WHITEPAPER

Laying the **Groundwork**

How to Build a Foundation in Google Cloud

sourced
cloud at scale™

Table of Contents

Executive Summary

Enterprises each face different challenges and will all have different experiences when embarking on a cloud journey. However, Sourced has identified an optimal approach to deliver sustainable and long-term success in the cloud, whatever the situation. This paper focuses on the **Google Cloud Platform** (GCP) which is rapidly expanding across all major regions. GCP has a differential and unique value proposition, specifically in application containerisation and data solutions.

Over the last 10 years, Sourced has had the privilege of working with a broad set of enterprises during varying stages of their cloud deployments. Consolidating this experience, Sourced has refined an approach to cloud adoption that focuses on building a strong foundational capability that can centralise compliance while allowing application teams to self-service their infrastructure within appropriate guardrails.

Sourced's recommended approach caters for both technology and organisational changes that cloud introduces into a business; this is defined as cloud-led business change. A lack of organisational alignment when implementing a fundamentally different way of consuming infrastructure regularly leads to adverse outcomes. The use of an aligned 'Cloud Centre of Excellence' (CCoE) rallying around a masthead application migration will help draw buy-in from all required stakeholders. The masthead will ensure that the features developed for the foundational platform are of the highest value, hence controlling scope.

Another major pillar of cloud success is the layered security approach. This involves applying governance that focuses on preventative controls during the early stages of cloud adoption, ensuring teams gain maturity within appropriate risk guidelines. The best method to achieve these control objectives is by adopting infrastructure and governance as code practices that a foundational platform can deliver. Additional types of controls can be continually layered and a combination of methods is recommended to achieve the best outcomes. As teams develop cloud maturity, a relaxation of preventative controls and an increase in detective controls may be appropriate for certain low-risk workloads that require bespoke solutions.

The described approach allows regulated enterprises to gain delivery velocity in the cloud while bringing the wider organisation along with them. The benefits of scalability, efficiency and availability can be achieved by any organisation regardless of regulatory requirements. The common misstep of seeking rapid single-workload migrations can lead to technical debt and minimal reusability, causing a diversion from the organisation's cloud strategy and its objectives. Long-term success for the whole of business change requires a thoughtful and measured approach in the early stages, that leads to cloud maturity and on to Cloud at Scale™.

Introduction

Google Cloud is rapidly gaining adoption within the enterprise as a result of its significant investment in cloud infrastructure (currently 67 zones globally) and subsequent increased maturity of the platform. As a result of this growth, Google Cloud is gaining traction in markets across the globe while leading with its unique and differential containerisation and data solutions.

Sourced's consulting team has delivered Google Cloud foundations for our Tier-1 banking clients in North America and Australia. These foundations have provided a consistent landing zone for several material workloads supportive of their regulatory and compliance considerations. Through our experience in the industry, Sourced has developed a framework for regulated enterprises looking to adopt Google Cloud and leverage Google's differential capabilities within their business. By leveraging automation, aligning tooling, and embedding a culture of managing infrastructure as code, Sourced balances the technology strategies of the enterprise. It is imperative to consider the requirements of Central IT, compliance, security, and developers, all while operating within appropriate risk boundaries.

This whitepaper will represent a high-level approach to deploying a scalable Google Cloud foundation which scales to support potentially thousands of heterogeneous workloads within a large, regulated enterprise.

Where We Are Today

The largest financial services organisations in Australia are pushing heavily to integrate technology into their offerings in order to deliver improved services and experiences to their consumers. The adoption of public cloud is a significant enabler for this movement. With this push, the **Australian Prudential Regulation Authority** (APRA) has been firm but supportive, providing one of the most mature approaches to public cloud risk management.

> **READ:**
>
> An Analysis of the APRA Cloud Computing Services Paper Update

The financial services industry can thereby use an APRA aligned approach to public cloud risk management to provide a target standard when leveraging public cloud in other regulatory regions globally.

Adherence to regulatory obligations requires organisations to undertake a measured approach when consuming public cloud services. Regulated organisations are required to distil their obligations into internal policy and eventually, into control objectives. The implementation and assurance of these controls or, **control management**, is paramount to the enterprise successfully consuming cloud.

Technology innovation is primarily driven from the areas in the business closest to the customer, owing to a desire to compete and maintain an edge in the market. These initiatives become the catalyst for cloud adoption and from here, the enterprise often goes one of two ways:

Workload Approach

This approach sees the business unit developing a bespoke approach with minimal involvement from the organisation's Central IT teams. This results in a deployment and operational philosophy tailored to the workload itself. This approach can also deliver short-term velocity but presents difficulties when the next wave of workloads begin their migration journey.

