Deloitte.

Embedding security into the public cloud DNA

Considerations for the public cloud migration journey

MAKING AN IMPACT THAT MATTERS since 1845

Contents

Securing your assets in the public cloud	2
Addressing the technology and cyber security risks associated with public cloud adoption	3
Developing a public cloud risk management strategy	5
Implementing strong controls in a cloud environment	9
Expanding the organisation's cyber security operations	12
Automation of security controls leveraging the same cloud technologies that automate technology and business functions	14
Ensuring adequate skillsets	19
Looking ahead	20
Authors and contributors	21
Key contacts	22

Securing your assets in the public cloud

The cloud is increasingly becoming the primary location for organisations to store data: most have already moved their applications to cloud platforms, and many of those that still have their data on-premise today are planning their imminent migration to cloud. Across all sectors, organisations are also modernising data platforms to leverage new-age applications and advanced analytics in tandem with their move to the cloud.

A lot of the power of the cloud comes from automation via Application Programming Interfaces (APIs) and native services offered by cloud platforms that solutions can leverage out-of-the-box via these APIs. This allows faster times-to-production with more changes and features (via continuous integration and deployment pipelines) while also optimising costs and performance.

However, rapid changes and automation bring security and compliance into greater focus. Traditionally, security has been a source of friction against business and information technology (IT) objectives. Where business and IT deploy changes and new solutions faster and more frequently with more automation, security has too often been only about checks and controls. With cloud native services and platforms being increasingly adopted, the traditional way of securing solutions is becoming increasingly ineffective.

We have seen two outcomes in such situations, neither ideal.

In one outcome, the business and the technology functions are more dominant and brush aside security concerns in favour of faster deployments and an increase in business function automation. While this allows them to move at full speed, the lack of effective security and compliance controls inevitably leads to the risk of a high impact incident.

In the second outcome, especially in regulated industries, the security and compliance functions have more dominance and can slow the changes and the speed at which new functionalities are introduced to the cloud so that the proper security checks and balances are performed. While this enables security, it can defeat the business objectives of being able to make full use of the power of the cloud and harm business competitiveness.

An organisation with a clear cloud risk management strategy–aligned with its overall cloud strategy–has a key foundation on which the objectives of its business, technology and security functions can be aligned.

Automating security alongside technology and business processes is one way of removing the friction that traditional security approaches can create. Not operating cloud assets in isolation but instead having an integrated cloud and cloud security management approach is another; it is also critical to the success of integrating security end to end. And having a talent pool that is conversant with cloud technologies and is keeping pace with the changes and new services that service providers routinely introduce is essential to ensuring that the integration and growth of the organisation in the public cloud are done correctly and securely.

We believe that organisations moving to the cloud should adopt a conscious, integrated approach right from the get-go. Such an approach would better position them to embed security into their cloud DNA at every step along the way–from conducting baseline analysis and assessing security requirements during discovery and cloud vendor selection, to determining the shared responsibility model with the cloud vendor, as well as setting up guardrails within the infrastructure, and managing DevSecOps processes.

We hope that this report will provide you with some insights into the security considerations associated with public cloud adoption, as well as the steps that you can take to ensure security by design as you lead your organisations on the cloud migration journey.

Addressing the technology and cyber security risks associated with public cloud adoption

The growing adoption of public cloud platforms, especially given the accelerated pace of digital transformation on the back of the COVID-19 pandemic, has seen a corresponding increase in the risk exposure of businesses as they move their assets to the public cloud.

Highlighted below are some of the more common key risks and the corresponding control measures that organisations should consider before adopting public cloud services.

Risk 1

The lack of cloud specific risk management strategies and governance leads to organisations leveraging their existing policies and processes which may not be cloud specific.

Develop a public cloud risk management strategy that takes into consideration the unique characteristics of public cloud services.

Risk 2

Insecure configurations and practices while leveraging cloud native platform services by the applications when they are migrated to the cloud.

Follow best practice guidelines and leverage the security services offered by the cloud platform itself in key security domains such as Identity and Access Management (IAM), cyber security, data protection, and cryptographic key management.

Risk 3

The lack of a central consolidated view (a 'single pane of glass') that covers the monitoring of all technology platforms, including multi and hybrid clouds, leads to the risk of key incidents going undetected or their impacts being underestimated.

Expand cyber security operations to include the security of public cloud workloads in combination with existing legacy/ on-premise monitoring.

Risk 4

Manually enforced security checks and controls act as a source of friction against the automation of business and technology processes in the cloud. This leads to vulnerabilities slipping past security teams who are unable to deal with the scale and speed of changes that are introduced by automation.

Automate security controls leveraging the same cloud technologies used to automate technology and business functions so as to remove friction caused by manual controls, while allowing security to keep pace with the scale and speed of deployments and changes.

Risk 5

The fast-changing nature of cloud services and the requirements of the organisation's technology and business functions to leverage new services leads to the risk that the organisation may not have sufficient and/or appropriate skillsets to understand, prevent and mitigate the myriad security impacts.

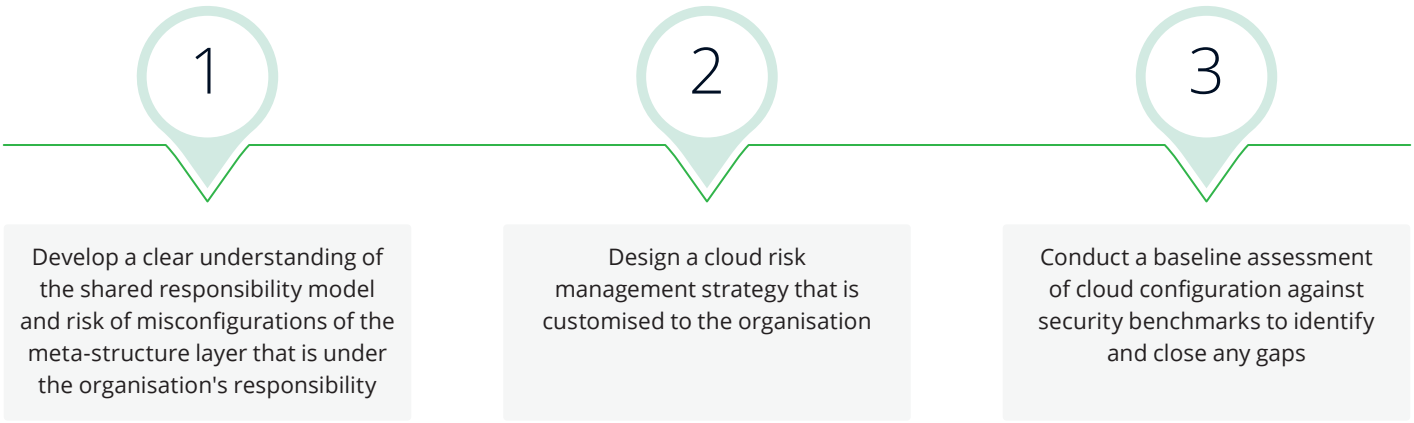
Ensure the organisation's skill and knowledge pool is of sufficient depth and breadth to ensure the appropriate understanding and management of the risks introduced by the new cloud services and capabilities being adopted.

In this report, we will take a closer look at each of the five risks and their associated control measures, and detail a series of steps that would enable organisations to overcome these security impediments by design–thereby benefiting from the advantages that public cloud platforms can offer while also mitigating the attendant technology and cyber security risks from the outset.

Developing a public cloud risk management strategy

To develop a public cloud risk management strategy, organisations first need to develop a clear understanding of the shared responsibility model and the risk of misconfigurations of the meta-structure layer they are responsible for. This will, in turn, inform the design of a cloud risk management strategy that is customised to the organisation's specific needs. Finally, to identify and close any existing gaps, organisations should conduct a baseline assessment of their cloud configuration management (see Figure 1).

Figure 1: Three steps to develop a public cloud risk management strategy



Step 1:

Develop a clear understanding of the shared responsibility model and risk of misconfigurations of the meta-structure layer the organisation is responsible for

Organisations should pay particular attention to the risks that can be introduced by public cloud platforms depending on:

- the type of cloud deployment model (i.e. whether single vendor, multi-cloud, hybrid cloud), and
- the type of cloud service models (i.e. primarily infrastructure-as-a-service, platform-as-a-service, software-as-a-service, or combinations).

Such risks can include, but are not limited to, a misinterpretation of the shared responsibility model, as well as misconfigurations of the meta-structure layer the organisation is responsible for.

