COSAC 2024

Rob Campbell

SESSION 2S

BUILDING CLOUD ARCHITECTURES TOP-DOWN: ALIGNING WITH BUSINESS MOTIVATIONS

COSAC

table of contents

Building Cloud Architectures Top-Down: Aligning with Business Motivations

While major cloud providers offer comprehensive reference architectures for implementing functional technical structures such as landing zones, these models often need more direct alignment with core business motivations. This misalignment frequently results in architectures developed from the bottom up, focusing on technical specifications rather than strategic business outcomes.

The bottom-up approach can precisely meet technical requirements yet fails to deliver on security and operational efficiency due to poorly defined service management and the absence of an effective operating model.

I propose a different approach using a top-down, business-driven approach to cloud architecture. I will outline a method for using business motivations and objectives to drive cloud strategy and design, ensuring that the technical deployment of cloud environments inherently supports and enhances business goals.

Bottom Up

Misalignment Between Technical Implementation and Business Objectives

Many organisations face challenges where their cloud architecture does not fully support or align with their overarching business goals. This misalignment often results in inefficiencies, increased costs, and security vulnerabilities.

Technology functions need to re-evaluate their approach and;

- Consider cloud architecture design from a business perspective, ensuring that every technical decision is made with strategic objectives.
- Implement frameworks and methodologies that bridge the gap between business leaders and technical teams, fostering a shared understanding and vision.
- Develop effective service management practices and operating models tailored to the business, enhancing security, efficiency, and adaptability in cloud environments.

Why do Businesses Fail to achieve the promised benefits from cloud adoption

Inadequate Planning and Strategy

- Lack of Clear Objectives: Businesses often jump into cloud adoption without a well-defined strategy or clear objectives. It becomes challenging to measure success or realise specific benefits without understanding what they aim to achieve.
- Poor Alignment with Business Goals: Cloud initiatives sometimes need to align with overall business goals or needs, leading to investments in solutions that do not add value.

Underestimating the Complexity of Cloud Migration

- Incomplete Assessment of Current Infrastructure: Many organisations must fully assess their existing infrastructure, applications, and dependencies before migrating. This can lead to unanticipated challenges during migration, such as compatibility issues and unplanned downtime.
- Inadequate Skills and Resources: Cloud environments require different skills compared to traditional IT operations. Without adequately trained staff or the necessary resources, businesses struggle to manage and optimise their cloud environments.

Cost Management Challenges

- Uncontrolled Cloud Spending: The pay-as-you-go cloud services model can lead to unchecked spending if not carefully managed. Businesses often face cost overruns due to a lack of visibility and control over cloud resources.
- Overprovisioning and Inefficiency: Without proper monitoring and optimisation, businesses may overprovision resources, leading to unnecessary costs.

Why do Businesses Fail to achieve the promised benefits from cloud adoption

Security and Compliance Issues

- Inadequate Security Measures: Cloud environments require robust security practices, but some businesses need to implement them effectively. This can lead to vulnerabilities, data breaches, and compliance failures.
- Regulatory Compliance: Different industries have varying compliance requirements. Failing to address these adequately in a cloud environment can lead to legal and financial repercussions.

Lack of Cloud Governance

- Poorly Defined Roles and Responsibilities: Without clear governance structures, it is unclear who is responsible for managing different aspects of the cloud environment. This leads to inefficiencies and potential risks.
- Inconsistent Policies and Procedures: Inconsistent or poorly enforced policies around cloud usage can result in shadow IT, security vulnerabilities, and inefficiencies

Failure to Optimise and Innovate

- Static Use of Cloud Services: Some businesses lift and shift their existing infrastructure to the cloud without optimising for the new environment. This prevents them from taking advantage of the full range of cloud capabilities, such as automation and advanced analytics.
- Resistance to Change: Cultural resistance within the organisation can hinder the adoption of new processes and technologies essential to maximising cloud benefits.

Why do Businesses Fail to achieve the promised benefits from cloud adoption

Vendor Lock-In and Limited Flexibility

- Over-reliance on a Single Vendor: Depending too heavily on a single cloud provider can lead to vendor lock-in, limiting flexibility and increasing costs in the long term.
- Limited Multi-Cloud or Hybrid Strategies: Not adopting a multi-cloud or hybrid cloud strategy can prevent businesses from leveraging the best services across different providers, leading to suboptimal performance or higher costs.

Inadequate Monitoring and Management

- Lack of Continuous Monitoring: With continuous monitoring and management, businesses may take advantage of opportunities to optimise performance, improve security, and reduce costs.
- Reactive Rather than Proactive Management: A reactive approach to cloud management often leads to missed opportunities for optimisation and can exacerbate issues when they arise.

Integration Challenges

- Difficulty Integrating with On-Premises Systems: Integrating cloud services with existing on-premises systems can be complex and may not deliver the seamless operation businesses expect.
- Inconsistent Data Management: Managing data across multiple environments (cloud and on-premises) without a consistent strategy can lead to data silos, governance challenges, and inefficiencies.

Why do Businesses Fail to achieve the promised benefits from cloud adoption

Misalignment of Expectations

- Overestimating Immediate Benefits: Businesses often expect immediate cost savings and performance improvements, but these benefits may take time to realise, especially if the transition needs to be carefully managed.
- Underestimating the Effort Required for Change Management: The transition to the cloud often requires significant organisational change, which can be overstated. With proper change management, the transition can be smooth rather than beneficial.

Using the analogy of modern automotive design the aspiration for cloud is:

- Precisely Engineered: Just as a modern vehicle is designed to function seamlessly through an integrated network of systems, the cloud service is crafted to operate efficiently within a cohesive ecosystem of interoperable services.
- Component Reusability: Like the shared components in vehicle manufacturing that drive both performance and cost efficiency, the cloud architecture is optimised for the reuse of common components, reducing redundancy and enhancing agility.
- User-Centric Design: As vehicles are tailored with the driver and passenger experience at the forefront, the cloud service is designed with the end-user's needs in mind, ensuring intuitive and effective interaction.
- Cost-Efficiency: Comparable to the way vehicles are engineered for economical production and operation, the cloud service is developed to be cost-effective, both in terms of deployment and ongoing operational expenses.
- Robust Support Infrastructure: Similar to the comprehensive support and service networks that keep vehicles running smoothly, the cloud service is backed by a strong support framework and well-defined processes, ensuring reliability and ease of maintenance.

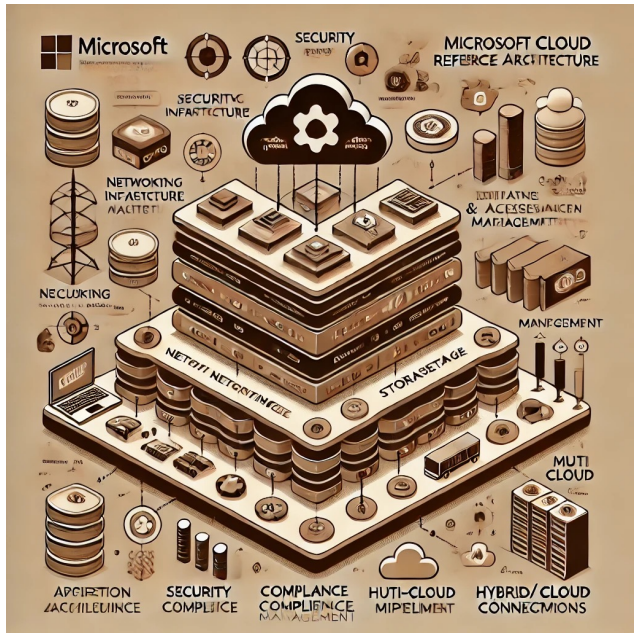
Why do Businesses Fail to achieve the promised benefits from cloud adoption

Conversely, when a cloud environment is developed without adequately aligning with business objectives, the result often reflects the opposite of a well-designed solution:

- Poorly Integrated Systems: Unlike a modern vehicle where systems work harmoniously, the cloud environment may become a collection of disjointed services that struggle to interoperate effectively, leading to inefficiencies and operational silos.
- Redundant and Inconsistent Components: Instead of optimising for reusability, components are often duplicated unnecessarily, leading to wasteful resource allocation, inconsistencies, and increased management complexity.
- Lack of User Focus: The design of the cloud service may overlook the end-user experience, resulting in a solution that is difficult to use, unintuitive, and fails to meet the needs of those it is intended to serve.
- High Costs and Inefficiencies: Without strategic planning, the cloud environment may incur excessive costs, both in initial setup and ongoing operations, due to a lack of cost-effective design and operational inefficiencies.
- Weak Support and Undefined Processes: The support structure may need to be developed, with clear or adequate processes, leading to difficulties in maintaining the environment, resolving issues, and ensuring consistent service delivery.