The next workload will see another set of bespoke public cloud configuration and this process repeats itself until the organisation is left with a complex footprint that introduces significant risk and operational overheads. Furthermore, visibility of controls becomes unclear and this lack of clarity can lead to breaches and exposures.

Platform Approach

An alternative approach is when the business unit integrates tightly with the centralised IT team to form a CCoE with a mission to build core cloud capability that can be leveraged across the entire enterprise. This will involve a scalable foundation which will allow the cloud to operate as a platform with the workload being used as a masthead to drive delivery.

This approach allows for a consistent control plane across the entire fleet of applications and helps centralise common functions such as networking, billing and security. This key element of cloud adoption is an essential part of Sourced's **Cloud at Scale**™ methodology.

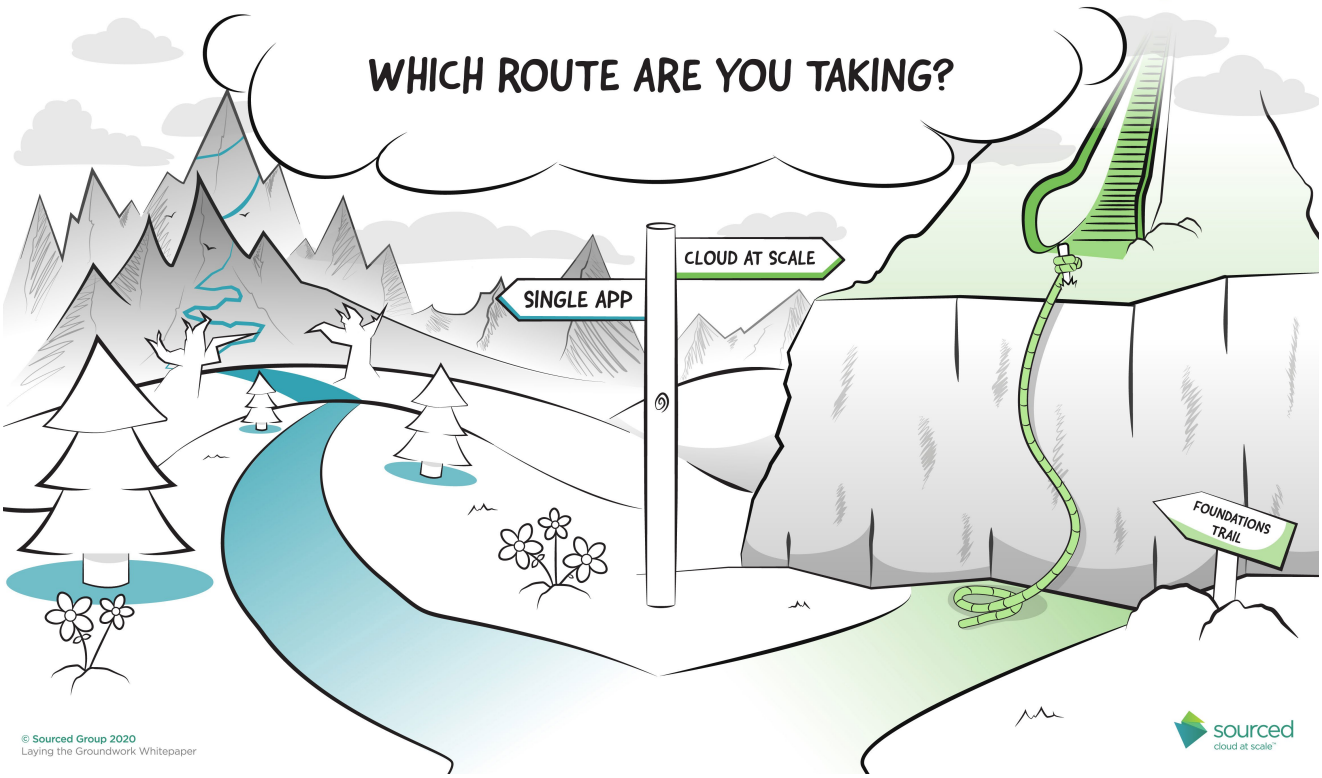


Figure 1. Workload or platform approach

It should be noted that the workload driven approach can act as a catalyst for change within the organisation. A responsible approach to building a bespoke cloud capability around a single workload can be a viable project, however care should be taken to ensure that a more strategic platform approach can be adopted as use cases for cloud broaden over time.

