Security by Design practices and challenges faced by organisations in an Agile Public Cloud world

Gopal Krishnan, Ramshanker

Security by Design practices and challenges faced by organisations in an Agile Public Cloud world

Name: Ramshanker Gopal Krishnan

1st Chair: Els De Busser

2nd Chair: Cristina Del Real

Course: Executive Masters in Cybersecurity

Date: 15/01/2024

Contents

Abstract

Background: Public Cloud usage is becoming mainstream with organisations increasing their dependence on Cloud technologies to build their digital platforms and services. Organisations are expected to spend over half a Trillion US dollars by 2023 in Cloud services spanning across workloads and types of businesses from large enterprises to small and medium sized businesses. As organisations transform to becoming more digital, there is an increasing need for speed to stay competitive in the market. This has led to them to adopt Agile methodologies to develop their digital platforms and solutions. These platforms and solutions make up a critical part of cyberspace and need to be secured. Adopting Cloud technologies and Agile methodology requires cultural and behavioural changes within organizations, including but not limited to how decisions are made, how risks are assessed, and most importantly skilling and readiness of employees.

Objectives: The aim of the study is to observe security by design (SbD) practices from experts and practitioners, who build Cloud based solutions using Agile delivery methodologies. Furthermore, we seek to explore the challenges they face implementing SbD practices when building Cloud based solutions.

Method: We use a qualitative approach using semi-structured interviews of 16 practitioners as our primary data collection method. We analyse the results of the interviews using a codebook created to identify themes, practices and challenges.

Discussions: The fast paced and changing Cloud environment presents some contradictions, with opportunities and challenges that influence SbD practices. From our discussions with interview participants, we observed nine practices, and four other factors that influences these practices. Furthermore, we observed various challenges they faced across (i) Cloud operating model, (ii) people and organisation, (iii) process and methods, (iv) threat landscape and, (v) tools and technologies. Organisations look to proactively move security related activities early in their engineering cycles. This is often referred to as “shifting left”. Ability to effectively “shift left” depends on driving the right accountabilities, investing in automation, addressing the security skills gap, and creating a security mindset within the organisation.

1 INTRODUCTION

Software and digitalisation are playing a crucial role in the evolution of cyberspace, as organisations and businesses increasingly leverage innovative technology to transform their business and create new digital experiences for their customers. Public Cloud (referred to as Cloud going forward) has enabled the widespread availability of storage, network, and computing on demand to help fuel Digital Transformation initiatives [1]. Cloud services spending is expected to reach 591 billion US Dollars in 2023 [2]. Flexera in their 2023 *State of the Cloud report* stated that Cloud adoption is becoming more mainstream with 84% of their respondents reported heavy or moderate usage [3]. More than 50% of the workloads are reported to be already migrated to the Cloud and that number is even higher at 67% for small and medium business. All this indicates that Cloud technologies are here to stay with a widespread adoption across businesses.

According to McKinsey, key benefits of adopting cloud are reduced time to market through increased automation and innovation, built on the hundreds of services and the ecosystems offered by the cloud service providers (CSPs) [1]. Capturing the value of Cloud requires organisations to reimagine their operating model, specifically around skills they need and processes that support agility such as Agile development methodologies (ADM): a methodology for software development that emphasizes iterative, incremental, and collaborative processes, such as Scrum[1], Kanban[2], or DevOps[3]. The model focuses on delivering solutions with high levels of agility achieved through deep collaboration between business and software engineering teams.

As digitalization becomes prevalent, the impact of security breaches is far-reaching irrespective of whether the source of the breach is intentional or accidental. As more sensitive data is moved to the Cloud, nearly 40% of the businesses experienced a data breach in the Cloud in 2022[4]. Janankhani et al., (2009) argues the need to factor security

[1] Scrum helps people and teams deliver value incrementally in a collaborative way. As an agile framework, Scrum provides just enough structure for people and teams to integrate into how they work, while adding the right practices to optimize for their specific needs. (Source: www.scrum.org)

[2] Kanban is a Japanese term that means signboard or billboard. An industrial engineer named Taiichi Ohno developed Kanban at Toyota Motor Corporation to improve manufacturing efficiency. Although Kanban was created for manufacturing, software development shares many of the same goals, such as increasing flow and throughput. (Source: https://learn.microsoft.com/en-us/devops/plan/what-is-kanban)