Using the MCRA as an example

An analysis of the Microsoft Cloud Reference Architecture (MCRA)



The Microsoft Cloud Reference Architecture is a comprehensive framework that provides best practices, design patterns, and implementation guidance for building and deploying cloud solutions on Microsoft Azure. This architecture is designed to help organisations create scalable, secure, and resilient cloud environments by leveraging a range of Azure services and technologies.

Business View (Contextual)

Defines business goals, objectives, and requirements, focusing on business context.

The Microsoft Cloud Reference Architecture touches on business drivers and strategies but primarily focuses on cloud services rather than in-depth business context. It aligns somewhat, but the focus is more on technology enablement than business strategy.

Architect’s View (Conceptual)

Translates business needs into a conceptual architecture, identifying key services.

Microsoft Cloud Reference Architecture aligns well here, providing a high-level overview of how cloud services can meet various business needs. It outlines key architectural principles and patterns relevant to cloud adoption.

Designer’s View (Logical)

Provides a logical design, mapping services and controls to business requirements.

The Microsoft Cloud Reference Architecture aligns strongly with this layer, offering detailed logical architecture components, such as security controls, identity management, and governance models.

Builder’s View (Physical)

Defines the physical architecture, including specific technologies and products.

Microsoft Cloud Reference Architecture is closely aligned with this layer, detailing specific Microsoft Azure services and configurations, including infrastructure, platforms, and security mechanisms.

Tradesman’s View (Component)

Focuses on implementation details, components, and configurations.

The Microsoft Cloud Reference Architecture provides significant detail at this level, offering guidance on deploying, configuring, and integrating Azure services, aligning well with the SABSA component layer.

Management (Operational)

Concerned with operational management and service delivery.

The Microsoft Cloud Reference Architecture includes operational best practices and management aspects, aligning well with SABSA's operational layer, particularly in monitoring, incident response, and compliance management.

Conclusions

Strong Alignment

The MCRA aligns strongly with the

- Designer's View (Logical),
- Builder's View (Physical),
- Tradesman's View (Component), and
- Service Management (Operational) layers.

These layers focus on the practical design and implementation of cloud services, which is the core strength of the MCRA.

Partial Alignment

The MCRA partially aligns with the

- Business View (Contextual) and
- Architect's View (Conceptual) layers.

While it addresses some business and conceptual aspects, its primary focus remains on technology and cloud service design rather than deep business strategy alignment.

Comparing the MCRA with POPIT

The POPIT Framework is a conceptual model that can enhance security architecture's alignment with business objectives by focusing on various dimensions beyond traditional technical concerns. Applying the POPIT framework to the Microsoft Cloud Reference Architecture (MCRA) can provide a deeper understanding of how well it aligns with broader enterprise needs, particularly regarding business value and security.

Aspect	Analysis
People	MCRA covers roles, governance, and training but lacks depth in change management and user adoption strategies, which are essential for aligning cloud architecture with business goals.
Organisation	MCRA effectively aligns IT and business strategies, ensuring cloud initiatives support the organisation’s broader objectives through readiness, strategy, and planning within the Cloud Adoption Framework (CAF).
Processes	MCRA’s guidance on operational frameworks like ITIL and DevOps ensures processes are optimised, supporting business-driven cloud objectives and preventing bottlenecks in the adoption journey.
Information Management	MCRA provides strong guidance on data governance, security, and compliance, ensuring information is managed as a strategic asset and protected according to business needs.
Technology	MCRA offers comprehensive guidance on technology selection, deployment, and management, with a strong focus on scalability, reliability, and security to support business growth and innovation.

The MCRA's Focus and the "What" vs. "How" Issue

MCRA's Strengths

Strategic Alignment:
MCRA excels in defining what needs to be done to align cloud adoption with business goals. It provides detailed guidance on key areas like governance, security, and technical architecture, ensuring that all necessary components are considered.

Comprehensive Coverage:
It covers a broad range of considerations, ensuring that each aspect of POPIT is addressed in terms of high-level requirements and best practices.

MCRA's Gaps

Implementation Depth:
MCRA can sometimes fall short in providing detailed, actionable steps on how to implement these strategies effectively. This is particularly evident in areas like change management, user adoption, and the practical integration of processes across the organisation.

Practical Guidance:
The gap often lies in translating these strategic objectives into operational reality for businesses. While MCRA tells organisations what they should focus on (e.g., aligning IT and business strategies), it may need to provide more detail on how to achieve this alignment in practice, particularly in complex, real-world environments..

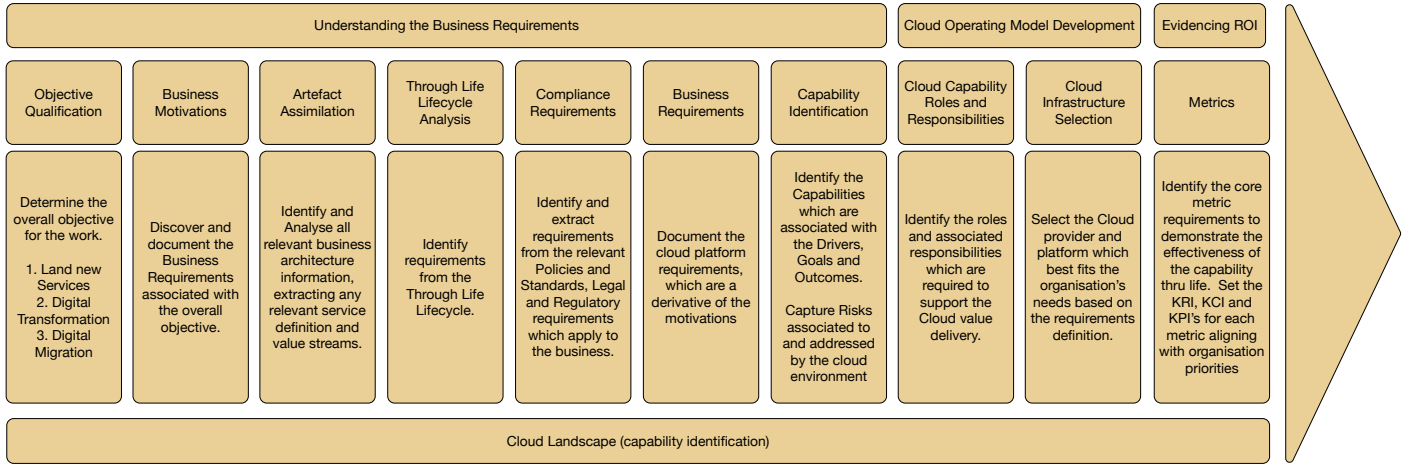
The MCRA's Focus and the "What" vs. "How" Issue

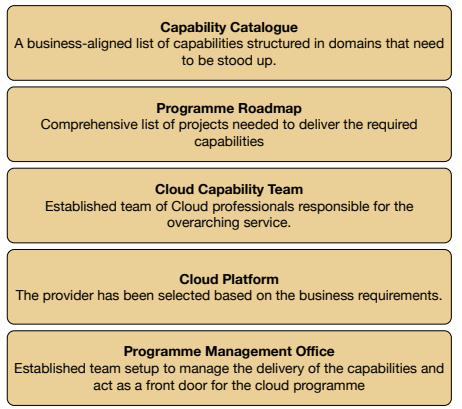
The MCRA does tend to focus more on the "what" than the "how" from a POPIT perspective. This can leave businesses with clear strategic goals but insufficient tactical guidance, leading to difficulties in effective implementation. For successful cloud adoption, businesses often need to complement MCRA with more detailed, practical frameworks or consulting services that focus on the operationalisation of these strategies, particularly in the areas of change management, process integration, and user adoption.