As a first step to addressing such risks, organisations may conduct a maturity benchmarking exercise of their security process, tools, and technologies. This exercise should be conducted with the use of an appropriate standards-based cyber cloud framework, such as that of the National Institute of Standards and Technology (NIST) and Cloud Security Alliance (CSA). Based on the outcomes of this exercise, organisations can then design a detailed strategy roadmap to close any identified gaps and develop cloud security reference architectures and design patterns to be implemented.

To ensure that all new interfaces, including those in the meta-structure layer, are taken into consideration during the cloud security design, implementation and subsequent assessments, organisations should follow up with a threat modelling exercise. Threat modelling will yield not only a detailed analysis of the risks and threats that may exist at the cloud-enabled interfaces, but also enable the creation of security-focused test cases to help organisations ensure that their solutions are compliant and in line with leading practices.

Step 2:

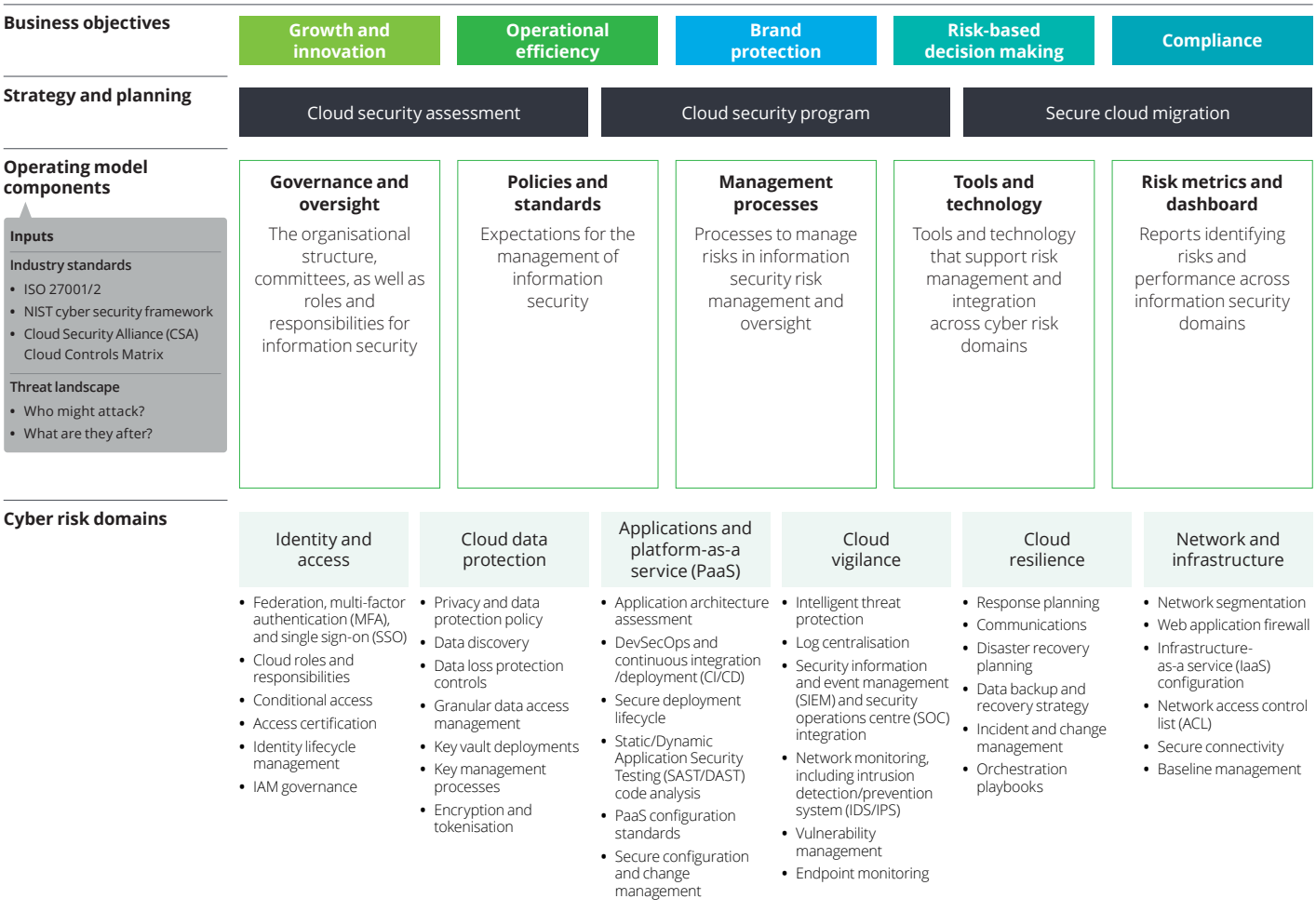
Design a cloud risk management strategy that is customised to the organisation

To develop a customised approach to managing cloud risks, organisations should leverage the use of an industry-standard cloud computing risk framework to understand their current states, and identify any gaps that may exist from people, process, and technology perspectives (see Figure 2).

Broadly, such a framework should cover all the key technology, cyber, and extended enterprise risks, including but not limited to: governance, risk management, and compliance; delivery strategy and architecture; infrastructure security; IAM; data management; business resiliency and availability; IT operations; vendor management; and business operations.

Based on better industry practices, organisations can then design customised reference architectures for their specific cloud security providers (CSPs), cloud-based solutions, and software-as-a-service (SaaS) deployments.

Figure 2: An industry-standard cloud computing risk framework



In order to customise the cloud risk strategy for an organisation, a current state assessment of the risks and gaps from an industry best practice perspective is often very useful. Many of our clients have found a detailed maturity assessment against frameworks from NIST and Cloud Security Alliance (CSA) very useful in creating their roadmaps and process improvements.

With this in mind, we have updated the cloud security areas in Deloitte's Cyber Strategy Framework (CSF) using these industry best practices. Through this the CSF provides organisations benchmarking for over 21 capabilities, 62 sub-capabilities, and 661 closed statements. This allows a comprehensive coverage of all the relevant areas to be covered in the risk assessment and benchmarking exercises.

21 cloud security capabilities: overview

Cloud governance
- Provider governance
- Compliance and audit
- Risk management
- Security governance

Devices and identity & access
- Devices
- Identity & access management

Network and infrastructure
- Platform protection
- Cloud integration
- Network protection

Data protection
- Data governance
- Cryptography
- Data loss prevention

Application security
- Secure design and development
- Secure deployment
- Secure operations

Cloud security monitoring
- Logging and monitoring
- Security configuration and detection
- Security and usage analytics

Cloud resilience
- Withstand
- Respond
- Recover

Step 3:

Conduct a baseline assessment of cloud configuration against security benchmarks to identify and close any gaps

To identify any existing security gaps, organisations should conduct a baseline assessment of their cloud configurations against security benchmarks. This assessment should cover areas such as cloud security, comprehensive container security, discovery scanning of assets, roles and responsibilities, and leading practices in account management, as well as a compliance review of policies and standards.

Typically, the outputs of such an assessment will take the form of comprehensive reports specifying the gaps and respective risk ratings, with detailed remediation recommendations. Additionally, good practices identified during the assessment should be analysed in greater detail to enable the organisation to continue to build on its strengths. Thereafter, the open risk items must be quickly remediated to create a clean baseline on which the organisation can build additional capabilities to automate cloud security for continuous compliance.