[3] DevOps combines development (Dev) and operations (Ops) to unite people, process, and technology in application planning, development, delivery, and operations. DevOps enables coordination and collaboration between formerly siloed roles like development, IT operations, quality engineering, and security. (https://learn.microsoft.com/en-us/devops/what-is-devops)

considerations both from a technical and social perspective in the initial stages of the solution development cycle [5]. The development process should facilitate deep understanding of the technical and social challenges and enable developers with the knowledge and tools to address these issues. Furthermore, it should provide the end user the required education and change management. Integrating security engineering with ADM is a challenge, as they are considered different paths with a lack of an aligned methodology, that handled security as a specialized requirement rather than treating it as core. Moreover, a lack of knowledge sharing among the two separate security engineering and software development communities could manifest in security requirements not being handled appropriately. Furthermore, specifying security requirements precisely for a complex system such as the Cloud, can be even more challenging given the emergence and innovative properties these systems exhibit.

Security by design focuses on addressing security in early phases of the software development lifecycle (SDLC) [6]. While there are popular frameworks such as the Microsoft Security Development Lifecycle (SDL) [7] and Comprehensive, Lightweight Application Security Process (CLASP) [8], that attempt to operationalize these principles, organisations could face challenges implementing them due to the high level, and abstract nature of the guidelines, especially for Cloud specific aspects.

I have been working for more than two decades with Microsoft, a leader in the Cloud space [9], and have led teams that deliver transformational solutions to our customers, across sectors. We have experienced the cultural and behavioural changes required to adopt Cloud and this is particularly true when you apply ADM to reduce time to market of Cloud solutions for our customers. These changes impact how decisions are made, including but not limited to architecture trade offs, design, training, investments and capability building. While Microsoft has the motivation and the means in terms of financials and talent pool to invest in transformation, the same cannot be assumed for all the other companies who grapple with different pressures such as competition, time to market pressures and skills shortages. Our motivation for this thesis is to observe Security by Design (SbD) practices in the context of Cloud and to better understand the challenges teams face with SbD practices when they build Cloud solutions in an Agile context, through the lens of experts and practitioners.

We use a qualitative approach of semi-structured interviews as our data collection method, to answer our two main research questions

RQ1: What are the SbD practices that organisations implement in developing Public Cloud solutions using ADM?

RQ2: What are the barriers and challenges that prevent effective implementation of SbD practices in developing Public Cloud based solutions leveraging ADM?

The rest of this Masters thesis is organised into Related work where we highlight some of the key developments in Cloud, ADM and SbD. In the Methods section, we discuss how we approach our semi-structured interviews, including participant recruitment. Following, in the Results section, we present our findings from the interviews. Next, in the Discussions section, we discuss the results from a technical, organisational and behavioural perspective. Furthermore, we discuss limitations of this research and potential for future research.

2 Related work

2.1.1 Cloud and Security

Cloud computing has been fast emerging as a technology that is enabling business to transform digitally [10]. Cloud leverages the internet to provide fundamental services like compute, network, and storage to higher order services such as authentication, authorization, database, web services as well as advanced services such as Internet of Things (IoT), Artificial Intelligence (AI) and blockchain. These services as illustrated in figure 1 are delivered through three primary service models (i) Infrastructure as a Service (IaaS), (ii) Platform as a Service (PaaS) and (iii) Software as a Service (SaaS). The fundamental characteristics of the Cloud is that of a shared service model[4], providing elastic scale and pay-per use. Traditionally, organisations that relied on technology had to build and manage their own IT infrastructure. This required high upfront capital expenditure (CapEx) to be spent on things like data centers, servers, and network equipment. With Cloud providing on-demand, pay-per-use model, organisations can treat it more like operating expense (OpEx) and not have to worry about utilisation of their infrastructure. In theory, this allows them to focus on their core business and treat technology as an enabler, leaving the management of these technologies to Cloud Service Providers (CSPs).

[4] Services shared by multiples customers (or tenants) but hosted on a shared infrastructure through virtualization technologies.