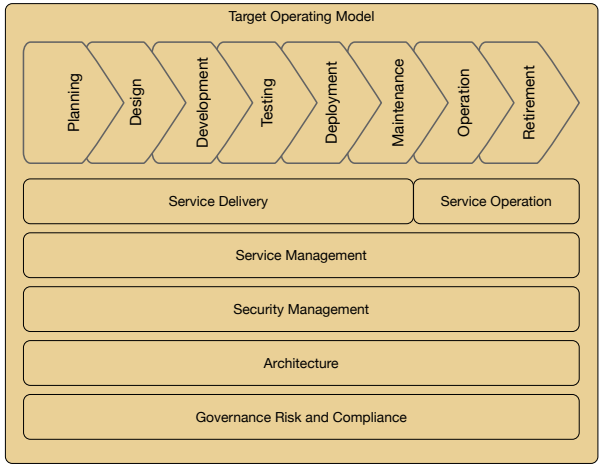
Aspect	Analysis
People	While MCRA identifies the need for role alignment and training, it doesn't always provide the detailed change management strategies necessary to drive user adoption and cultural change. Without these, businesses struggle to engage their workforce effectively, leading to resistance and suboptimal use of cloud technologies.
Organisation	MCRA aligns organisational needs with cloud objectives at a high level but may lack guidance on operationalising this alignment across different departments, especially in organisations with siloed structures.
Processes	Although MCRA supports frameworks like ITIL and DevOps, businesses often need more granular, step-by-step guidance on how to adapt these frameworks to their specific processes and workflows.
Information Management	MCRA is strong in outlining *what* information governance should look like but may not delve deeply into *how* to implement these governance frameworks in a way that balances control with agility, especially in rapidly changing environments.
Technology	The guidance on technology selection and management is robust in MCRA, but the "how" of integrating new technologies into existing infrastructures, particularly legacy systems, can be complex and is often underrepresented.

Stage 1 : Understanding the Business Requirements

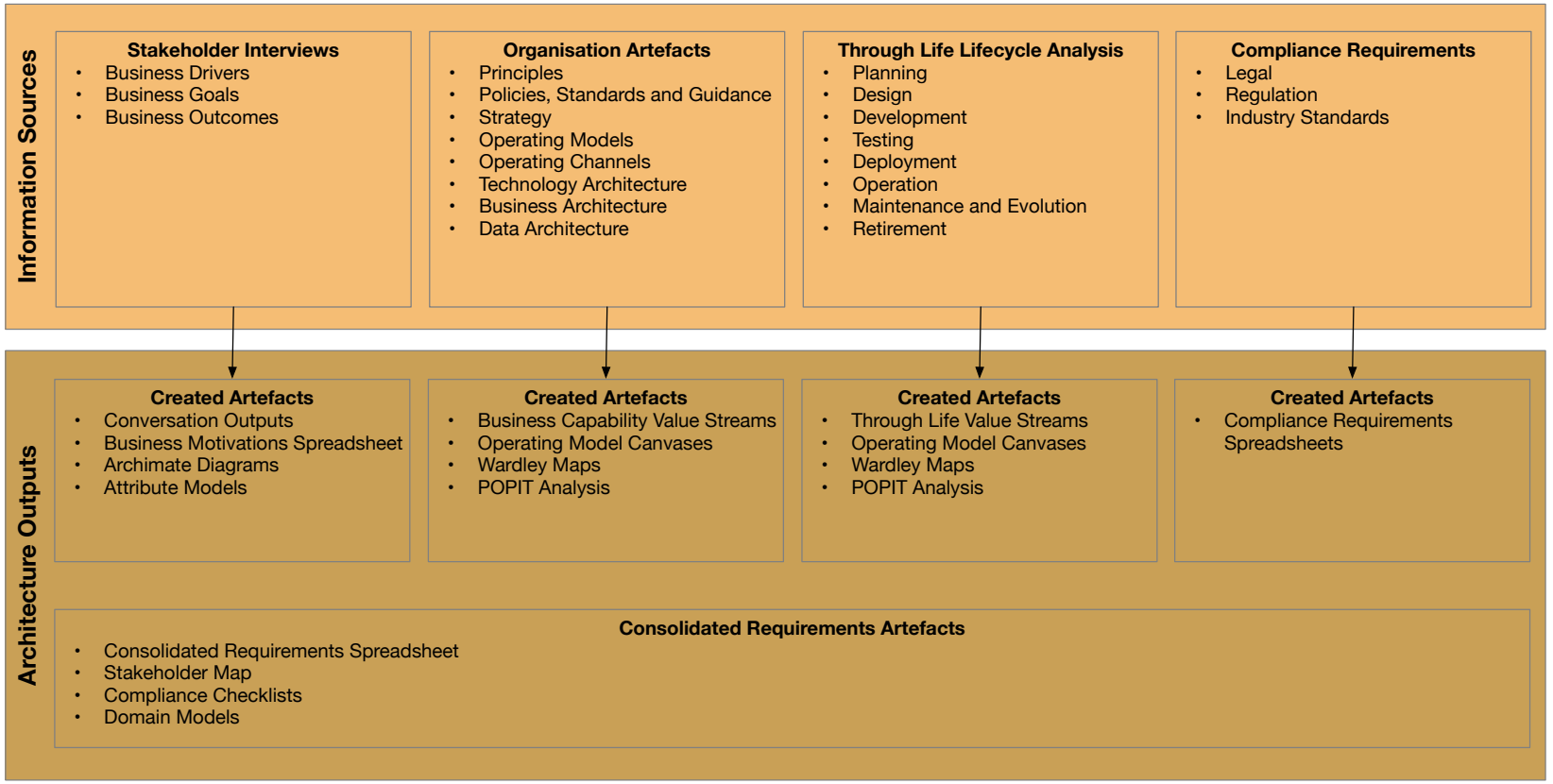
This is a critical initial phase in any organisational transformation or capability development initiative. This process involves deeply exploring the business's objectives, motivations, and the specific capabilities needed to achieve desired outcomes. By aligning these elements with the overall business strategy, we can ensure that initiatives, whether they involve cloud adoption, digital transformation, or other strategic goals, are effectively tailored to meet both current and future needs. This phase sets the foundation for a successful transformation by clearly defining the goals, identifying potential risks, and ensuring that all subsequent efforts are aligned with the organisation's core priorities.



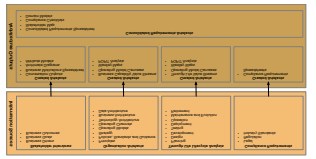




Sourcing Requirements



SABSA emphasises stakeholder interviews and attribute mapping to gather requirements; however, gaining access to these stakeholders can be difficult, and the scope and detail of the information collected often need enhancement to ensure a comprehensive requirements analysis.



Modelling Business Motivations to Define Cloud Architecture

Objective Qualification

Purpose:

Determine the overall objective for moving to the cloud. This involves understanding the strategic drivers behind the decision to adopt cloud services.

Key Objectives:

1.Land New Services: Innovate and deploy new digital services quickly and efficiently.

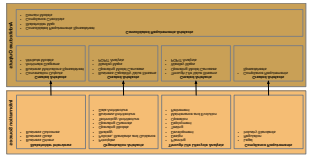
2.Digital Transformation: Enable broad organisational change through enhanced digital capabilities.

3.Digital Migration: Transition existing services and infrastructure to the cloud to modernise and reduce legacy burdens.

Modelling Motivations

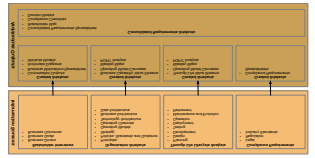
Drivers:

Definition: Drivers are the underlying forces or pressures that compel the organisation to consider cloud adoption. These can be external or internal factors.



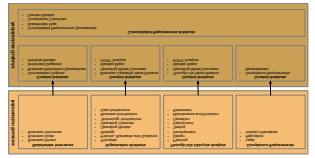
Why move to the cloud in the first place?

