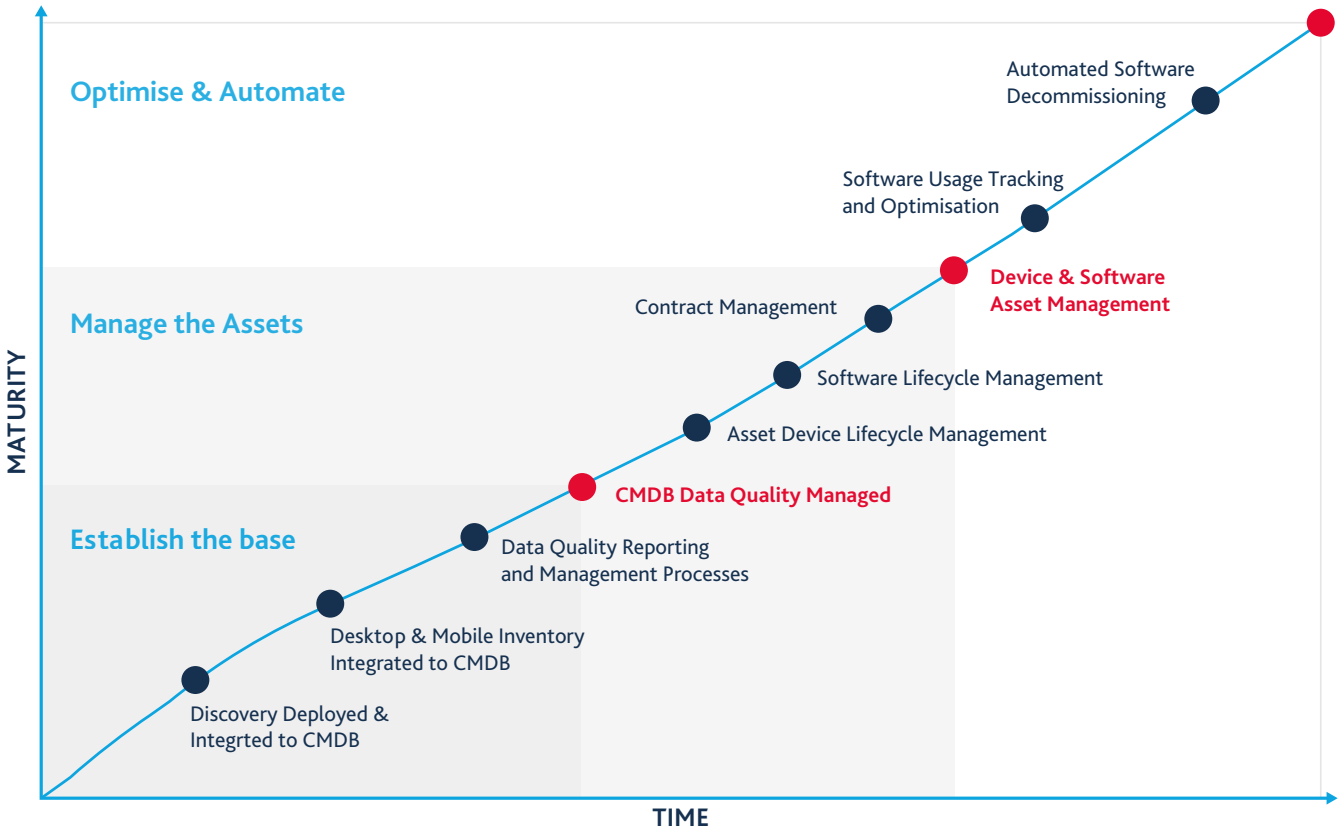
FUSION TIPS:

Data quality management must be a continuous effort to eradicate bad data. Good governance means that data quality is integral to all data-consuming processes.

Outcomes and Benefits:
Maturing Your Asset Management Process

At Fusion, we don't apply a standard InfoSec approach. Instead, we prioritize the current state of your processes and data quality, then compare it to the desired state—your InfoSec outcomes. This difference helps us establish the plan for moving you away from chaos and towards a more defined, proactive, and even strategic process.