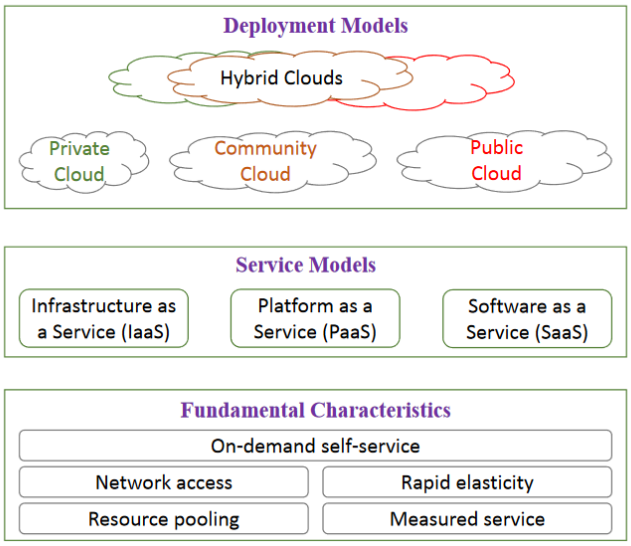


Figure 1: Cloud computing fundamental characteristics, service models, and deployment models [10]. Source: Surbiryala et al, (2019)

Application architectures need to evolve to be able to leverage the benefits of the Cloud as outlined in Figure 2. According to Microsoft, which is one of the leading Cloud providers, "The cloud is changing how applications are designed and secured. Instead of monoliths, applications are decomposed into smaller, decentralized services. These services communicate through APIs or by using asynchronous messaging or eventing" [11].

Traditional on-premises	Modern cloud
Monolithic	Decomposed
Designed for predictable scalability	Designed for elastic scale
Relational database	Polyglot persistence (mix of storage technologies)
Synchronized processing	Asynchronous processing
Design to avoid failures (MTBF)	Design for failure (MTTR)
Occasional large updates	Frequent small updates
Manual management	Automated self-management
Snowflake servers	Immutable infrastructure

Figure 2: Cloud based solutions approach. Source: Microsoft Azure application architecture fundamentals[5]

New architectural styles are emerging such as N-tier, Microservices, Event driven, Big Compute, Big Data. These along with the distributed, virtualized, multi-tenancy and internet

[5] https://learn.microsoft.com/en-us/azure/architecture/guide/

facing attributes presents a set of Cloud specific security issues [12]. Cloud security issues can be classified under policies, user oriented security, Data, Application and Network as illustrated in Figure 3 [13]. Data related threats get particular prominence due to the high risk of compromise, leakage, and unauthorized access due to the inherent nature of Cloud architecture [14].

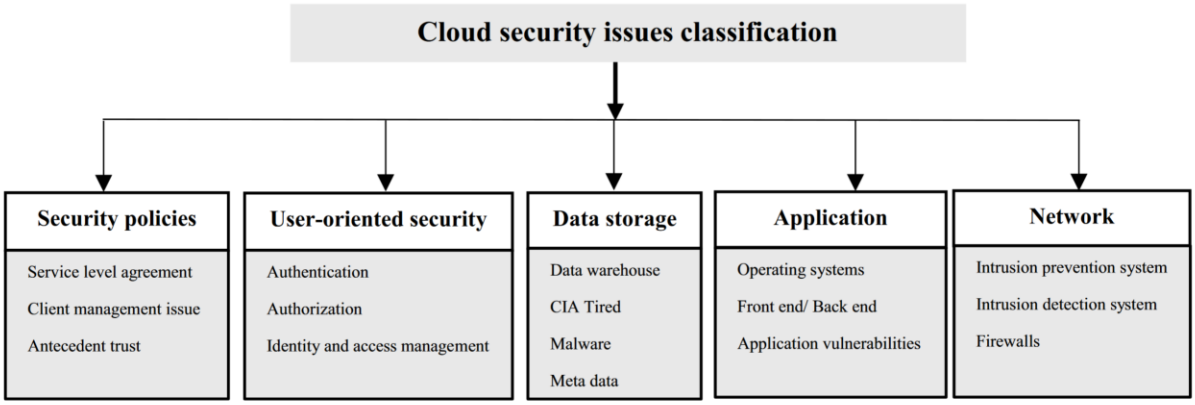


Figure 3: Cloud security issues – categories [13]. Source: Tabrizchi et al., (2020)

One of the key success measures in adopting Cloud is speed of delivering new products and services (Figure 4). While Cloud technologies provide the underlying platform to enable this through easy on-demand provisioning of infrastructure and services available over the internet such as Web API (Application programming interface), organisations prioritize agile practices in order “to accelerate time to market” [15].