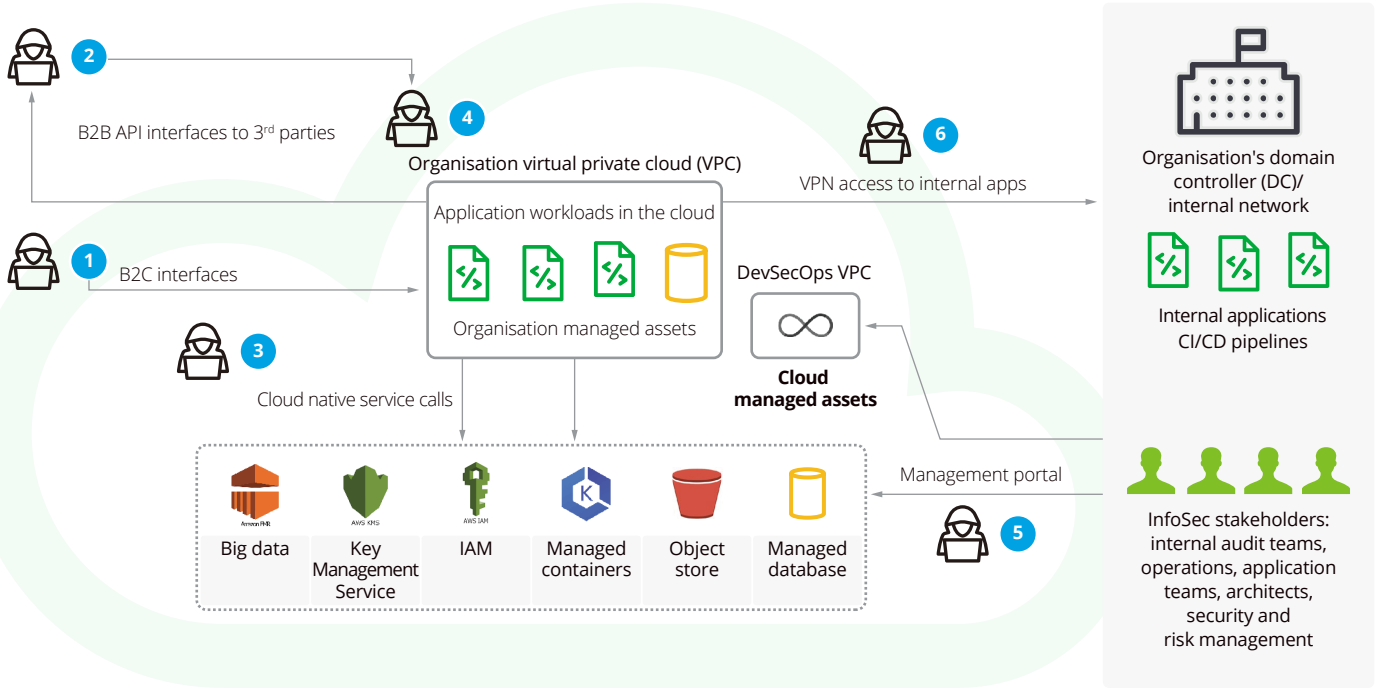
Depending on the whether the model in question is a platform-as-a-service (PaaS) or software-as-a-service (SaaS), the automation of cloud security could differ in terms of the implementation.

For a PaaS model, organisations would be able to work with their managed service provider(s) to implement cloud security posture management (CSPM) and cloud workload protection platform (CWPP) solutions.

For a SaaS model, organisations will need to pay more attention to the configuration of their applications. With some enterprise SaaS solutions today possessing more than 200 service configuration settings–not to mention third-party integration and other customisation options–this challenge is becoming increasingly complex for organisations. To flag any insecure configurations in the SaaS solution as soon as it reaches the user acceptance testing (UAT) or production phases, monitoring tools can be deployed to provide SaaS security posture management. Incident response can also be managed by integrating the detailed remediation recommendations for specific events with the organisation's IT service management (ITSM).

Unlike traditional vulnerability assessment/penetration testing (VA/PT), which only looks at the infrastructure and web/API interfaces exposed to the end customer, the cloud security assessment tests all of the areas under the customer's responsibility. It is important that these areas are tested, especially the cloud meta-structure configurations which define the security of interactions between the customer's applications and the cloud native services.

Figure 3: The many interfaces a typical cloud application is exposed to



Interfaces 1 and 2 refer to the traditional web, mobile (Business to Customer) interfaces and API (Business to Business/Customer) interfaces that are well understood and tested for security issues.

The configurations and the meta-structure of the cloud should also be considered as they can introduce additional interfaces that need to be secured.

Interface 3 deals with the integration of the cloud native services with the organisation's solutions.

Interface 4 deals with the solutions/workloads on the cloud itself (e.g. IaaS Virtual Machines (VMs) or customer managed container deployments).

Interface 5 refers to the management rules, policies, roles, and so on, which can be defined through the management portal or API-based access of the CSP.

Interface 6 refers to the secure integration of the workloads which have moved to cloud.

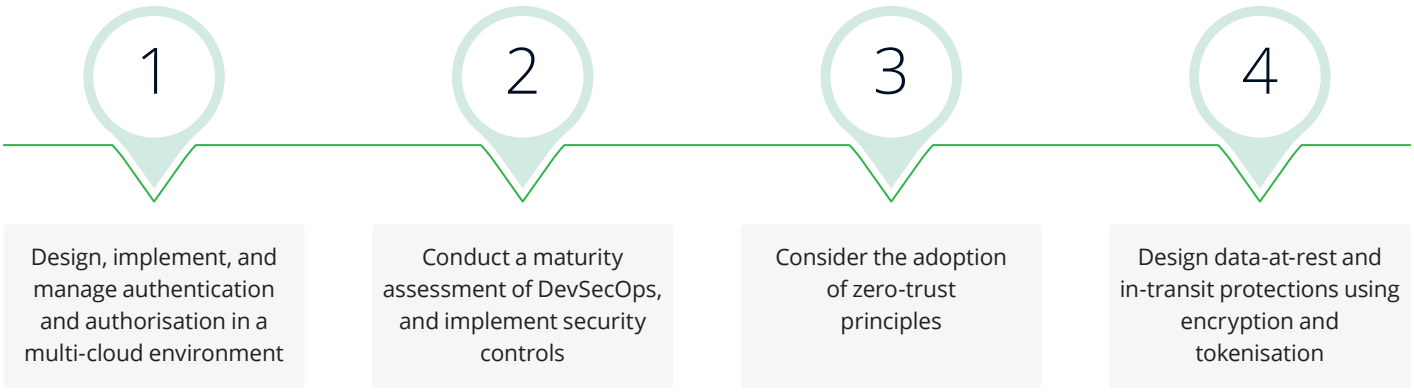
We recommend that the cloud security assessment approach complements the traditional VA/PT approach (of testing interfaces 1 and 2) by additionally testing interfaces 3 to 6 comprehensively and by using the correct tools.

From a security design and implementation perspective, we pay close attention to interfaces 3 to 6, to ensure that the solution moving to the cloud is secured from misconfiguration and cloud-meta structure related vulnerabilities.

Implementing strong controls in a cloud environment

Organisations will be expected to implement strong controls for their cloud environments particularly in areas such as IAM, cyber security, data protection, and cryptographic key management. This requires them to design, implement, and manage authentication and authorisation in a multi-cloud environment, conduct a DevSecOps maturity assessment and implement commensurate security controls, consider the adoption of zero-trust principles, as well as design data-at-rest and in-transit protections using encryption and tokenisation (see Figure 4).

Figure 4: Four steps to implement strong controls in a cloud environment



Step 1:

Design, implement, and manage authentication and authorisation in a multi-cloud environment

To design and implement enterprise-wide identity access management (IAM) and privileged access management (PAM) in the cloud, organisations should seek to leverage the use of cloud native services. These include role-based access controls, multi-factor authentication (MFA), as well as blast radius containment strategies to integrate the authentication processes of on-premise and cloud environments.

Key activities include defining users, roles, and permissions; designing authentication specifications; defining platform processes for privileged identity management (PIM) and PAM; building user profiles, user groups, and roles; implementing MFA for users; performing user mapping; developing user management processes; and developing privileged access management processes.

Step 2:

Conduct a maturity assessment of DevSecOps, and implement security controls

To ensure that security is embedded throughout their continuous integration and deployment (CI/CD) pipelines, organisations should adopt the appropriate secure software development lifecycle practices (SSDLC) for their DevOps. This approach, known as DevSecOps, is especially relevant for organisations operating in the cloud environment.