Delivering a foundational platform can be a potentially difficult decision due to longer adoption times. However, in the context of a broader enterprise cloud strategy, it is an essential ingredient for success longer term.

Foundational platforms help us achieve several key outcomes:

Operations

Minimises operational irregularities and manual work through a consistent and automated approach to cloud

Security

Ensures an enterprise security posture is applied holistically across the cloud environment

Scale

Provides a method to scale cloud deployments from one team to any number of teams without a linear increase in operational cost

Maturity

Provides a secure, consistent, and controlled deployment methodology allowing teams to gain significant maturity in public cloud within the enterprise's approved guardrails

Velocity

Provides consistency in outcomes through automation, hence reducing the number of unique assessments, reviews, and political debate required to deliver value add

Control Pane

Measures against regulatory obligations using a single, auditable view of controls

Achieving these outcomes builds trust, confidence and predictability for public cloud deployments. Where manual processes breed complexity, which in turn leads to a higher probability failure, automation provides predictability and consistency, which in effect is a control. It is worth noting that the two summarised approaches are typical but not all encompassing.

There are many ways to consume public cloud and determining what will suit your organisation best requires discovery and analysis. This whitepaper discusses cloud foundations as the typical recommended first step, however, **Sourced will always make informed and tailored recommendations that are in the best interests of the client's goals.**

How Can I Build My Foundations in Google Cloud?

Each enterprise cloud platform will differ slightly based on many factors including strategic goals, geographical distribution and regulatory considerations, however most will follow a common progress as detailed in this section. Starting from the ground up, **Central IT** will begin the process of architecting and designing a cloud foundation which consists of, but is not limited to, the following:

- **Organization** – Top level hierarchy, Organization, Policies, Billing, Logging
- **Shared Networking** – VPCs, NAT, DNS, Firewalls, Routes, VPN, Interconnect
- **Projects and IAM** – Folders, Service Projects, IAM

Sourced will always make architectural decisions based on client needs but often approaches Google Cloud Foundations leveraging a centralised host project to manage further application or "service projects" spanning into the host to leverage network connectivity as below:

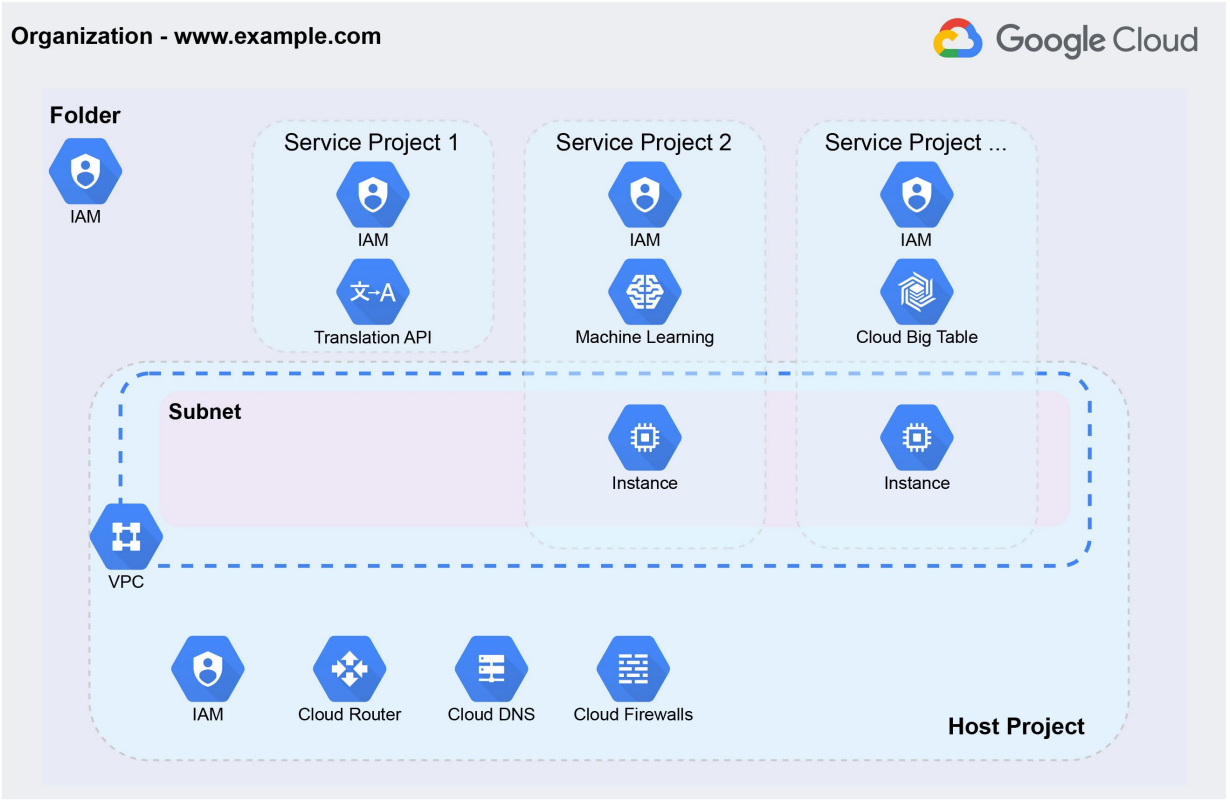


Figure 2. Scalable host project with multiple service projects

Given the requirement for consistency in deployment and configuration across the broad set of structures and resources, automation is naturally introduced into the process. For the Central IT team to implement this automation when building, deploying, and operating these foundations, the following two options will have focus:

1

A CI/CD pipeline leveraging **Google's native Deployment Manager** or **Config Connector** to deploy infrastructure as code

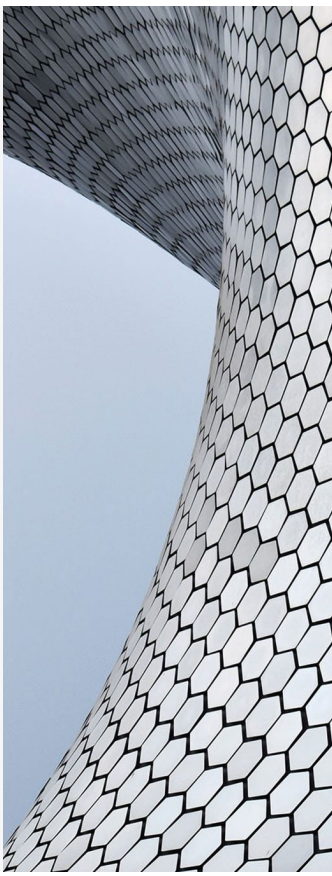
2

A CI/CD pipeline leveraging **third party tooling**, such as Terraform, which uses a declarative language to define infrastructure as code

The **Continuous Integration Continuous Deployment** (CI/CD) pipeline, synonymous with platform automation, is the method in which Sourced links all the automation components together to achieve this consistent outcome, whether it be leveraging Terraform, Deployment Manager or Config Connector.

"Central IT departments that fall behind in establishing cloud governance risk security breaches, denial of service (DoS) attack, loss of control and cloud resources overspending. Implementing automated governance is part of transforming Central IT's role from fulfilling users' requests to empowering self-service for teams that need the agility to use cloud services with native tools."

Gartner, 'Implementing Governance for Public Cloud IaaS',
Richard Watson, VP Analyst, Marco Meinardi, Sr Director Analyst, 25 January 2019



Given these infrastructure as code methods are common, Google has invested in a valuable initiative to provide enterprise-ready templates as open source under the Cloud Foundations Toolkit (CFT). Sourced has had the privilege of directly contributing to this initiative which allows teams to pick up any of the **50+ templates** and drop them into their Google Foundations in a modular approach and tuning as desired. The CFT helps to ensure a reduction of upfront development when building your core foundations.

Regardless of the tooling of choice, the key to a core foundation is that it maintains **configuration management authority** across all cloud deployments. This is paramount to providing the consistency in applied controls, state management and immutability.