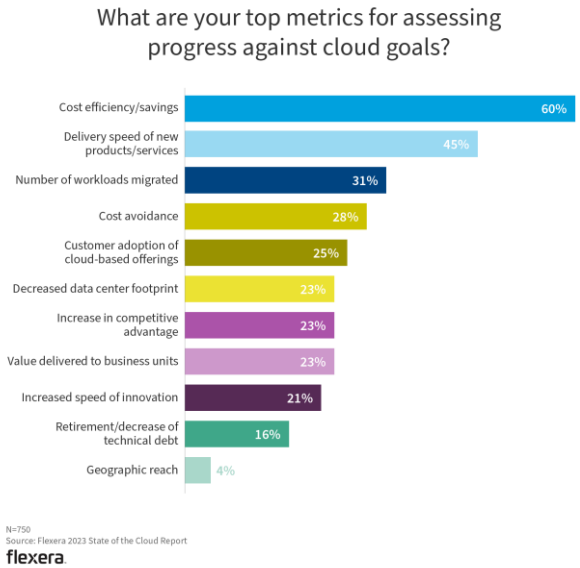


Figure 4: Cloud goals (source: www.flexera.com)

2.1.2 Agile and Security

As organisations continue to transform digitally, they depend on platforms built by software development teams, that are purpose built either inhouse or otherwise. Software development teams work in an ecosystem that requires a collaborative approach with key suppliers such as Cloud providers, hardware vendors and Independent Software Vendors (ISVs) [16]. Failing to meet user needs and requirements has been one of the biggest issues with traditional approaches of delivering these platforms [17]. ADM has been widely adopted as a solution to address these challenges and reduce time-to-market by focusing less on heavy front-end planning and documentation compared to traditional waterfall approaches, while adapting dynamically to changing requirements in shorter cycles called "sprints" through self managed and self organised teams. ADM has gained traction since it was formally backed by leading members of the development community in 2001 with the publication of the Agile Manifesto [18]. The *State of Agile* report which tracks ADM adoption trends noted in their 2021 report that there has been a significant increase in adoption with over 86% of the respondents reported using Agile methodologies (Figure 5) [19] . A study of security practices in the context of ADM was conducted on 61 practitioners working for Finnish software companies, empirically verified that security activities to be effectively embedded within agile practices. However, the limitation is that the respondents were all from Finnish software companies and would make it hard to generalize the results more broadly, given the influence culture has on effective implementation of processes. Another study of ADM implementation in 28 organisations identified risks with short term compromises teams make, that negatively impacts the solution in the future [20]. This is commonly referred to as technical debt by Agile practitioners, which is essentially the perceived cost for future rework. Furthermore, they identified "Separation of development and IT operations", "Increased defects in new ASD teams", "Unstandardized project management tools" and "Lack of knowledge retention" as key ADM risks. These risks except for "unstandardized project management tools" can have a detrimental impact on security. DevOps (Development and Operations) is a process that has been adopted to break the "silos" between development and IT teams to facilitate faster and more frequent deployment of solutions from development to production [21]. Rajapakske et al., (2022) identified security along with 21 challenges in their systematic literature review of 54 peer reviewed articles. They identified 31 specific solutions and

highlighted “need for developer-centered application security testing tools that target the continuous practices” of DevOps.

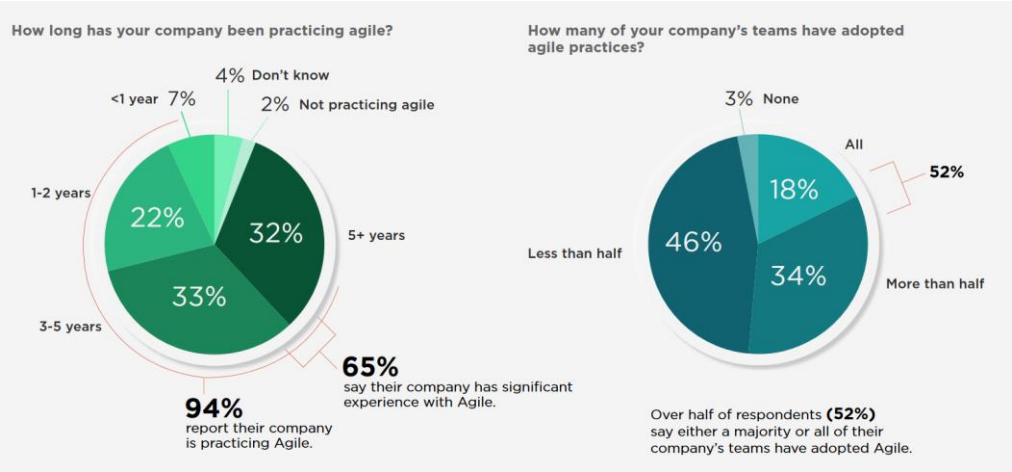


Figure 5: Agile adoption and experience [19]. Source: Digital.AI 15th State of Agile Report