This top-down, agile approach offers many benefits, but the most unique and long-lasting may be how the asset and configuration management processes continue to mature as you iterate on several use cases. This matures and improves data quality across all use cases.



Phases of the Model

Three distinct phases on the journey to asset maturity

1. **Establish the Base** focuses on inventory visibility of assets though data quality and full estate coverage
2. **Manage the Assets** Mature the processes, organisation and tools usage to manage the assets through their lifecycle
3. **Optimise and Automate** Optimise the asset usage and costs. Automate the lifecycle state changes and maintenance

The Future of Asset Management

Maturing asset management makes it clear that you must become more scientific and data-driven in order to become proactive. Machine learning, data science, and AI capabilities will play significant roles, moving your company from a reactive InfoSec position to a proactive one. You will transition from being hunted by threats to proactively hunting for potential areas of vulnerability across your estate and remediating before an attack occurs.

Case Study in Brief, Part 4

Our global retail partner now had the right asset and configuration processes in place and a method for maturing the processes and the quality of inherent data. Maturing your asset management process becomes part of your ongoing InfoSec work—but the right tools can ensure that it isn't overwhelming.

Our Discovery Exploitation as a Service (DEaaS) continues to operate the following services for our global retail partner:

- Managing the DEaaS platform daily
- Exploiting data and providing bespoke reports
- Continuously monitoring data quality against comprehensive SLAs to identify and remediate poor-quality data
- Upskilling and training the company's IT staff.

With the data and processes in place, the InfoSec team now focus their activities on using the trusted data to assist the following outcomes:

- Verifying impact and assessing risk of proposed service changes
- Comparing various lines of enterprise network defence for blind spots (unknown unknowns)
- Tracking CIs against approved secure configuration baselines, which helps identify unauthorized breaches
- Investigating potentially harmful modifications of configurations (especially helpful when understanding what created a vulnerability)
- Controlling versions and authorizing production of hardware and software components, which helps prevent vulnerable systems being released into production.

What's next? Our unique, iterative, outcomes-based approach enabled our global partner to complete this first use case (the internal information security audit) by obtaining and deploying actionable solutions. Because their asset and configuration management processes are now functioning properly, this next use case will take no more than three months to complete, which is much faster than a bottom-up approach. Our partner will continue to iterate using these fundamental tips and processes.

FUSION TIPS:

Showcase your achievements. Our speedy, agile outcomes-based approach means you'll have solutions in mere months. Show and tell these solutions to get more buy-in and to continue your InfoSec journey.

Next Steps

Approaching Asset and Configuration Management per COBIT 5 is just the beginning of your information security journey. Some companies are handling information security selectively, but most companies resemble our global retail partner from the case study. They need guidance and they need it quickly.

To accelerate delivery on your information security, partner with Fusion Global Business Solutions to deploy Discovery Exploitation as a Service (DEaaS) and revolutionize your asset and configuration management. DEaaS can be used to solve InfoSec as well as a variety of other use cases thanks to our unique approach:

- Agile, top-down methodology which focuses on business outcomes that deliver the right data at the right time for your prioritized use cases
- Each use case iteration takes no more than four months
- Each iteration offers deeper asset understanding, improved asset coverage, and asset management maturity
- The iterative approach continuously improves data quality.

Deploying DEaaS means your information will be significantly more secure in less than four months.

FUSION TIPS:

InfoSec is iterative and continuous: you can't do everything in one go. Start small and iterate frequently. Each iteration is quicker, more accurate, and smarter, ensuring ongoing InfoSec success.

fusion
GLOBAL BUSINESS SOLUTIONS

Contact:

www.fusiongbs.com

London: +44 208 814 4888
New York: +1 844 456 1342
Madrid: +34 91 790 1106

Enquiries@fusiongbs.com

Resources:

- What is information Security? (Cisco)
- COBIT 5 created by ISACA
- COBIT 5 Periodic table (InfoTech Research group)
- ISO/IEC 27001 Information Security management