Business Driver	Goal	Outcomes	Motivation
Compliance with Regulatory Requirements	Achieve full compliance with regulations (e.g., GDPR, HIPAA, PCI-DSS)	Secure storage, data sovereignty, and controlled access; improved auditability	Meet Stringent Regulation
Cost Optimisation	Shift from capital expenditure (CapEx) to operational expenditure (OpEx)	Reduced upfront costs, scalable pricing models, and improved budget predictability	Cost Saving
Enhancing Customer Experience	Provide seamless, high-quality digital services to customers	Improved service delivery speed, personalised customer interactions, and increased customer satisfaction	Digital Transformation
Agility and Flexibility	Increase the organisation's agility to respond to market changes	Faster time-to-market for new products/services, easier scaling of resources	Digital Transformation
Business Continuity and Disaster Recovery	Implement robust disaster recovery and backup solutions	Reduced downtime, enhanced data protection, and improved business resilience	Risk Management
New Service Deployment	Enable the rapid deployment of new digital services	Quicker launch of products, real-time service updates, and improved market competitiveness	Digital Migration
Data-Driven Decision Making	Leverage cloud analytics for informed decision-making	Enhanced data analysis, business insights, and strategic decision support	Digital Transformation
Enhancing Collaboration	Enable seamless communication and collaboration across the organisation	Improved remote work capabilities, enhanced team productivity, and unified communication platforms	Digital Transformation
Security Enhancement	Strengthen the organisation's security posture with cloud-native tools	Advanced threat detection, automated compliance checks, and improved data encryption	Meet Stringent Regulation
Operational Efficiency	Streamline operations using cloud automation and managed services	Reduced IT overheads, automated patching, and improved resource management	Cost Saving
Modernising Legacy Infrastructure	Migrate legacy systems to a more scalable, flexible cloud infrastructure	Reduced maintenance costs, improved system performance, and enhanced scalability	Digital Migration
Global Expansion	Use cloud infrastructure to support global business expansion	Reduced latency, localised service offerings, and compliance with regional regulations	Digital Transformation
Product Innovation	Enable innovation with cloud-native development tools and services	Accelerated product development cycles, access to emerging technologies (AI, ML, IoT)	Digital Transformation
Competitive Advantage	Leverage cloud capabilities to differentiate from competitors	Improved market positioning, faster response to market trends, and increased customer retention	Digital Transformation
Risk Reduction	Reduce risks associated with on-premises infrastructure	Improved data security, reduced hardware failure risk, and enhanced compliance	Risk Management
Talent Attraction and Retention	Attract and retain skilled workforce by offering modern, flexible work environments	Enhanced remote work capabilities, access to cutting-edge tools, and improved employee satisfaction	Digital Transformation
Green Initiatives	Reduce carbon footprint through efficient cloud utilisation	Improved sustainability, reduced energy consumption, and compliance with environmental policies	Corporate Responsibility



Requirements Capture - Interviews

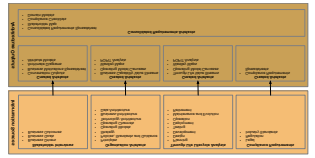
Business Attribute	Stakeholder	Requirement	Reasoning
Cost Efficiency	CFO	We need to transition from our high-capital IT investments to a more cost-efficient cloud model with lower upfront costs.	The CFO is focused on reducing the capital expenditures associated with traditional IT by shifting to a cloud model that emphasises lower initial costs and ongoing operational expenses.
Predictable Operating Costs	CFO	The shift to the cloud must provide predictable and manageable operating expenses, reducing the financial volatility we see with on-premises infrastructure.	The CFO values the ability to forecast and control expenses better with the cloud's pay-as-you-go model, as opposed to the unpredictable costs of maintaining on-premises systems.
Return on Investment (ROI)	CEO	Our move to the cloud should deliver a clear and measurable return on investment, reducing our overall IT spending while improving performance.	The CEO expects the cloud transition to not only lower costs but also to enhance business performance, thereby ensuring the investment yields a strong ROI.
Cost Reduction	COO	The transition to the cloud must help us reduce operational costs by streamlining processes and eliminating the inefficiencies of legacy systems.	The COO aims to leverage cloud technologies to drive down operational costs by removing the inefficiencies inherent in maintaining outdated IT systems.
Financial Flexibility	CFO	We need to maintain the flexibility to scale our cloud usage up or down based on business demands without long-term financial commitments.	The CFO is focused on the cloud's ability to offer financial flexibility, allowing the organisation to adjust expenses in real time according to current business needs.
Budget Adherence	Finance Director	Our cloud migration strategy must include strict budget controls to ensure that we do not exceed our planned expenditure during and after the transition.	The Finance Director requires stringent financial oversight during the cloud transition to prevent cost overruns and ensure that spending stays within the approved budget.
Vendor Cost Management	Procurement	We need to negotiate cloud service contracts that provide the best value and include cost controls to prevent unexpected charges.	The Procurement Manager is focused on managing the cost aspect of cloud service contracts, ensuring that the organisation gets the best value while avoiding hidden or unexpected fees.