2.2 Security by Design in Cloud

To the best of our knowledge and searching through prominent databases for research on the topic of SbD in Cloud, we found none that directly addressed the topic of SbD practices in the Cloud. Casola et al., (2016) proposed a service level agreement (SLA) based approach as a result of two European projects SPECS and MUSA[6] [22]. They propose an “security-by-design methodology for the development of multi-cloud applications, strongly relying on Security SLAs as a means to specify the security requirements of the applications and of their components”. Furthermore, the authors extended the methodology by introducing automation and focusing on developers without security skills [23]. However, their paper does not provide a holistic overview of current SbD practices and challenges that organisation’s face. An empirical study of non-technical factors by Arizon-Peretz et al., (2022) of 499 software developers from a single enterprise across branches in seven countries, found that “organizational security climate and security self-efficacy” had a positive impact on proactive security behaviors [24]. However, study was based on survey conducted in one enterprise and did not share details on the Cloud adoption of that particular enterprise.

[6] SPECS and MUSA are two cybersecurity projects funded by the European Union. SPECS stands for “Secure Provisioning of Cloud Services based on SLA Management” and is aimed at developing a secure cloud computing infrastructure. MUSA stands for “Multi-cloud Secure Applications” and is aimed at developing a framework for secure multi-cloud applications.

3 METHODS

3.1 Recruitment

To understand how organisations approach SbD, we seek to interview practitioners who are involved directly in building Cloud based solutions in their organisation. We identified 21 candidates based on our direct and extended network. We did not restrict our choice of participants to just security experts. This is to enable us to get a holistic picture of SbD approaches in organisations from different actors and roles. Furthermore to remove any role specific bias, we identified variety of roles and seniority levels to interview. Out of the 21 potential candidates, we interviewed 16 participants across 14 interview sessions. We conducted the interviews in a semi-structured format by asking prepared questions to the participants, while having the flexibility to ask follow-up or clarifying questions. 12 out of the 14 interviews were one to one meeting, and two sessions had two participants. While we managed to talk to two more participants who shared their views, they did not consent to being recorded and have been excluded.

3.2 Participants

Our participants represent various roles such as Engineer, Solution Architect, Chief Architect, Chief Technology Officer (CTO), Chief Information Security officer (CISO), and Security SME. Furthermore, collectively our participants represented ten companies across four geographical areas. Our participant's geography and organisation distribution is illustrated in Figure 6 and Figure 7 respectively.

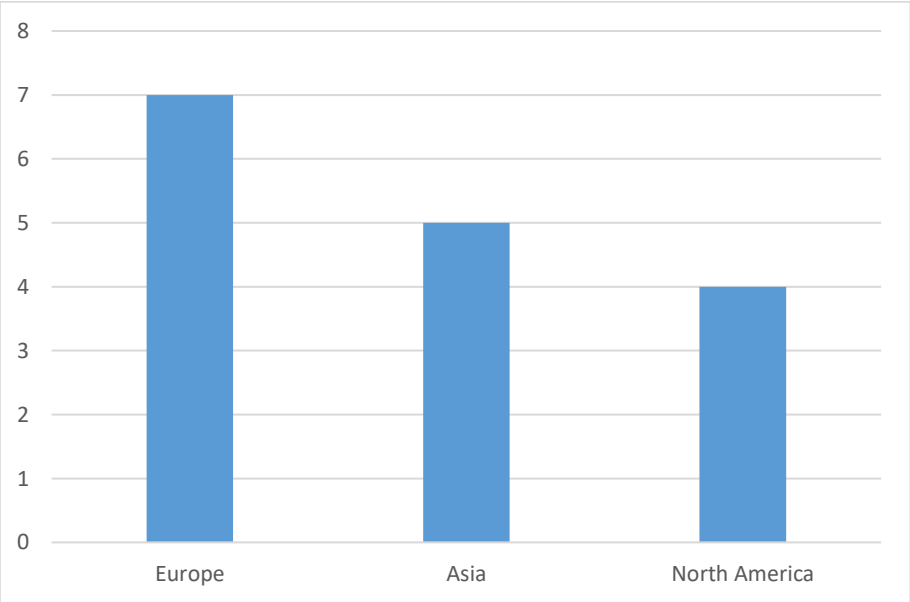


Figure 6: distribution of participants by the geography they reside in. Source: created by the author.