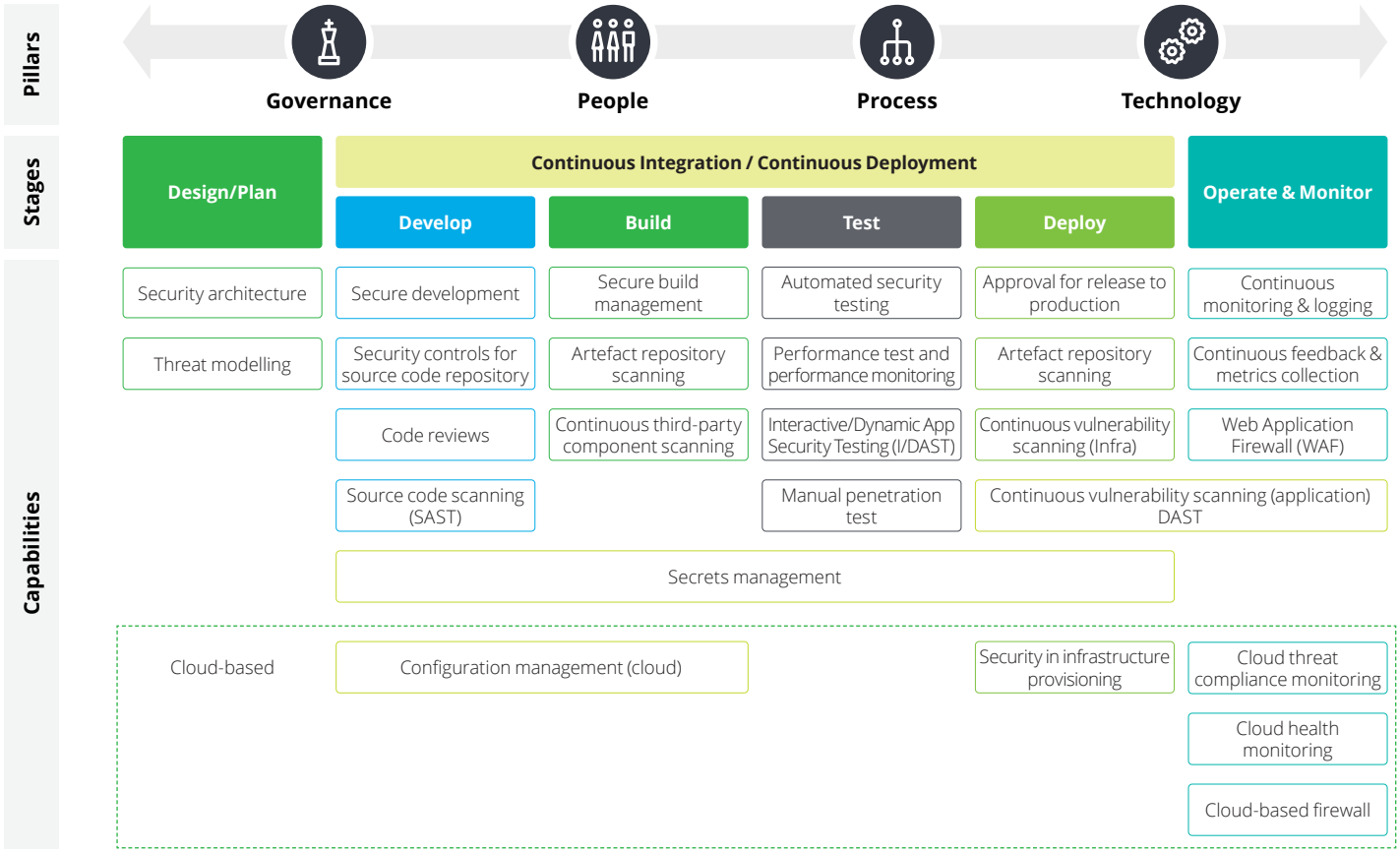
Generally speaking, DevSecOps enables organisations to embed security into their workflows rather than as a bolt-on to development. This allows developers and security professionals to have the shared goals of secure configurations being continuously monitored, remediated, and managed for cybersecurity while still driving the creation of agile, resilient solutions.

Cloud platforms typically provide their users with comprehensive sets of tools and services to accelerate the development and deployment of their software pipelines. However, this increased speed also tends to be accompanied by a corresponding increase in software vulnerabilities.

To design, implement, and operate DevSecOps pipelines securely in the cloud, organisations should therefore conduct a maturity assessment and gap analysis by benchmarking their DevSecOps processes against industry standards. Broadly, the DevSecOps framework should cover the six main stages of a pipeline–Design; Develop; Build; Test; Deploy; as well as Operate & Monitor–with the security capabilities and controls for each stage mapped to leading practices (see Figure 5).

Apart from detailed maturity assessments, the framework can also be leveraged to generate health scorecards and strategy roadmaps for an organisation's DevSecOps journey across both on-premise and cloud environments. At this juncture, security controls–such as static application security testing (SAST), dynamic application security testing (DAST), container security, and cloud compliance monitoring–should also be designed and implemented to bolster the security of the organisation's cloud applications and pipelines.

Figure 5: Six main stages in a DevSecOps pipeline



Step 3:

Consider the adoption of zero-trust principles

Organisations should consider the adoption of zero-trust principles in their overall cloud architectures. Broadly, a comprehensive adoption and implementation of zero-trust principles should entail the development of strong capabilities across five pillars: Users; Workloads; Data; Networks; and Devices. These five vertical pillars should, in turn, be supported throughout by two horizontal pillars: Telemetry & Analytics, and Automation & Orchestration (see Figure 6).

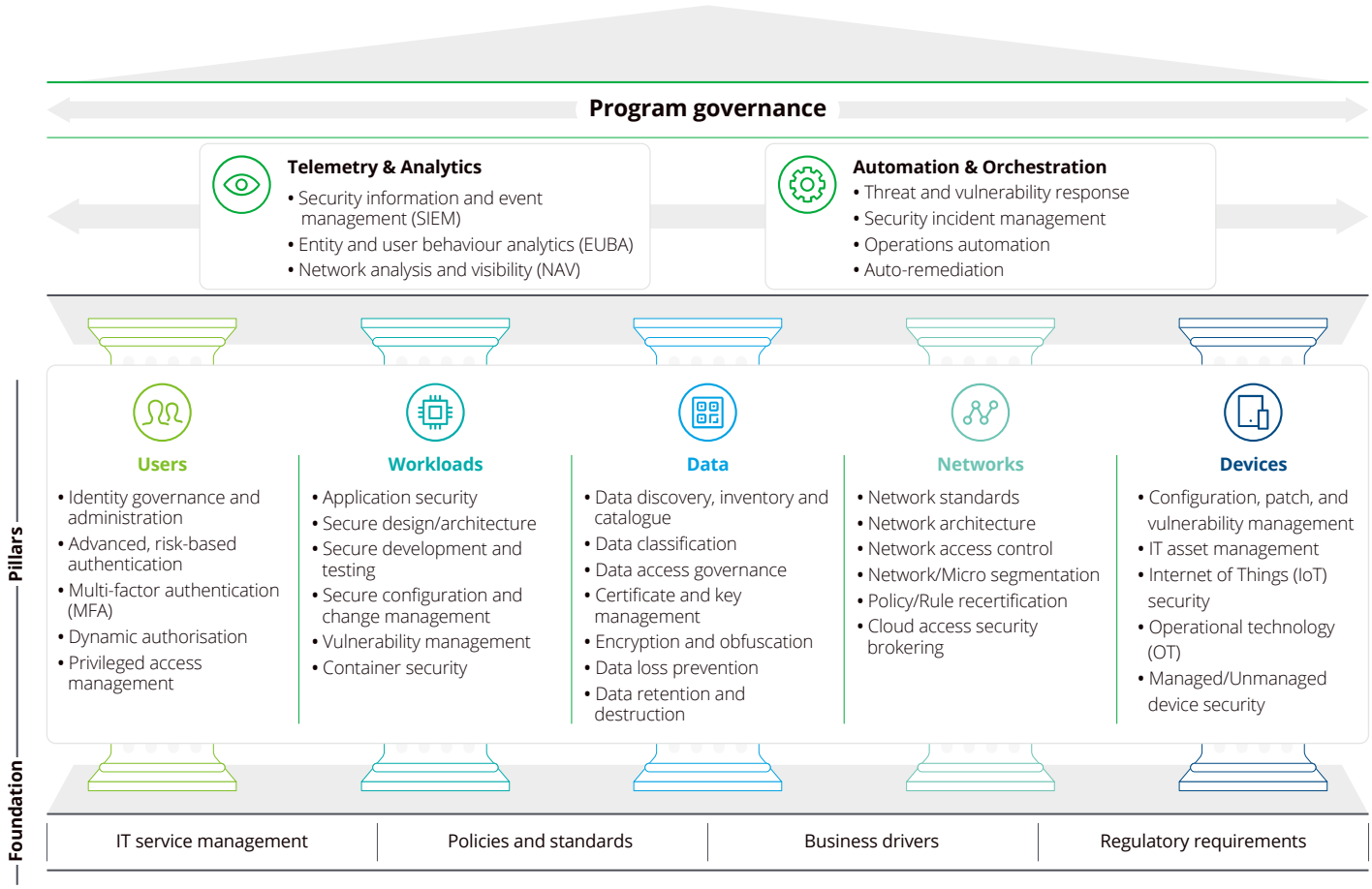
As organisations differ in their maturity levels across each pillar, a customised roadmap should be developed to cover the different zero-trust milestones. Key initial activities could include determining the zero-trust scope; establishing foundational capabilities and mapping traffic flows or application relationships; federating and centralising user management; as well as establishing data discovery, inventory, encryption, and governance. In tandem, organisations should

also begin implementing telemetry and analytics, as well as automation and orchestration, to give these capabilities a sufficient runway to mature over time.