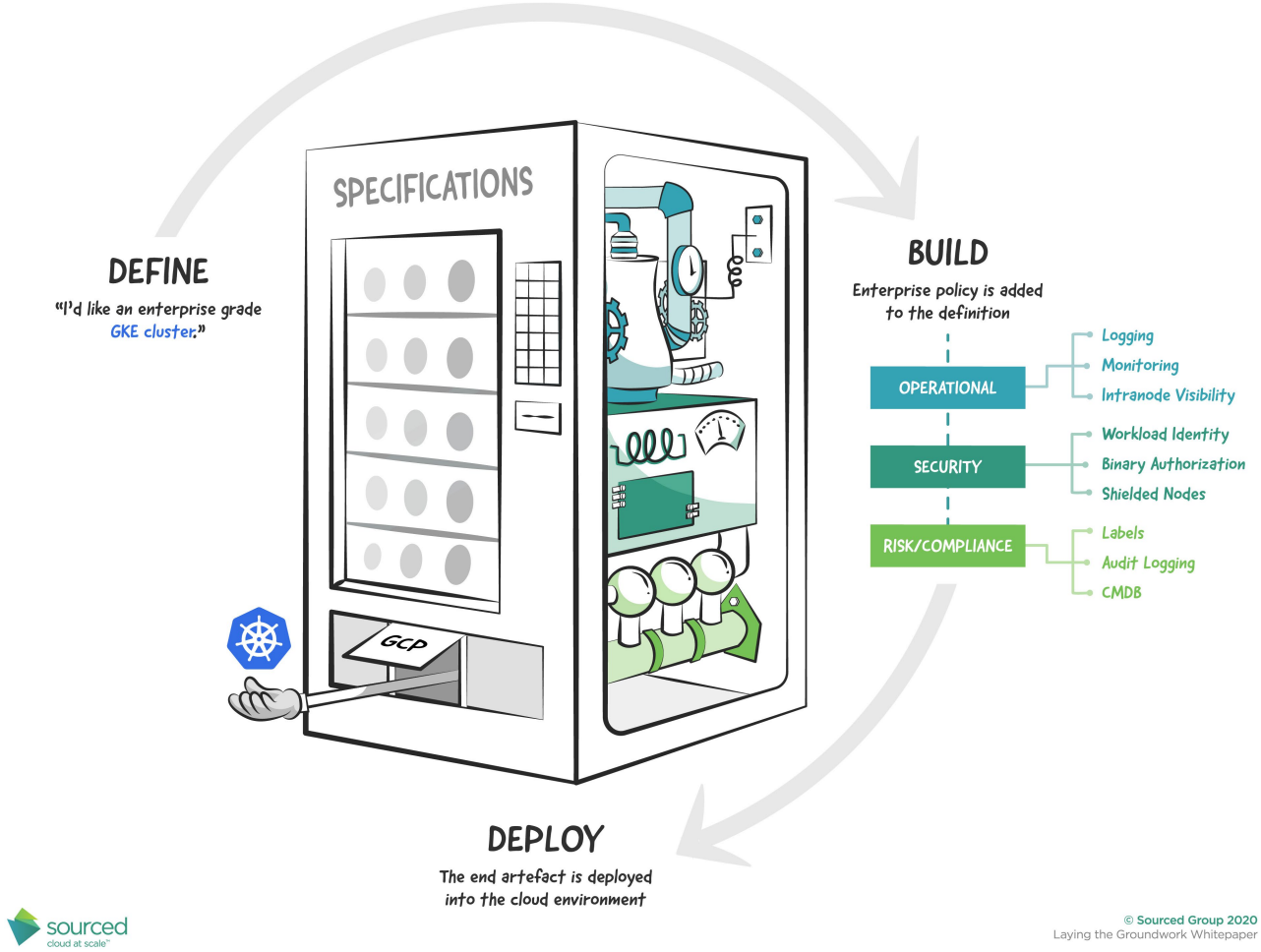


Figure 3. Opinionated pipeline concept

Moving forward, a decision must be made commensurate with the maturity of teams in public cloud across the enterprise. In line with the measured approach to cloud adoption, Sourced recommends that for teams taking their first step into cloud, a higher proportion of preventative controls to detective controls is implemented. There are two main control concepts discussed here that are contextualised to public cloud deployments:

CONTROL TYPE	DEFINITION	EXAMPLE	APPLICABILITY
Preventative	A preventative control is where the deployment automation will have embedded controls or opinions which will restrict an event from occurring **prior to the deployment taking place**.	A common example is stopping Google Cloud Storage (GCS) buckets to be deployed with access from the public internet but these controls can be as granular as restricting the use of certain node image versions when deploying in Google Kubernetes Engine (GKE). Preventative controls can also enforce operational considerations such as **frequency of backups** and deployment mechanisms such as **blue/green** or **canary releases**.	This is a highly effective approach for most teams in an enterprise, providing a stringent risk-based approach to cloud consumption which assists in providing regulators such as APRA comfort in your risk management approach.
Detective and Corrective	A detective control is where the **deployment automation is relaxed** to allow deployments to take place **without prevention.** A service is then used to scan and 'detect' any misconfigurations in the deployment triggering alerts and workflows. When a critical risk is identified, a corrective engine or human can then reach into the deployment after the fact and remediate the misconfiguration.	In the GCS example, this would allow the deployment to occur with public internet access enabled. Additional responsibility is shifted to the application teams to manage these risks but in the context of their application. This means a brochureware website does not have to maintain the same controls as a system of record transactional database. The brochureware will be allowed to maintain 'public' classified information in its public bucket, whereas applications with confidential data will trigger a corrective control.	This approach is beneficial for teams with a **high level of cloud maturity** who understand how to identify, mitigate, and manage risk when deploying in cloud. These teams will benefit from the **increased flexibility** which provides the ability to use alternative tooling preferable to their application. Vendor applications may also benefit in this consumption mode as they often are not built to support the restrictions put in place by the preventative approach.
Multi-modal	In a multi-modal approach, **both above modes are made available to application teams**. Depending on the application use case and maturity, they can choose the control option that suits them best.	In large enterprises, cloud adoption occurs at different paces. Smaller teams with fewer applications and lower cloud maturity will opt for the preventative approach as it embeds most of the organisation's 'best practice' into each deployment. Larger teams or those with higher cloud maturity will be able to take advantage of the detective and corrective approach giving them additional freedoms to meet their control objectives. This, however, places a larger portion of control responsibility with the teams requiring careful consideration.	The multi-modal approach naturally occurs as cloud maturity increases in the organisation. There is **additional engineering effort** to build and maintain both consumption modes in the multi-modal approach which is why this approach is not recommended for an organisation's initial foray into public cloud.

Over time, we witness enterprises beginning with a preventative approach then progressively moving towards enabling a detective and corrective approach as they gain maturity. Sourced observes that even in high maturity organisations, there is benefit to maintaining a preventative consumption mode given it services a larger portion of application teams as opposed to the detective and corrective consumption mode.