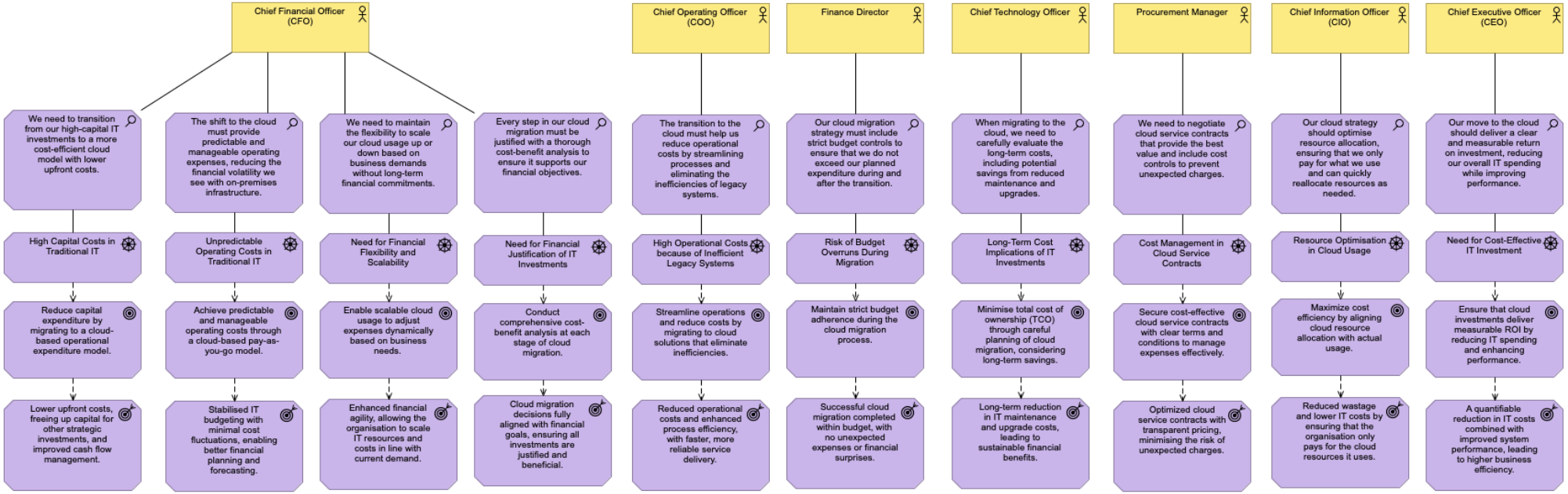
Example : Driver, Goals and Outcomes

Driver	Definition	Constraints	Goals	Outcomes

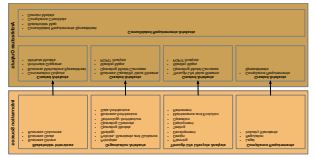
High Operational Costs	**High operational costs** in the existing technology landscape refers to the substantial expenses incurred by maintaining and operating on-premises infrastructure, legacy systems, and traditional IT services. These costs can include hardware maintenance, energy consumption, software licensing, IT staff overhead, and ongoing upgrades. Such costs often grow as systems age and become more complex, making it increasingly difficult to justify the financial outlay without corresponding business value.	• Increasingly costly hardware and software maintenance
		• Rising energy and cooling costs for data centres
		• High staffing costs for managing and supporting legacy systems
		• Difficulty in scaling operations without significant capital expenditure
		• Inefficiencies due to outdated technology and processes
			• **Reduce Total Cost of Ownership (TCO):**
			  • **Description:** Aim to decrease the overall costs associated with owning, operating, and maintaining IT infrastructure.
			  • **Target:** Achieve a 20-30% reduction in TCO over the next 2-3 years by transitioning to more cost-effective cloud solutions.
			• **Improve IT Cost Efficiency:**
			  • **Description:** Enhance the efficiency of IT spending by shifting from capital expenditure (CapEx) to operating expenditure (OpEx) models through cloud adoption.
			  • **Target:** Shift 50-60% of IT costs to a variable, usage-based model that aligns expenses with business activity.
			• **Optimise Resource Allocation:**
			  • **Description:** Free up resources (financial, human, and technical) by reducing the time and money spent on maintaining legacy systems.
			  • **Target:** Reallocate 25% of IT budget savings to innovation and business growth initiatives within 12 months.
				• **Significant Cost Savings:**
				  • **Outcome:** Realisation of substantial cost savings through the elimination of legacy system maintenance and the adoption of a more scalable cloud-based infrastructure.
				  • **Measurement:** A reduction in IT operational costs by 20% within the first year of cloud migration.
				• **Increased Financial Flexibility:**
				  • **Outcome:** Improved financial flexibility by moving from fixed, upfront capital investments to a more flexible, pay-as-you-go model.
				  • **Measurement:** A 30% increase in available capital for strategic investments in new technologies and business initiatives.
				• **Enhanced IT Operational Efficiency:**
				  • **Outcome:** Streamlined IT operations, leading to quicker deployment times, reduced downtime, and improved system reliability.
				  • **Measurement:** A 15% improvement in IT efficiency metrics such as system uptime, deployment times, and incident response rates within 18 months.
				• **Reallocation of Resources to Strategic Initiatives:**
				  • **Outcome:** IT staff and financial resources freed up from legacy system maintenance can now be directed towards innovation, improving customer experience, and supporting digital transformation efforts.
				  • **Measurement:** 25% of the IT workforce redirected towards strategic projects and innovation, resulting in the faster rollout of new services and products.



Using Archimate to show relationships

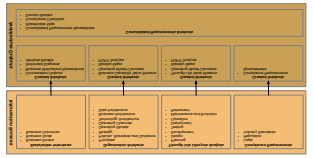


In this example, the relationships are very one-dimensional, but by using the Properties and Name Value pairs, you can start to model and visualise different aspects.



High Operational Costs - Attributes Modelling

Business Attribute	Associated Security Attribute	Justification	Reasoning
Cost Efficiency	Cost Effectiveness	Security measures must be cost-effective to ensure that security investments do not negate the cost savings achieved through cloud adoption. Cost-effective security solutions help maintain overall budget goals.	Aligning security spending to reduce operational costs is crucial. Security solutions must provide maximum protection without undermining the financial benefits of the cloud adoption strategy.
Operational Efficiency	Operational Resilience	Operational efficiency can be undermined by security incidents. Ensuring operational resilience through robust security controls supports uninterrupted service delivery and contributes to overall efficiency.	Operational efficiency in cloud environments can be easily compromised by security incidents. Ensuring resilience through well-planned security controls ensures continuity and supports overall efficiency goals.
Scalability and Flexibility	Scalable Security Controls	As the organisation scales operations in the cloud, security controls must be scalable to protect expanded infrastructure without compromising performance or flexibility.	As cloud environments can rapidly scale, security measures need to be equally flexible and scalable to accommodate growth without introducing vulnerabilities or excessive costs.
Resource Optimisation	Efficient Security Management	As resources are reallocated to strategic initiatives, security management must be efficient, reducing the burden on IT staff while maintaining robust security postures.	With a focus on reallocating resources to strategic initiatives, efficient security management ensures that the security posture is maintained without consuming disproportionate resources.
Financial Flexibility	Risk Management and Compliance	To protect financial flexibility, security measures should include robust risk management and compliance frameworks, preventing costly breaches and fines that could impact financial agility.	Protecting financial flexibility involves managing risks that could lead to significant financial losses, such as data breaches, and ensuring compliance to avoid regulatory penalties.
Agility in IT Operations	Adaptable Security Framework	The need for agility in IT operations requires an adaptable security framework that can quickly respond to new threats and changes in the IT environment without causing significant disruptions.	Security frameworks must be adaptable to support the need for agility in IT operations, allowing for quick adaptation to new threats or changes in the business environment.
Innovation Enablement	Security by Design	Security should be integrated into the development process ('Security by Design') to ensure that new innovations are secure from inception, avoiding costly rework and vulnerabilities.	Embedding security into the development process enables innovation without compromising on security, preventing vulnerabilities from being introduced as new products or services are developed.

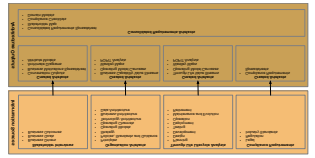


Organisational Artefacts

All sorts of things will impact the success of the Cloud implementation which extend beyond mere IT.

Analysis needs to extend to other elements which may constrain or present opportunities when defining the cloud requirements.

Element	Constraints	Opportunities
Principles	Define non-negotiable rules that limit design flexibility.	Provide a foundation for consistent and aligned cloud adoption.
Policies, Standards, and Guidance	May impose strict compliance and security requirements.	Ensure best practices and regulatory compliance in cloud design.
Strategy	May restrict adoption to certain cloud providers or models.	Aligns cloud initiatives with long-term business objectives.
Operating Models	Existing processes can limit cloud integration and automation.	Enable new ways of working, improving efficiency and scalability.
Operating Channels	Legacy channels may not support cloud-native interactions.	Open up new digital engagement channels through the cloud.
Technology Architecture	Legacy systems can limit cloud migration and integration.	Facilitate modern, flexible architecture through cloud services.
Business Architecture	Business constraints may limit the scope of cloud adoption.	Supports business agility and innovation through cloud capabilities.
Data Architecture	Data sovereignty and compliance can constrain data placement.	Enhances data availability, analytics, and insights through cloud services.



At the Cloud Capability level, consider the....

Through Life Value Stream

Governance

Planning	This phase involves the initial decision to create the service. It includes understanding the need or problem the service will address, defining the business goals and objectives, identifying stakeholders, and establishing the scope of the service.
Design	In this phase, the functional requirements and non-functional requirements (such as performance, security, and reliability) of the service are defined. The service's interface is designed, along with its interactions with other services and components.
Development	During this phase, the service is coded and built according to the design specifications. This includes implementing the business logic, the service interfaces, and the data models.
Testing	In this phase, the service is tested to ensure it meets the functional and non-functional requirements. This can include unit testing, integration testing, performance testing, security testing, and user acceptance testing.
Deployment	After testing, the service is deployed into the production environment. This may involve setting up the necessary servers, databases, network configurations, and other infrastructure required to support the service.
Operation	During this phase, the service is actively used to support business operations. It is monitored to ensure it is performing as expected, and any issues or errors are addressed.
Maintenance and Evolution	After the service is in operation, it will typically require ongoing maintenance to fix bugs, improve performance, or add new features. The service may evolve over time in response to changing business needs or technological advances.
Retirement and Replacement	Eventually, a service may become obsolete or no longer fit for purpose. It might be replaced by a new service, or its functionality might be incorporated into other services. In this phase, the service is decommissioned, and any associated resources are cleaned up or repurposed.