Thereafter, organisations should implement device security services, secure their wide area networks (WANs) and the network security between cloud and on-premise environments to support cloud adoption, restrict network access using software defined perimeters (SDP), build zero-trust cloud environments, and integrate or extend cloud-native security capabilities to on-premise environments.

Once organisations have assessed and migrated their applications to a zero-trust cloud environment, they would then need to define a strategy for their applications. This could entail virtualising systems that are not suitable for the cloud, implementing micro-segmentation in the cloud enclave, and finally, further advancing their zero-trust capabilities through additional integrations and the adoption of leading capabilities across the five fundamental zero-trust pillars.

Figure 6: Comprehensive adoption of zero-trust principles across five vertical pillars



Step 4:

Design data-at-rest and in-transit protections using encryption and tokenisation

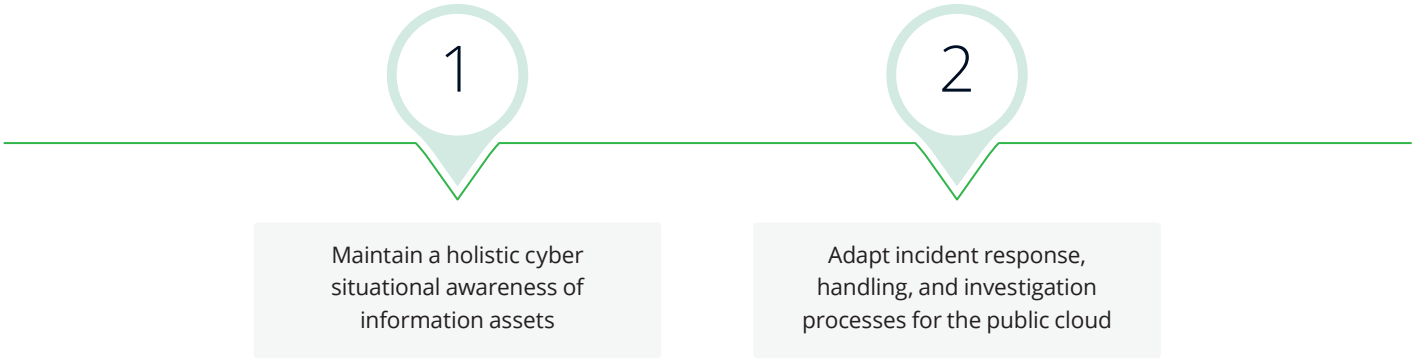
To ensure adequate and appropriate data protection coverage at all stages–from in-use to at-rest, and in-transit–organisations should adopt a cloud-native perspective in the design, implementation, and deployment of managed services for data protection.

Key focus areas here should include designing and integrating data protection on the cloud with the use of encryption, tokenisation, and masking; cryptography and key management, including managed key services offered by CSPs and dedicated cloud-hosted hardware security modules; as well as certificate management and mutual transport layer security authentication.

Expanding the organisation's cyber security operations

In order to expand their cyber security operations to include security of public cloud workloads, organisations will need to maintain a holistic cyber situational awareness of information assets, and adapt their incident response, handling, and investigation processes for the public cloud (see Figure 7).

Figure 7: Two steps to expand the organisation's cyber security operations



Step 1:

Maintain a holistic cyber situational awareness of information assets

To maintain a holistic cyber situational awareness of information assets, organisations must avoid performing the security monitoring of their cloud and on-premise assets in silos. This, however, would require adequate monitoring capabilities to cover all the new assets and technologies introduced by the cloud environment, as well as the seamless integration of logging and monitoring solutions with existing on-premise solutions to create a single, integrated security incident event monitoring (SIEM) solution.

Organisations should look at the end state of a 'single pane of glass' architecture to centralise all monitoring and logging activities. The advantages of having such a single point of access and control include a consistent view of all monitoring and logging activities, ease of managing data storage and retention, as well as centralised access control and auditing.

The caveat, however, is that organisations will need to take measures to ensure the security of data that is in transit to this central repository.

Although every CSP has its own solutions for monitoring and management of the different services, containers, applications and infrastructure, some leading practices have been observed across the board. Examples include setting up log storage to ensure compliance for log retention (as per the requirements of the organisation and the regulations they operate under), setting up log exports for security and access analytics, enabling data access audit logs to track users who have accessed data for sensitive engagements, and creating rules to filter sensitive log data to comply with relevant standards.

Step 2:

Adapt incident response, handling, and investigation processes for the public cloud

Additionally, organisations should integrate non-compliance alerts from their cloud security posture management (CSPM) and cloud workload protection platforms (CWPPs) to their ITSM tools. To achieve this, organisations will first need to baseline their cloud security controls frameworks before leveraging the capabilities of their CSPM/CWPP tools for cloud compliance monitoring, or cloud security posture management. They would then need to establish continuous cloud compliance metrics and analytics, before integrating the security alerts into their ITSM tools.

With new advances in automation of security, the CWPP and CSPM solutions have started to evolve into a cloud-native application protection platform (CNAPP), which focuses on a complete lifecycle approach to application security in the cloud, by integrating CWPP and CSPM features into one platform.

To enable near real-time auto-remediation of non-compliance–which would represent a drastic reduction in the risk window from minutes or even hours–organisations will also need to consider how they can operate their incident response processes at DevSecOps speed.

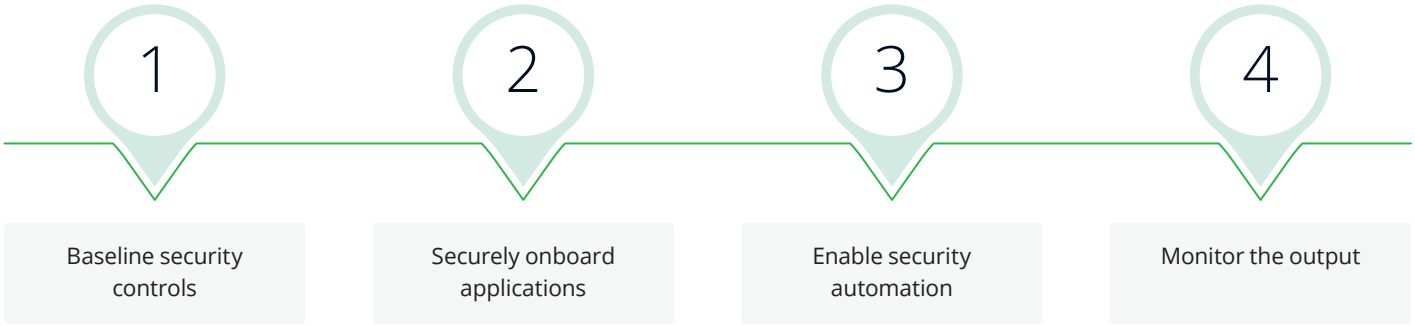
Automation of security controls leveraging the same cloud technologies that automate technology and business functions

Without the automation of security controls, security functions cannot keep pace with the speed of changes that automation brings to business and IT functions in the cloud.

The move to a cloud platform introduces risks that require a different approach from that of traditional controls. These risks include outsourcing risks, change management risks, and risks due to misunderstanding of shared responsibility.

The automation of security controls is a must when dealing with such risks (see Figure 8).

Figure 8: Four steps to introducing automation of security controls



Step 1:

Baseline the security controls

Before automating security controls, a baseline must be established to give an objective definition of what is acceptable (from a security perspective) and what is considered insecure. The 'what' may be security and technology configurations of the applications and their integration with the cloud platform services.

This is achieved by having clear policies and standards, with an evolving library of security patterns mapped to these. The application users can then reference the security patterns to understand what 'good' looks like when they are getting their applications to be cloud-secure.

Step 2:

Onboard the applications

This may be done via checklists for manual reviews, one time security assessments, point-in-time automated scans, and so on, to get a picture of the current state of the security controls.