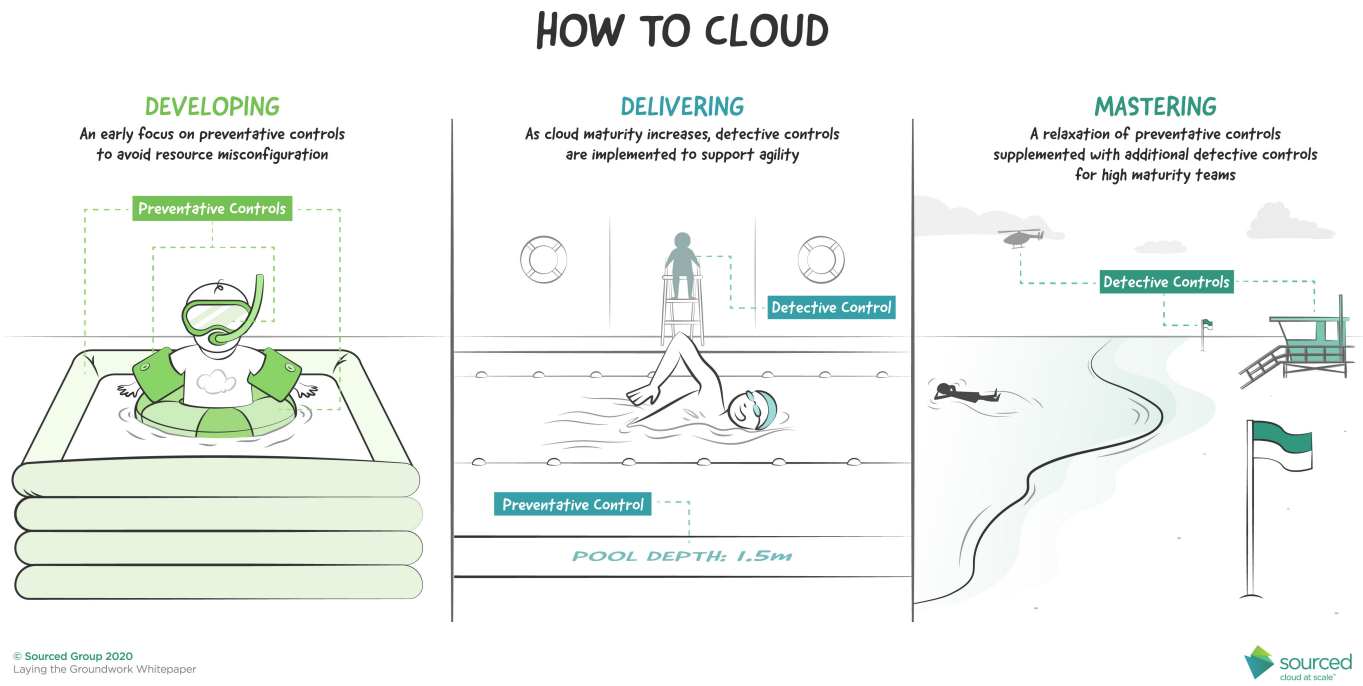


Figure 4. Control methods over time

Incremental Approach to Platform Design

Cloud-Led Business Change

Efficient technology design and delivery is only made possible if the business is structured and aligned. Sourced is not only an expert in delivering outstanding technology solutions; it also leverages ten years' experience delivering cloud in some of the world's largest banks and enterprises to execute a cloud-led business change.

As part of the Cloud at Scale™ framework, Sourced identifies, designs and executes organisational change elements to better support the new cloud operating model. A common outcome of this sees the introduction of a **Cloud Centre of Excellence** (CCoE).

The CCoE organisationally sits in the Central IT team and operates similarly to an agile product team. Creation of this team occurs before any design or build activities take place. The team ordinarily consists of a product owner, a scrum master and several cross-functional DevOps engineers. The CCoE's responsibilities begin with designing all elements of the foundational platform, soon progressing to build activities. The team will then continue to incrementally iterate on the platform, adding further features and automating further components.

As applications on-board to the platform, the CCoE provides an operational capability to support the foundational platform and shared services that applications leverage. As the CCoE matures, additional capabilities are introduced including cloud evangelism, internal consulting and training. One of the fundamental changes that this team introduces is shifting from thinking of cloud as a project to cloud as a product. A project is a temporary and unique initiative to achieve a goal whereas a product is a continual development journey that will iteratively release new features to its users. Cloud in an organisation must continually adapt as new requirements arise, new features become available and as security posture changes. To help control scope and ensure development aligns to business value, especially in the early stages of cloud adoption, Sourced recommends the use of a masthead application.

Masthead Applications

As a product delivery team, the CCoE will need to make several decisions about how and when to deliver what piece of functionality/feature. This prioritisation exercise can be difficult if the platform is built with no application in mind as features will be delivered without realised value. If there are several application team feature requests being considered, there can be a conflict of priorities resulting in inefficient delivery of features. To resolve this conflict, a masthead application should be chosen which allows the CCoE to maintain laser focus on building the most useable features first.

A masthead is an application that acts as the tip of the spear in driving requirements for the foundation platform delivery as it helps prioritise the features that are required for that application to be successful on the platform. The masthead is one of the first applications to be migrated to cloud that will help signal change in the organisation. Therefore, the application itself needs to be chosen carefully. An ideal candidate will:

- Be a known quantity in the enterprise so it can be used to evangelise the cloud and drive adoption
- Be reflective of a typical application in the enterprise to allow highest reuse of delivered features
- Be appropriately risk weighted, significant enough that the enterprise enforces rigour but not the most critical services such as core banking
- Have strong executive sponsorship and support willing to drive the migration forward
- Touch on many aspects of the enterprise to help disseminate a change in thinking as part of the migration
- Provide a sound business case grounded in either risk reduction, efficiency, agility, cost or a combination of the above
- Be internally facing to avoid the additional security complexities introduced by internet facing workloads
- If an existing application, have an appropriate architecture which does not require significant uplift to operate in a dynamic and immutable cloud world

Path to Production

Once complete, the masthead application will signal to applications within the business the readiness and availability of cloud in the organisation. The CCoE will continually iterate on the platform seeking opportunities to enhance automation, which will allow for the team's workload to remain somewhat static while application on-boarding increases.

What's Next?

The possibilities when leveraging Google Cloud are vast and Sourced has been involved in many ground-breaking initiatives for numerous global Tier-1 banks, including several industry 'firsts'. As Financial Services organisations naturally take privacy seriously, these important material initiatives have leveraged the broad set of services in Google including their key strengths in data services and containerisation.

As an example of Google's capability, Sourced created a demo application for a recent Google Cloud event. This application was developed to demonstrate ways Google Cloud can assist with data handling in a regulated enterprise.