Education and Training

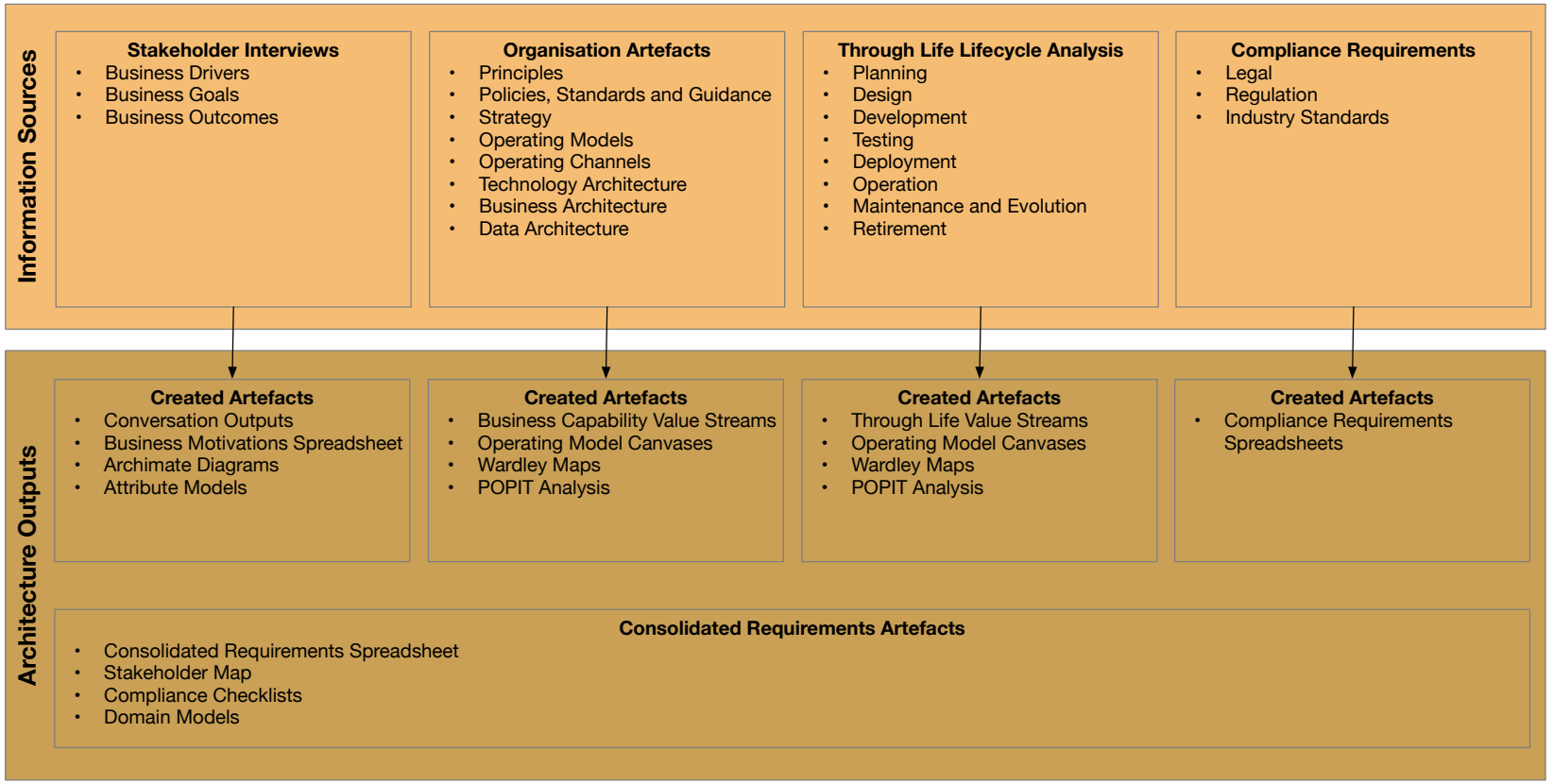
Compliance and Regulation

Platform Capabilities

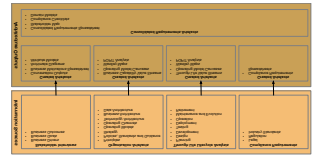
Security Capabilities

Multi Cloud and Enterprise Posture Management (Security and Operations)

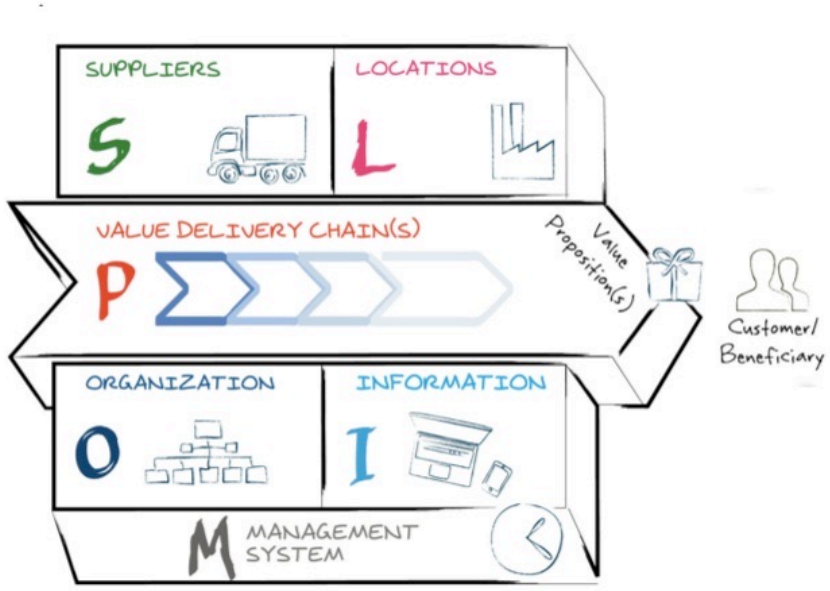
Sourcing Requirements



SABSA emphasises stakeholder interviews and attribute mapping to gather requirements; however, gaining access to these stakeholders can be difficult, and the scope and detail of the information collected often need enhancement to ensure a comprehensive requirements analysis.



Operating Model Canvas

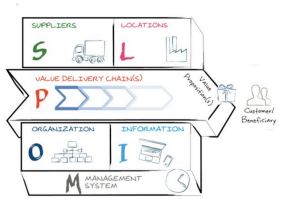


What is an Operating Model Canvas – A simple, lightweight way to represent the security environment

1. **Unified Security Framework**
- ***Processes & Information***: Describes how security is embedded across processes and data flows.
- ***Organisation & Suppliers***: Aligns roles, responsibilities, and third-party security requirements, enhancing collaboration and risk management.
- ***Location***: Allows you to describe data sovereignty and compliance with geographical considerations.
- ***Management Systems***: Describes GRC systems for continuous monitoring and improvement.

2. **Alignment with Business Objectives -** Ensures security requirements support, rather than hinder, business agility and cloud scalability.
3. **Enhanced Communication & Collaboration -** Facilitates clear, cross-stakeholder communication, translating complex security needs into actionable terms.
4. **Scalability & Flexibility** – Allows for the dynamic adaptation of security requirements as cloud environments evolve.
5. **Improved Risk Management** - Comprehensive mapping of risks across domains, enabling effective mitigation.
6. **Regulatory Compliance** - Supports adherence to standards like GDPR and ISO 27001, ensuring data protection and legal compliance.
7. **Continuous Improvement** - Embeds feedback loops for ongoing refinement based on emerging threats and regulatory changes.

Use OMC's before and after cloud delivery



Cost Management Operating Model Canvas - Suppliers

Suppliers

Support and Maintenance Vendors - IBM, Oracle, Dell EMC.
These vendors work closely with the company to provide ongoing support and maintenance for legacy systems. They collaborate on system upgrades, patches, and troubleshooting, ensuring the systems remain operational and compliant. The partnership often includes consulting on optimising system performance and managing costs related to system upkeep.

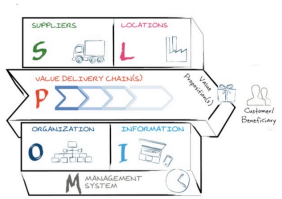
Third-party IT service providers like Infosys, TCS.
These providers offer specialised support services for legacy systems, including incident management, system monitoring, and performance optimisation. They collaborate by taking on routine maintenance tasks, which allows the company's internal IT team to focus on strategic initiatives. The partnership aims to reduce operational costs through efficient outsourcing of routine IT support functions.

Compliance Partners - PA Consulting, Deloitte.
Compliance partners help ensure that legacy systems adhere to evolving regulatory requirements. They collaborate by conducting audits, offering compliance consulting, and helping to implement necessary changes to meet legal and regulatory standards. This partnership is crucial for avoiding fines and reducing non-compliance costs.