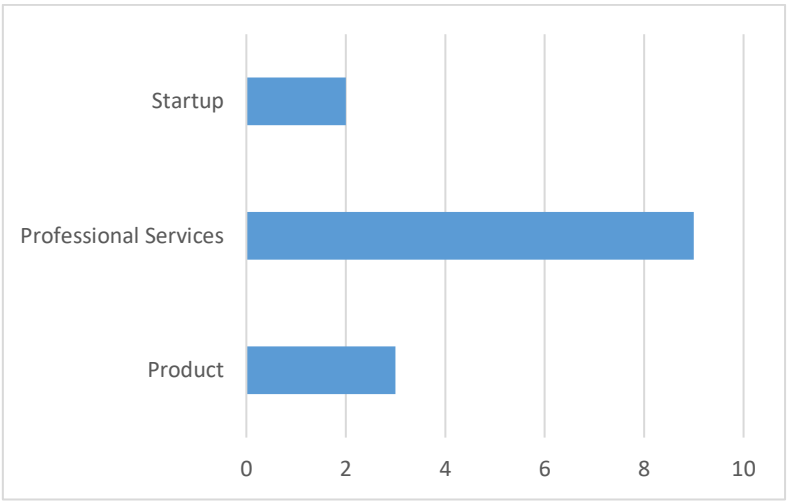


Figure 7: distribution of participants by the type of business they work in. Source: created by the author

3.3 Interview Strategy/ Data collection

We contacted the participants primarily through LinkedIn[7] and email, where we briefed them about the motivation of our research and asked them for a 60 minute timeslot for an online video interview. Once we had the confirmation from them about their willingness to participate, along with time slots for the interview, we sent them more details such as the interview questions, data handling procedures and interview process and need for transcription as part of a participant information pack that is attached in the appendix. We scheduled the interviews and shared the Microsoft Teams link for the session. During the interview, we enabled recording and automatic transcription features that Microsoft Teams offers. This was done after getting explicit consent from the participants. Microsoft Teams also automatically shares the location of the recording and transcription to the participants, for increased transparency. We then cleaned and anonymized the transcripts where required, for any errors or sensitive information. This was done after reviewing the recordings multiple times within Microsoft Teams.

[7] https://www.linkedin.com/

We identified 11 interview questions (detailed questions shared in the appendix) to help us answer our research questions. With the first two questions, we try to get an understanding of the organisation's ADM approach and any specific methodology they leverage. The next five questions cover their SbD definition and approach in the context of Cloud and Agile, including getting an understanding of their perception of key shifts they are observing with Cloud. This helps address our research question RQ 1. The final three questions were about challenges and barriers along with the impact of Agile Culture on SbD. These would address our research question RQ 2. While we organised our interview questions to map to our research questions, in reality during the conversations we observed that our participants would provide their insights that might not strictly aligned to the intended mapping. For instance, when defining their approach to SbD, a lot of them already started covering some aspects of challenges, and while discussing Agile culture, they would refer to enablers and challenges to SbD practices. We developed a codebook and leveraged Atlas.Ti to help analyse the raw transcripts.

3.4 Analytical strategy

3.4.1 Data Extraction

Data extraction was primarily carried out in Atlas.Ti 23. The cleaned up interview transcripts were exported from Microsoft Teams as text files and were stored in a common location with access control. We then imported the text transcripts from the location into Atlas.Ti 23 for systematic coding of the transcripts and thematic analysis. We studied the transcripts and developed a conceptual codebook that is attached in the appendix.

3.4.2 Codebook

Each of the interview transcripts were analysed and coded according to the codebook, to identify themes of SbD definition, SbD practices, factors and sentiment (challenge or enabler). Using Atalas.Ti 23's code co-occurance analysis we identified factors with a coding of challenge, to support RQ 2. Coding of SbD definition and SbD practices support our research question RQ 1. The details of code names and the number of quotations per code is attached in the appendix.

3.4.3 Ethics

We have been transparent to our participants about data handling and maintaining their privacy by anonymising any quotations that we use in our paper. Furthermore, we have also

anonymised the organisations they work for as well a generalized the location they are based to a broad region. We have obtained explicit consent for the recording and transcription of the interviews as part of the interviews. Moreover, this was the first question that was asked to the participants and the recording was started only after their consent. Furthermore, they were also asked for the consent once again after the recording had begun. Moreover, we have removed any references to potentially sensitive areas such IP or business specific aspects and kept the focus of discussions to their approach of SbD. Participants can withdraw their consent during the interview or later by contacting us directly and at which point their interview transcripts and recording would have been deleted from our repository. We maintained an excel spreadsheet to track the actual participant information and the link to their relevant data in the same file location as of the transcripts and the recordings. This location was restricted to the author only.