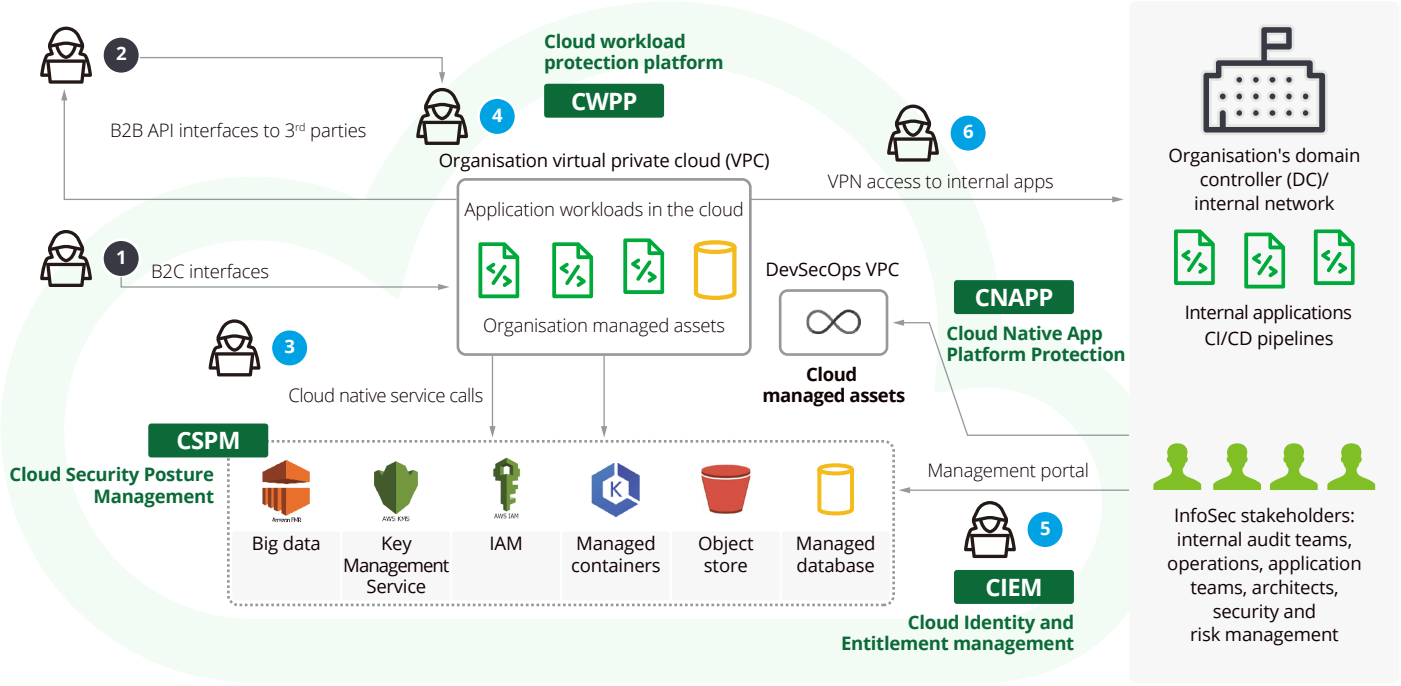
The application then goes through a process of hardening where the gaps noted are fixed so that the security automation can start from a clean state.

The risk of not doing the onboarding correctly creates a scenario where the security automation generates numerous issues which can be overwhelming to analyse manually.

Step 3:

Enable security automation

Figure 9: Security automation in the cloud



There are multiple areas where security can be automated. Below are some of examples:

- Cloud security posture management (CSPM): for automating the identification (and also remediation in some cases) of security misconfiguration in the cloud services consumed by the application workloads.
- Cloud workload protection platform (CWPP): for protecting server workloads (e.g., containers) both statically (e.g. via scanning when the container images are being built in the pipeline) and dynamically at runtime (e.g. CWPP monitors the runtime services and traffic for anomalies and threat patterns when the containers have been spun up).
- Cloud infrastructure entitlement management (CIEM): for managing the identities and access entitlements of various principals (users, services, roles etc.) in cloud and multi-cloud environments.
- Cloud native application platform protection (CNAPP): for combining the elements of all the three technologies above to provide a consistent security approach and posture from development to build to deploy/operate in the cloud.
- Infrastructure as code (IAC) security: Securing the IAC via secure scanning/secure deployments in line with the DevSecOps processes is critical to eliminate misconfigurations when deploying infrastructure in the cloud.

Organisations may adopt different strategies for choosing the appropriate technology and products to implement the above examples. There are various third-party off-the-shelf products as well as cloud native services that achieve the automation of security, and organisations may choose the solutions that fit their needs after duly evaluating the options.

Step 4:

Continuously monitor the output of automation

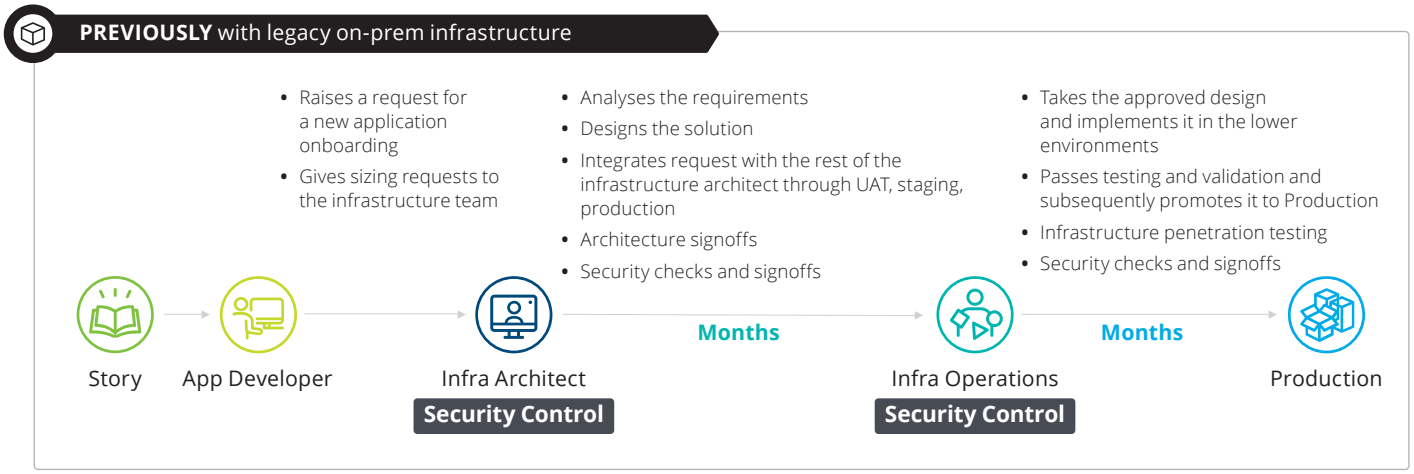
A critical component to automating the security controls would be to monitor the output of the actions that the automation has resulted in.

The output of the tools listed above may be piped into the SIEM solution that the organisation uses, so as to alert the operations teams to take appropriate actions when security events are detected by the automation.

An example

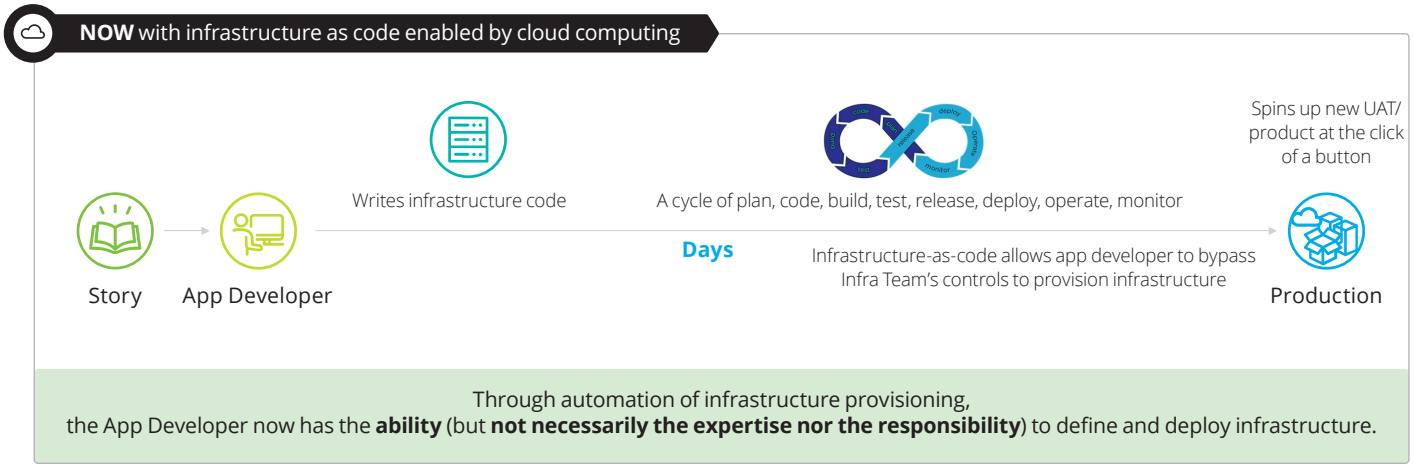
Consider the impact of infrastructure as code (IAC) to security. This feature of the virtualisation technology implicit in cloud platforms allows infrastructure to be defined in scripting languages and submitted to the cloud platform's APIs for modifying infrastructure on cloud on demand.