Hardware and Software Suppliers - Cisco, HP, Lenovo.
Hardware suppliers provide essential infrastructure components such as servers, storage, and networking equipment. They collaborate by offering maintenance services, advising on hardware upgrades, and assisting in extending the lifecycle of existing equipment. This partnership focuses on minimising capital expenditure by optimising the use of current hardware and planning cost-effective upgrades.

Energy and Physical Suppliers - Schneider Electric, Siemens.
These consultants work with the company to optimise energy consumption in data centres and other facilities housing legacy systems. They provide expertise in energy efficiency strategies, helping to reduce the operational costs associated with power and cooling. The collaboration includes regular audits, implementation of energy-saving technologies, and continuous monitoring of energy usage.

Service Delivery Consultancies - PA Consulting, Capgemini.
These consultants work with the company to identify and eliminate inefficiencies in the operational processes tied to legacy systems. They collaborate on re-engineering processes, implementing automation, and optimising workflows. The focus of this partnership is to reduce labour costs and improve overall operational efficiency.



Cost Management Operating Model Canvas - Locations

Locations

Primary On-Premises Data Centre

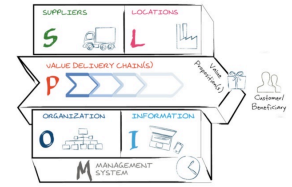
Location: London, UK – Corporate Headquarters Building.
Nature of Work: Hosts the core financial applications, databases, and critical legacy systems that support the company's operations.
Assets :
Servers and Storage: High-performance servers and extensive storage arrays to handle large volumes of transaction data.
Networking Equipment: Robust networking infrastructure to ensure seamless connectivity and data transfer within and outside the data centre.
Power and Cooling Systems: Redundant power supplies, backup generators, and advanced cooling systems to maintain optimal operating conditions and ensure system uptime.
Security Systems: Physical and network security systems, including firewalls, access control systems, and surveillance, to protect sensitive financial data.

Backup Data Centre

Location: Manchester, UK – Dedicated Disaster Recovery Facility.
Nature of Work: Provides redundancy for critical systems and data, ensuring business continuity in case of failure at the primary data centre.
Assets :
Mirrored Servers and Storage: Identical servers and storage infrastructure to support rapid failover and data recovery to the primary data centre.
Disaster Recovery Tools: Specialized software and tools for data replication, backup, and disaster recovery planning.
Network Redundancy: Secondary networking paths to ensure uninterrupted connectivity between the primary and backup data centres.
Security Measures: Enhanced physical and cybersecurity measures to safeguard the backup facility, including restricted access and encryption.

Corporate Offices

Location: London, UK – Corporate Headquarters Building.
Nature of Work: Centralized management of IT operations, financial planning, vendor management, and strategic decision-making.
Assets :
IT Operations Centre: A dedicated control room equipped with monitoring tools, dashboards, and communication systems to oversee the performance and status of legacy systems.
Workstations: High-performance desktops and laptops for IT staff, equipped with software for system management, financial analysis, and reporting.
Collaboration Tools: Video conferencing systems, collaboration platforms (e.g., Microsoft Teams, Slack), and project management tools to facilitate teamwork and communication.
Documentation and Compliance Systems: Secure storage for compliance documents, audit records, and operational manuals, both in physical and digital formats.



Cost Management Operating Model Canvas - Processes

Processes

Assessment of Legacy Systems:

Activity: Regularly assess the performance and costs associated with existing legacy systems.
Objective: Identify cost drivers, inefficiencies, and potential areas for cost reduction.
Outcome: Comprehensive understanding of where operational costs are highest, enabling targeted cost-reduction strategies.

Vendor Management and Contract Negotiation:

Activity: Negotiate and manage contracts with legacy system vendors, hardware suppliers, and support service providers.
Objective: Optimise vendor contracts for better pricing, payment terms, and service levels.
Outcome: Reduced costs through more favourable contract terms and effective vendor relationship management.

System Maintenance and Upgrades:

Activity: Conduct regular maintenance and necessary upgrades to legacy systems to ensure reliability and compliance.
Objective: Minimise downtime and the risk of costly failures while keeping systems compliant with regulatory standards.
Outcome: Reduced operational disruptions and extended system life, leading to cost savings in the long term.

Energy and Facilities Management:

Activity: Manage energy consumption and facilities costs for running on-premises data centres.
Objective: Implement energy-saving initiatives and optimise facility use to reduce overheads.
Outcome: Lower energy and facilities costs, contributing to overall operational cost reduction.

Budgeting and Financial Planning:

Activity: Develop and manage budgets for maintaining legacy systems, including capital expenditures (CapEx) for hardware upgrades and operational expenditures (OpEx) for support and maintenance.
Objective: Ensure that financial resources are allocated effectively to maintain system uptime while controlling costs.
Outcome: Controlled and predictable operational costs, with budgets aligned to strategic cost management goals.

Resource Allocation and Utilisation:

Activity: Allocate IT resources (e.g., servers, storage, network bandwidth) based on usage patterns and system requirements.
Objective: Maximise resource utilisation to avoid wastage and reduce operational costs.
Outcome: Improved efficiency in resource usage, leading to lower operational costs and reduced wastage.

Process Optimisation:

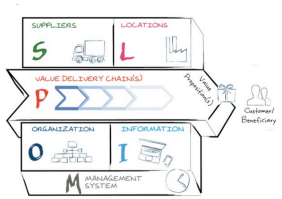
Activity: Review and streamline operational processes to reduce manual interventions and improve efficiency.
Objective: Identify and eliminate inefficiencies in workflows related to legacy systems.
Outcome: Lower labour costs and increased operational efficiency through automation and process improvements.

Risk Management and Mitigation:

Activity: Implement risk management strategies to prevent costly system failures and data breaches.
Objective: Reduce the financial impact of unexpected incidents by proactively managing risks.
Outcome: Decreased likelihood of costly disruptions, leading to more stable and predictable operational costs.

Reporting and Performance Monitoring:

Activity: Regularly monitor and report on operational performance and cost metrics.
Objective: Provide visibility into cost drivers and areas for improvement, enabling informed decision-making.
Outcome: Enhanced ability to manage and reduce operational costs through data-driven insights and continuous monitoring.

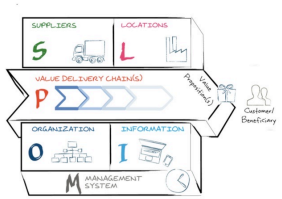


Cost Management Operating Model Canvas - Organisation

Organisation

Component	Description
Roles & Responsibilities	Leadership oversees strategy, Ops handle daily management.
Reporting Structure	Top-down with cross-functional collaboration.
Governance	Board ensures compliance; Ops team reviews monthly performance.
Skills & Capabilities	Key: Finance, IT, Ops. Gaps: AI, Cybersecurity.
Culture	Collaboration & cost-efficiency driven.
Capacity Planning	Workforce sized for current needs; regularly reviewed.
External Stakeholders	Vendors & consultants for cost optimisation.

Roles and Responsibilities: Define the key roles within the organisation, both at the leadership and operational levels.
Reporting Structure: Identify the formal reporting lines and hierarchies within the organisation.
Governance and Leadership: Document how decisions are made, including the governance structures in place.
Skills and Capabilities: Define the key skills and capabilities required within the organisation to support the operating model.
Culture and Values: Capture the core values, cultural attributes, and behaviours essential to the organisation's success.
Capacity and Workforce Planning: Analyse the current workforce size and the capacity needed to support the operating model.
External Stakeholders and Relationships: Identify key external stakeholders, such as suppliers, partners, or regulators, and how the organisation interacts with them.



Cost Management Operating Model Canvas - Information

Information

Financial Transaction Processing

Customer account data, transaction records, and financial reporting data.

IT Applications

Core Banking System (Bespoke): A customized core banking application that handles all financial transactions, account management, and reconciliation. It needs to be bespoke due to the financial services company's specific regulatory requirements and unique business processes.

Integration: Must be part of an integrated enterprise system to ensure real-time updates and consistency across all financial records.

Business Owner: CFO and Head of Banking Operations.