4 RESULTS

4.1 SbD practices in organizations

To answer our first research question: *What are the SbD practices the organisations implement in developing Public Cloud solutions using ADM?*, we first explore the elements participants use to define SbD in their organisation, to help set the context for the nine SbD practices we observed in our discussions with our participants. Furthermore, we explore four factors that influence SbD practices in organisations.

4.2 Elements defininig SbD

During the interviews, we asked participants if their organisations defined SbD. Every participant affirmed that their organisations did indeed have a formal approach. Moreover, we observed from their explanation, the definitions covered one more of the following eight elements: (i) embedding security related activities earlier in the engineering process and moving it from discrete one time approach to a continuous *lifecycle approach*, (ii) aligning Development and Operations activities through *DevOps*, (iii) identifying and managing *risks* continuously, (iv) set of rules, standards and policy that provides the foundation for security and *compliance*, (v) *frameworks* that they leverage, (vi) protecting Confidentiality, Integrity and Availability or *CIA Triad*, (vii) the *mindset* with which individuals and culture operate in, and (viii) protecting specific targets. The distribution of each of these elements is detailed in Table 1.

Elements of SbD definition	Number of particpants (N)	%
Lifecycle Approach	14	100%
DevOps	12	86%
Risk Management	12	86%
Compliance	11	79%
Frameworks	9	64%
CIA Triad	3	21%
Culture and Mindset	3	21%
Target protection	2	14%

Table 1: Elements in SbD definition. Source: created by the author

4.2.1 Systems Lifecycle:

The first element that we observed participants use to describe, how their organisations defined SbD was through their software development lifecycle and incorporating security activities across all the stages of the lifecycle. Five participants referred to leveraging Microsoft SDL, while the others described the various phases of their lifecycle and how security would be incorporated into that, even though they did not refer to it by a specific name - *"each stage, the design stage is where we're gonna think about each architectural decisions that we're making, the kind of designs were making, are they built in with security first in mindset? And then development is where we're gonna incorporate the tools, technologies and checkpoints in the process of how engineers are actually building and developing that sort of service" (P11).* Two participants cited their organisation mandating the lifecycle. While this was not explicitly called out by other participants, many of the elements they referred to within the lifecycle like mandatory tools and assurance steps, indicated that some level of enforcement was aimed to be achieved within all the participant's organisations - *"As part of the testing we have embedded security testing app as a mandatory fashion" (P1).*

All the participants referred to change in approach from the past where security was considered an after thought to now taking a proactive approach - *"it was more like look, I have developed this product, let's secure it. Now it has become [that] I am going to develop a*

product, how is actually security being taken into the design" (P6). We observed that our participants approached security as a continuous concept rather than as a one-time activity and this aligns well with their agile approach where the system and the architecture evolves with each agile iteration or sprint. Furthermore, one participant mentioned the cost of not considering security early in the lifecycle - *"retrofitting things back into the code or your solution is almost impossible without really causing a lot of churn"* (P5). We furthered observed the lifecycle referred to by our participants extended beyond construction activities and into operations aspects as well. They referred to this approach as DevOps or "Development and Operations"

4.2.2 DevOps

The next element that we observed the participants use to describe in their definition of SbD was DevOps (Development and Operations). According to our participants, DevOps was the implementation of the software lifecycle that included process, people and tooling elements. We observed all of them refer to 'pipelines' when it comes to the process and automation elements of 'how' the solution was being built rather than the 'what' or scope of the solution being built. Furthermore, we observed some of them had dedicated teams focused on building and managing the DevOps pipelines that automated and integrated processes between engineering and IT operations team. Our participants referred to this as "CI/CD" pipelines as well. "CI/CD" stands for "continuous integration / continuous delivery or continuous deployment" [25]. Four participants referred to DevOps as DevSecOps as well, stressing that security is an integral part of the approach. Their focus was to ensure that code that was stored in organisation's chosen repository meets the security standards. This was done by integrating security tools and assurance steps into their DevOps approach – *"development is where we're gonna incorporate the tools, technologies and checkpoints in the process of how engineers are actually building and developing that sort of service is built into it, then we move into operations that requests a slightly different kind of muscle. So once you have in the operation this at constant DevOps cycle happening, there's a constant new code being released"* (P11).