Figure 10: Legacy infrastructure deployment



As illustrated by the figure above, setting up new infrastructure environments could take months for a large enterprise.

Figure 11: Infrastructure deployment using infrastructure as code in the cloud



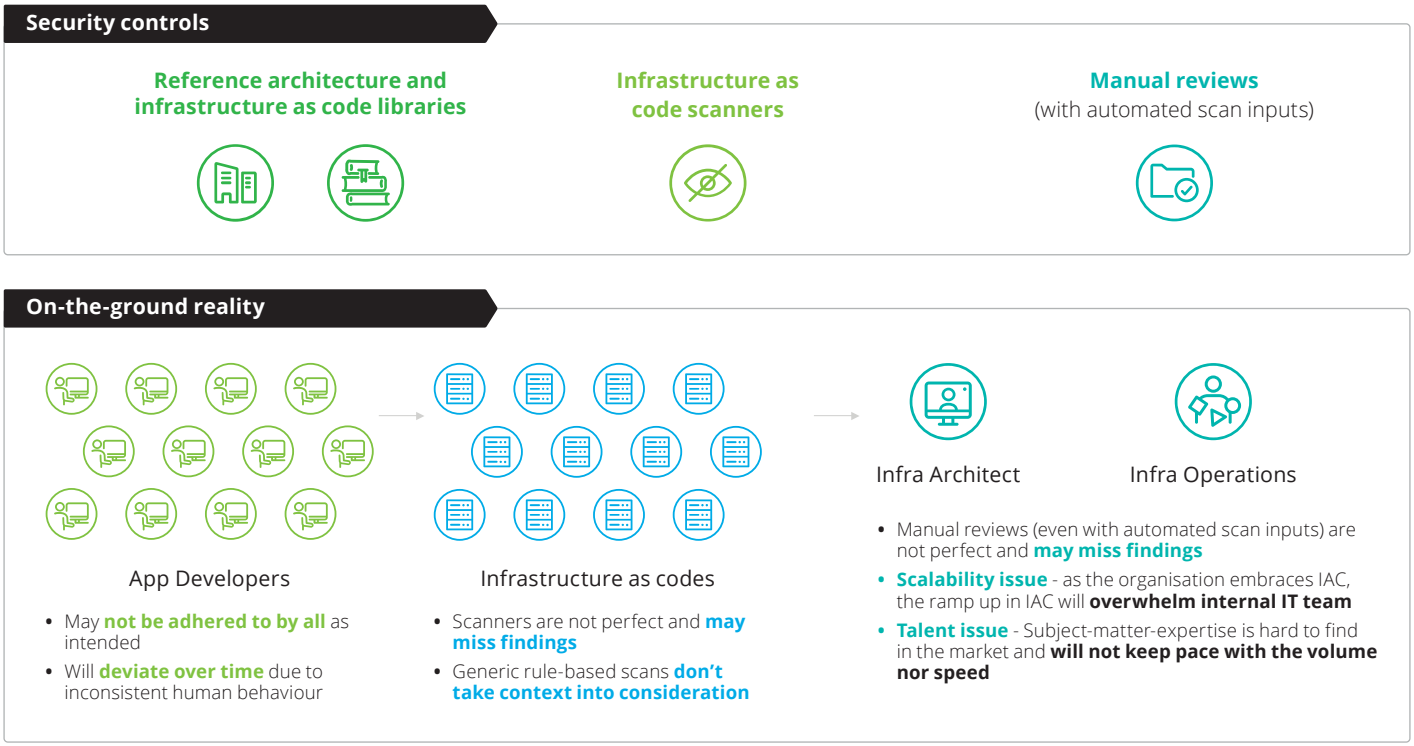
With IAC, the activity which used to take months for an enterprise is now reduced to not even a few weeks or days, but to mere hours. But this kind of leap from automation technology can have grave implications for security, the primary risk being that **the infrastructure configuration may not be secure, compliant with existing company security policies, or well-designed**.

The organisation may attempt to deal with this using its existing security controls and governance setup. It may mandate that:

- Every IAC change goes through a subject matter expert review
- Reference architectures and templates for IAC are provided
- Scanning of the IAC happens in an automated manner in the DevSecOps pipelines.

However, the realities of operating at scale and the limitations of manual controls in the existing review process (for example, the review of changes by subject matter experts) may render this approach ineffective in the long run. Such a situation is especially likely to happen when an institution starts making full use of the power of automation and scale of IAC features to aggressively push multiple changes and solutions to their cloud based solutions.

Figure 12: Typical security controls for infrastructure as code

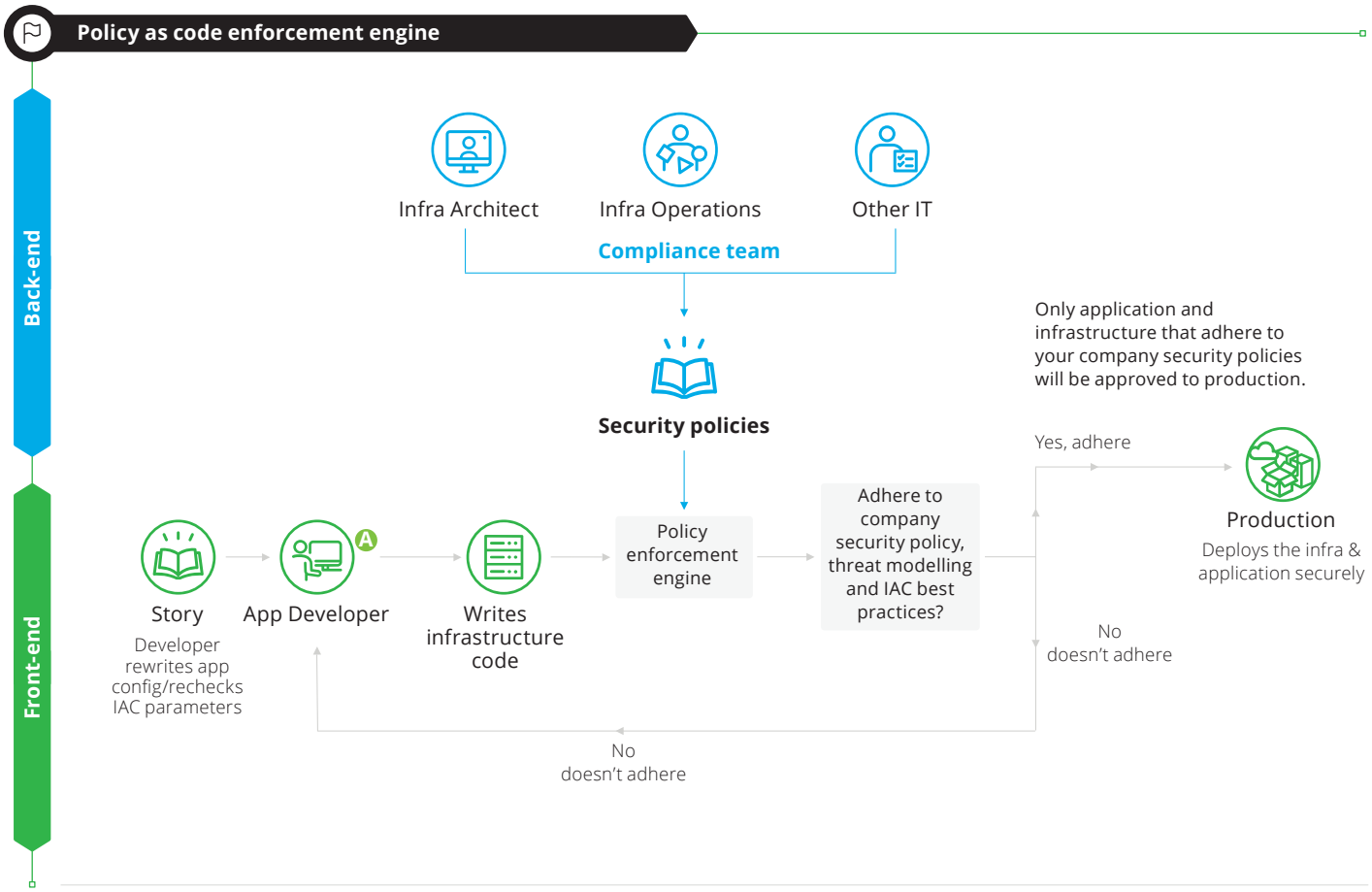


In order to solve this issue, one approach would be to enforce a policy engine that replaces human checks in favour of automating security controls in the IAC itself.