Restrictions around data handling and secure data handling are often a regulatory requirement, however these data sets present significant value for analytics purposes. Providing a method to democratise this data for analysts, whilst still meeting regulatory obligations, can be difficult, especially with large data sets. Google, however, has an effective data suite which greatly simplifies this.

With four well-defined services, the demo application can ingest raw transaction data, locate confidential or personally identifiable information, de-identify these fields and write these transactions to a new destination for analytics purposes.

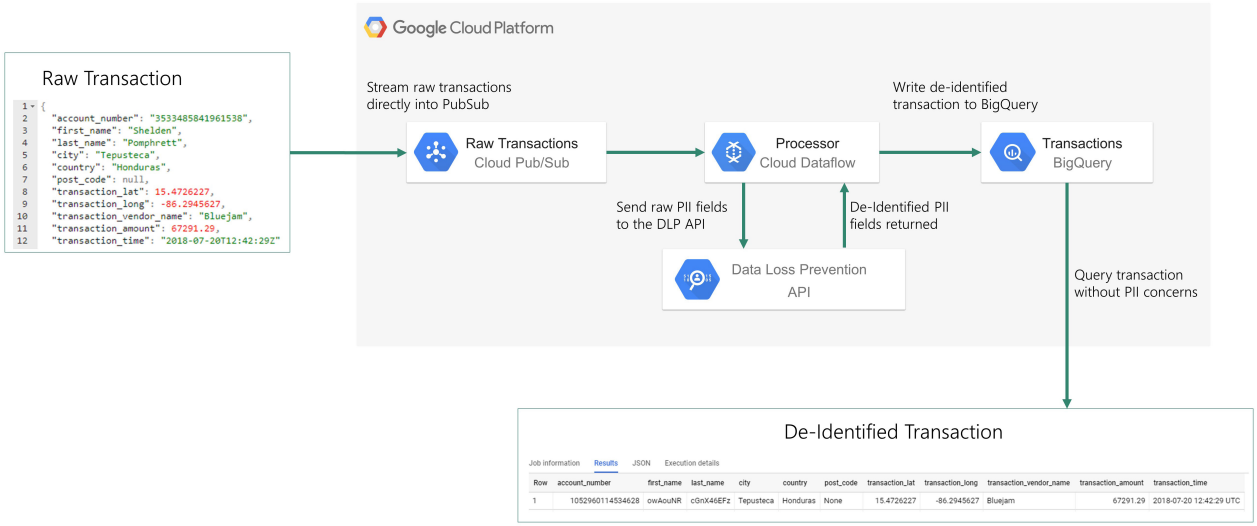


Figure 5. De-identification of confidential data from transactions

This example shows how a regulated institute like a bank, can take vast amounts of transaction data and de-identify any **Personally Identifiable Information** (PII) or confidential information. From here, this data can be shared widely in the organisation so different teams can leverage the data set to gain insights and make better business decisions.

The source code for this demo application is available here.

Conclusion

The benefits of cloud are well understood which is why you will find a published cloud strategy in most enterprises today. However, having a defined cloud strategy does not guarantee cloud transformation success. Cloud providers offer endless configurability to the multitude of features and services available, which may increase complexity for enterprises looking to adopt cloud. Without experience and guidance, organisations may make inefficient decisions, impacting their cloud adoption targets and success.

Sourced recommends structuring a cloud program that delivers a masthead application simultaneously with a scalable foundational platform. These two decisions will help align the organisation to rally around the unified goal of cloud delivery. With a common goal and a finite scope, application and Central IT teams will work more effectively, efficiently and have aligned stakeholders removing common points of friction. Organisationally, changing the way teams are structured and work is a must. Cloud introduces a fundamental shift in managing infrastructure and the foundational platform team or CCoE are at the heart of this change. Allowing these teams to operate the platform as a product will help the organisation continue to build, operate, and iterate on their cloud capability.

This paper introduces a handful of key concepts Sourced recommends when consuming cloud. Each organisation is different and there are immeasurable permutations and alterations that can be made to ensure your organisation's cloud journey is successful.

About **Sourced**

Sourced Group is a global cloud consultancy that helps enterprises make the most of cloud services with a focus on security, governance and compliance. With offices in **Australia, Canada, Singapore** and **Malaysia**, we provide professional services for securing, migrating and managing the cloud infrastructure of large enterprise customers in highly-regulated industries.

For more information, get in touch with us at **enquiries@sourcedgroup.com**

sourced
cloud at scale™

Sourced Group
sourcedgroup.com