Associated Activity: Process transactions, manage customer accounts, generate financial statements, and ensure compliance with financial regulations.

Customer Relationship Management

Customer profiles, interaction history, product holdings, and service requests.

IT Applications

CRM System (Standard OTS with Custom Modules): A standard off-the-shelf (OTS) CRM solution with customised modules to cater to the specific needs of financial services, such as compliance tracking and financial advisory.

Integration: This needs to be integrated with the core banking system for seamless access to customer financial data and transaction history.

Business Owner: Head of Customer Service and Chief Marketing Officer (CMO).

Associated Activity : Manage customer interactions, track service requests, support marketing campaigns, and provide customer insights for personalised service delivery.

Regulatory Compliance and Risk Management

Regulatory guidelines, risk assessment reports, compliance audit trails, and incident records.

IT Applications:

Compliance Management System (Bespoke): A bespoke application tailored to the company's specific regulatory environment, managing all compliance-related activities, including audits, reporting, and risk management.

Risk Management Tool (Standard OTS): An off-the-shelf risk management application used for identifying, assessing, and mitigating risks and integrated with compliance management to ensure comprehensive risk oversight.

Integration: Both applications must be part of the integrated enterprise system to ensure compliance and risk data are synchronised across the organisation.

Business Owner: Chief Risk Officer (CRO) and Chief Compliance Officer (CCO).

Associated Activity: Ensure regulatory compliance, manage risks, conduct audits, generate compliance reports, and track risk mitigation activities.

Also includes: Data Analytics and Reporting, IT Operations and Infrastructure Management and Human Resources Management

Suppliers

Support and Maintenance Vendors	IBM, Oracle, Dell EMC
3rd Party Service Providers	Infosys, TCS
Hardware and Software Suppliers	Cisco, HP, Lenovo, SAP
Service Deliver Consultancies	PA Consulting, Capgemini
Compliance Service Providers	PA Consulting, Deloitte
Energy providers and consultancies	Schneider Electric, Siemens

Locations

Primary On-Premises Data Centre	**Location**: London, UK – Corporate Headquarters Building. **Nature of Work**: Hosts the core financial applications, databases, and critical legacy systems that support the company's operations.
Backup Data Centre	**Location**: Manchester, UK – Dedicated Disaster Recovery Facility. **Nature of Work**: Provides redundancy for critical systems and data, ensuring business continuity in case of failure at the primary data centre.
Corporate Offices	**Location**: London, UK – Corporate Headquarters Building. **Nature of Work**: Centralised management of IT operations, financial planning, vendor management, and strategic decision-making.

Cost Management Process

Assessment of Legacy Systems: Regularly assess the performance and costs associated with existing legacy systems.

Budgeting and Financial Planning: Develop and manage budgets for maintaining legacy systems, including capital expenditures (CapEx) for hardware upgrades and operational expenditures (OpEx) for support and maintenance.

Vendor Management and Contract Negotiation: Negotiate and manage contracts with legacy system vendors, hardware suppliers, and support service providers.

Resource Allocation and Utilisation: Allocate IT resources (e.g., servers, storage, network bandwidth) based on usage patterns and system requirements.

System Maintenance and Upgrades: Conduct regular maintenance and necessary upgrades to legacy systems to ensure reliability and compliance.

Process Optimisation: Review and streamline operational processes to reduce manual interventions and improve efficiency.

Energy and Facilities Management:

Review and streamline operational processes to reduce manual interventions and improve efficiency.

Risk Management & Mitigation: Implement risk management strategies to prevent costly system failures and data breaches.

Reporting and Performance Monitoring: Regularly monitor and report on operational performance and cost metrics.

Value

Ensures optimal resource utilisation, scalability, and financial predictability: Utilises automated monitoring and continuous optimisation to minimise unnecessary expenditures while maximising operational efficiency.

Organisation

Roles & Responsibilities	Leadership oversees strategy, Ops handle daily management.
Reporting Structure	Top-down with cross-functional collaboration.
Governance	Board ensures compliance; Ops team reviews monthly performance.
Skills & Capabilities	**In Place:** Finance, IT, Ops. **Current Gaps:** AI, Cybersecurity.
Culture	Collaboration & cost-efficiency driven.
Capacity Planning	Workforce sized for current needs; regularly reviewed.
External Stakeholders	Vendors & consultants for cost optimisation.

Information

- Financial Data: Budgets, actual expenditures, revenue, invoices, and financial forecasts.
- Procurement Data: Purchase orders, vendor contracts, and payment details.
- Asset Management: Costs of assets, depreciation, maintenance, and upgrades.
- Operational Costs: Payroll, utilities, facility expenses, and IT infrastructure costs.
- Project Costs: Project budgets, resource allocation, and labour expenses.
- Risk & Compliance: Costs of risk mitigation, audits, and compliance.
- Reporting: Cost variance analysis, efficiency metrics, and performance dashboards.

Management Systems

Enterprise Resource Planning (ERP) Systems: Used for financial planning, budgeting, and managing expenditures. Integrates various business processes, such as accounting, procurement, and inventory management, facilitating cost tracking and reporting.
Financial Management Systems: Dedicated systems for tracking expenses, managing budgets, and forecasting financial performance. It could include modules for accounts payable, accounts receivable, payroll, and fixed asset management.
Project Management Systems: For managing resource allocation and tracking project costs. Involves scheduling, resource planning, and cost estimation to ensure projects stay within budget.
Procurement Management Systems: Manages vendor contracts, purchase orders, and supplier payments. Helps in cost negotiation and ensures compliance with budgetary constraints.

Human Resource Management Systems (HRMS): Handles payroll, benefits administration, and workforce planning. Assists in understanding labour costs and aligning them with organisational budgets.
Asset Management Systems: Monitors and maintains physical assets, managing their lifecycle costs. Assists in planning for capital expenditures and ongoing maintenance.
IT Management Systems: Tracks IT infrastructure costs, including hardware, software, and network resources. Involves monitoring the utilisation and maintenance of legacy systems.
Facilities Management Systems: Manages the costs associated with facilities, including utility expenses, maintenance, and space utilisation.

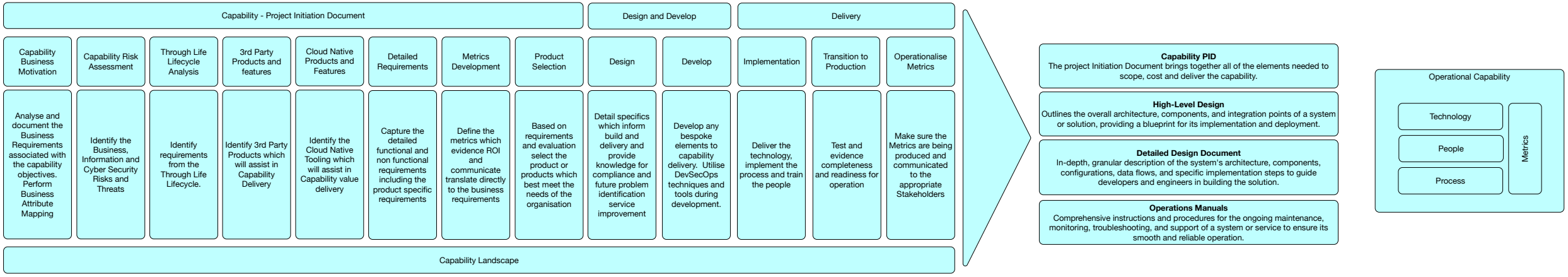
Cost Management – As Is

Ver: 1.0
Date: July 2024
Author: Rob Campbell

Stage 2 : Developing the Capabilities

Now you have an understanding of the overarching motivations and cloud requirements, you can start developing the individual capabilities. These will need to be structured and delivered in a series of projects. Each project will have its own refined motivations and requirements and decisions will need to be made.

This should look familiar to most of you.



Rob Campbell

I love to talk about my work. Feel free to contact me as I am happy to share my knowledge and will happily share templates and examples where I am able.

Email: rob@assuredcontrol.com

or Robert.Campbell@paconsulting.com

Phone : +44 7989 163 138

SESSION FEEDBACK

Paper feedback forms are available from the front of the room