By passing developer code to such a service, IAC best practices and design patterns can be embedded in the IAC directly to make sure the security aspects of the IAC are not left to the developers.

Such a 'policy as code' approach would help ensure the organisation's infrastructure is compliant with its security policies and that security enforcement is automated. This would remove the bottleneck of manual checking and approvals that can cause friction against the automation offered by IAC while still ensuring policies are complied with.

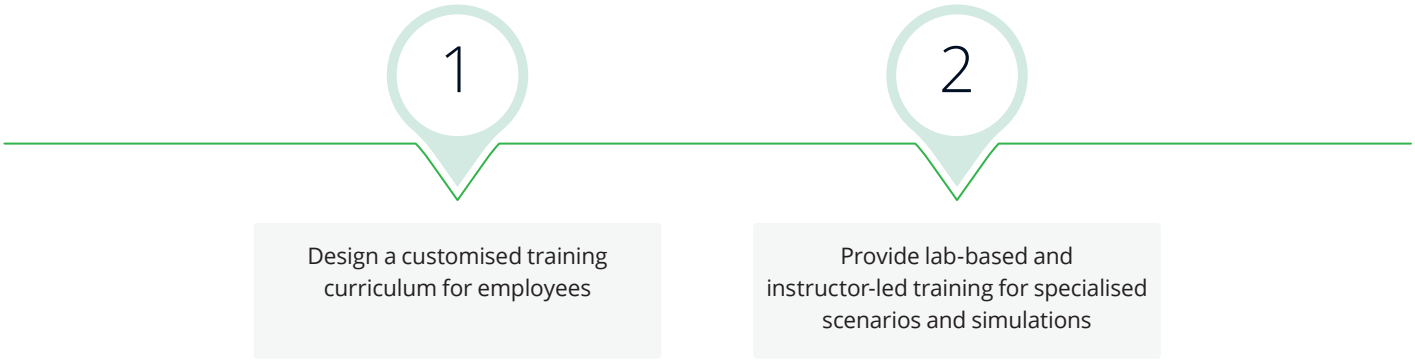
Figure 13: Policy as code



Ensuring adequate skillsets

To ensure that organisations possess the appropriate skillsets to manage public cloud workloads and risks, they should design customised training curriculum for their employees to cover cloud and technology-related topics. Lab-based and instructor-led training may also be useful in equipping employees with the necessary skills to manage specific scenarios.

Figure 14: Two steps to ensure adequate skills



Step 1:

Design a customised training curriculum for employees

To bolster cloud and technology-related skills across the organisation, organisations could benefit from the design of a customised training curriculum for their employees. For frontline IT teams in particular, a simulated cyber training curriculum could be beneficial in helping them to learn to respond to real-world cyber attacks.

By providing a hyper-realistic, virtual environment–one that closely mimics the organisation's real environment–such a curriculum could enable application developers to experience realistic, real-time attacks on their applications, and develop the necessary security acumen and cross-team communication skills that they will need to effectively protect their organisation's infrastructure.

Other training areas could also include cyber cloud topics such as continuous compliance, security monitoring, and security configuration; DevSecOps topics, such as maturity planning, roadmaps and SAST/DAST; as well as zero-trust topics, including roadmaps to zero-trust maturity and the design of zero-trust reference architecture.

Step 2:

Provide lab-based and instructor-led training for specialised scenarios and simulations

Often, specific situations that an organisation can face may also necessitate specialised training sessions. Examples include the need for IT and security teams to increase their familiarity with new platforms that the organisation is looking to migrate to, or the need to resolve certain specific issues that exist within the organisation.

Ideally, such training activities should be conducted through labs or other instructor-led demonstrations to enable employees to gain more hands-on experience. In certain instances, it may also be possible to combine other organisational goals with the training curriculum, for example by facilitating the employees' creation of a minimum viable product or some form of prototype as part of a training session.

Looking ahead

The threat landscape is continuously evolving with malicious actors employing new cyberattack tactics. Several of these tactics utilise the very same technologies that are being used to drive business and technology objectives, such as artificial intelligence and cloud based automation. The risks from these threats are amplified with the fast pace at which organisations are adopting cloud services, and the pace at which these services are evolving as well.

As we have reiterated throughout this report, staying one step ahead of these threats will require organisations to adopt a conscious, integrated approach to security by design from the get-go.

Nevertheless, we are cognisant that even the most well-designed integrated strategies can fail if they are not implemented by an integrated team.

In many organisations, cyber security teams tend to be siloed from the rest of the organisation, often with minimal or incomplete transparency. As organisations continue to accelerate their cloud migration journeys, this issue will likely only grow–and perhaps even cause the migration process itself to become jeopardised.

What is thus urgently needed is for cloud and cyber teams to come together under a shared operating model–one that takes into consideration the various aspects of the cloud migration journey, including but not limited to the talent operating model, DevSecOps, and microservices.

Apart from enabling higher levels of collaboration, coordination, and implementation across controls, such a shared operating model could also ensure that risk management, compliance, and other security practices are built into the IT infrastructure layer from the very beginning, thereby allowing organisations to focus their efforts on more value-adding activities such as leveraging the cloud platform for enhanced business performance and improved customer experiences.

Ultimately, the cloud migration process presents organisations with both the opportunity and necessity to rethink their security models, tools, and capabilities. As they embark on this journey, now is the time for organisations to re-examine their controls frameworks, enhancing them with a more integrated cloud and cyber approach, and building secure cloud landing zones that will eventually form the basis of their operating models for a long time to come.

Authors and contributors

Author

Amol Dabholkar
Asia Pacific Cyber Cloud leader
+65 6216 3115
adabholkar@deloitte.com

Key contributors

Karen Grieve
Director
kagrieve@deloitte.com.au

Ho Kyoo Hahn
Director
hhahn@deloitte.com

David Hawks
Partner
dhawks@deloitte.com.au

Tomoki Ishii
Managing Director
tomoki.ishii@tohmatsu.co.jp

Eric Leo
Director
eleo@deloitte.com.au

Max Y Lin
Partner
maxylin@deloitte.com.tw

Joanne Lu
Partner
joannelu@deloitte.co.nz

Rahul Mengale
Director
rmengale@deloitte.com

Tonny Xue
Partner
tonxue@deloitte.com.cn

Key contacts

Amol Dabholkar
Asia Pacific Cyber Cloud leader
+65 6216 3115
adabholkar@deloitte.com

Ian Blatchford
Asia Pacific Cyber leader
+61 2 9322 5735
iblatchford@deloitte.com.au

Australia

David Hawks
Partner
+61 400 032 693
dhawks@deloitte.com.au

Chinese Mainland/Hong Kong SAR

Tonny Xue
Partner
+86 10 8520 7315
tonxue@deloitte.com.cn

Japan

Tomoki Ishii
Managing Director
+81 3 6213 1900
tomoki.ishii@tohmatsu.co.jp

Korea

Ho Kyoo Hahn
Director
+82 2 6676 1922
hhahn@deloitte.com

New Zealand

Joanne Lu
Partner
+64 4470 3651
joannelu@deloitte.co.nz

South Asia

Chintan Matalia
Partner
+91 22 6122 8010
chmatalia@deloitte.com

Southeast Asia

Amol Dabholkar
Partner
+65 6216 3115
adabholkar@deloitte.com

Taiwan

Max Y Lin
Partner
+886 (2) 2725 9988 (ext. 7779)
maxylin@deloitte.com.tw

Designed by CoRe Creative Services. RITM1298919

This is printed on environmentally friendly paper