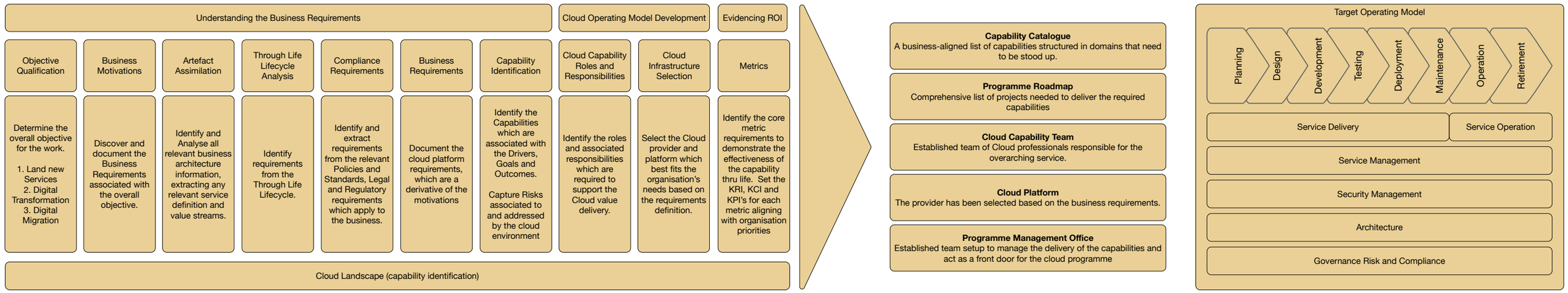
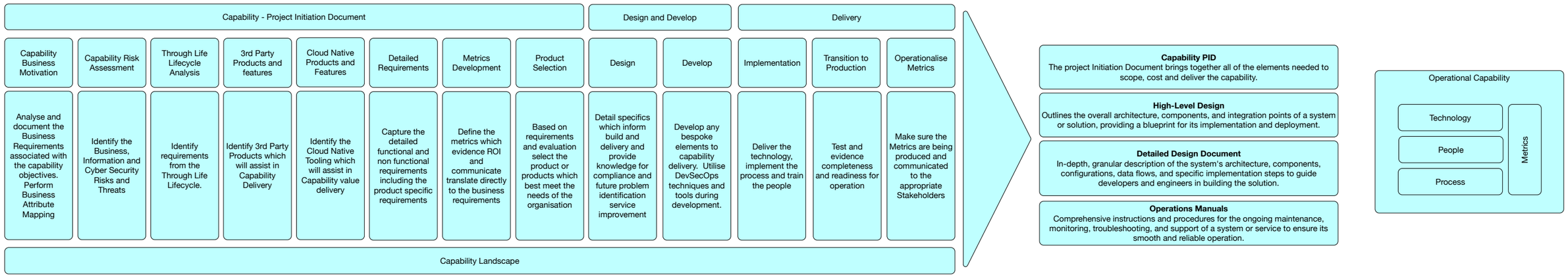
Business-Driven Cloud Architecture Process

This stage of the process focuses on the contextual and conceptual aspects, which are often absent from most provider reference architectures. The primary goal here is to understand the business motivations and establish the overarching requirements. This understanding will help identify the necessary business and technical capabilities to be developed.



In this second stage, the process is repeated several times, concentrating on developing specific business requirements for each capability identified earlier. Once a Project Initiation Document is defined for each capability, the Cloud Providers Reference Architectures are utilised to guide the High and Low-Level Designs for those capabilities. The end result is a cloud environment that aligns with the business's original



Rob Campbell - 07989 163 138 Email - esa@assuredcontrol.com

Domains and Capabilities - Context and Concept

In the context of the SABSA framework, the concepts of domains and capabilities within cloud environments are pivotal at both the Contextual and Conceptual levels of the SABSA Matrix.

At the **Contextual level**, which represents the business view, domains and capabilities are defined in terms of the organisation's overarching objectives and requirements. Here, **domains** encapsulate the broad categories of business needs related to cloud operations, such as Service Management, Security and Compliance, and Financial Management. These domains answer the fundamental questions of **"What"** the business aims to achieve and **"Why"** these objectives are critical. For instance, a domain like Security and Compliance reflects the need to protect assets and adhere to regulatory mandates, driven by the imperative to maintain trust and avoid legal penalties.

Within these domains, **capabilities** represent the essential functions and services required to fulfil the business objectives. They address the **"How"** aspect at a high level, outlining the methods by which the organisation intends to meet its needs. For example, under the Security and Compliance domain, capabilities such as Threat and Vulnerability Management and Identity and Access Management are identified as crucial for safeguarding the cloud environment and ensuring only authorised access.

Moving to the **Conceptual level**, which offers the architect's perspective, the focus shifts to developing a conceptual security architecture that satisfies the requirements identified at the Contextual level. Here, the **domains** are refined into conceptual models that define the principles and standards guiding the cloud strategy. The domains address the **"How"** in greater detail, establishing a blueprint for implementing the necessary controls and mechanisms.

The **capabilities** at this level are further elaborated to specify the services and processes that will operationalise the conceptual models. They consider the **"Who"**, **"Where"**, and **"When"** aspects, determining who is responsible for each capability, where in the organisation or system they are applied, and the timing or sequencing of their implementation. For instance, the capability of Security Operations within the Security and Compliance domain might involve establishing a Security Operations Centre (SOC) staffed by skilled analysts who monitor the cloud environment continuously.

In essence, by applying the SABSA framework's Contextual and Conceptual levels to cloud environments before they even choose a provider, organisations can ensure that their domains and capabilities are aligned with business goals and systematically designed to comprehensively address security and operational requirements. This approach facilitates a coherent strategy where every capability within a domain contributes to a robust and secure cloud architecture, effectively bridging business needs with technical solutions.

Rob Campbell - 07989 163 138 Email - esa@assuredcontrol.com