4.2.3 *Risk Management*:

Risk management was the next element that we observed our participants define SbD with. Their approach to SbD involved evaluating risks - *"look at how, how things could go wrong in from a, from a customer standpoint"*(P1). They cited that it was about considering security beyond quality and consider abuse cases - *"we look at things from an attackers perspective. security is kind of all about abuse cases. How would a system be abused and you know, quality doesn't really focus that much on that"* (P2). Moreover, participants cited risk management approach helped their teams prioritise security. We observed that this was achieved when teams prioritise security tasks among other tasks that needs to be performed to complete the development of the product. This was also referred to as product backlog - *"the current product [backlog] is assessed through the risk perspective. So risk first cost, second speed and agility, and innovation the last one. I would say so triaging of a backlog, if you have the risk is the number one triaging dimension. Typically security related things will float to the top"* (P4).

Furthermore, we observed that participants use risk management approach to achieve the right trade off with other business priorities such as time and budget. Identifying the right actions and response depended on tailoring the responses to the risks – *"if it is a low risk component, we're gonna go fly through automation. If there is a high risk component, we're going to have humans reviewing it"* (P11). Participants further cited that risk management was an integral part of the frameworks they used to support SbD.

4.2.4 Frameworks

The next element we observed in the definition of Sbd cited by our participants was the various frameworks they used within their organisations. We have provided more details on the frameworks that participants referred to in Table 2.

Framework	Participants	Description
FMA – Failure Mode Analysis	P1	Step by step approach for identifying all possible failures in a design, construction or assembly of a product or service. "Failure mode" refers to all possible ways something might fail and "Effects analysis" refers to better understanding the consequence of those failures.[26]

Microsoft SDL	P2, P5, P6, P11,	Microsoft Security development lifecycle [7]. It is a set of practices aimed at improving software security. The main tasks it focuses on are training, defining a bug bar, attack surface analysis, threat modelling, defining you tool chain, avoiding banned functionality, using static and dynamic analysis tools, security code review, incident response plans and penetration testing.
NIST	P9	National Institute of Standards and Technology is US agency focused on measurement science, traceability and the development and use of standards [27]. The Computer Security Resource Center [8] provides information on many of NIST's cybersecurity related initiatives and publications.
ISO 27001	P4, P9	"Information security, cybersecurity and privacy protection — Information security management systems — Requirements" standards from the International Organisation for Standardisation [28]. These are standards from and guidance from ISO [9] provided to companies for establishing and managing their information security management systems (ISMS).
EBIOS	P14	EBIOS stands for Expression des Besoins et Identification des Objectifs de Sécurité - Expression of Needs and Identification of Security Objectives. It is a set of guidelines and tools to support risk management. [29]
SOC 2	P10	System and Organisational control – internal controls, reports of service organisations "relevant to security, availability, processing integrity, confidentiality, or privacy" [30, p. 2]. The American Institute of Certified Public Accountants (AICPA)[10] is the governing body of the framework that assesses organisation's security posture based on its Trust Services Criteria (TSC).

Table 2: Frameworks. Source: created by the author

4.2.5 *Compliance*

Compliance was the next element we observed our participants cite when they defined SbD. Participants cited that compliance was with relation to policies they had in the organisation. Policies laid the foundation for security standards that were expected to be followed in the

[8] https://csrc.nist.gov/
[9] https://www.iso.org/standard/27001
[10] https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2

organisation - *"set the ground rules to ensure that security if first"* (P1). We observed that policies were supported by reviews and other mandatory requirements. A number of participants called out mandatory requirements for their organisation were driven by regulatory needs, customer's compliance programs or internal compliance programs, leading to reviewing risks and mandating trainings. P11 noted that compliance has been broadly been driven from the boardrooms with a perspective that compliance and certification equates to security. He called out *"that notion is changing. That notion is evolving, but it's very, very important. Compliance is just the reflection of your security posture. So if you don't have a solid security posture, having four stamps on your website is not gonna save you from the consequences of a security breach"*. Furthermore, to the question of how compliance helps drive security requirements where customers typically have compliance programs, one participant (P2) stated that these are typically broad requirements that does not take into consideration the specific end product's requirements.

4.2.6 Individual Mindset and Organisational culture

Participants emphasised the focus on proactively driving security activities, and not "bolt-on" security after the fact. Some participants cited the need for mindset shift that involves everyone in their organisation to be committed to security. Moreover, it is also a mindset shift to not relate security to just tools, processes and technologies, but take a holistic approach towards looking at things from an attacker's perspective, assessing risk, and taking timely actions - *"it's more about building secure systems as opposed to sort of just security features like just, you know, throwing a firewall in there and what have you"* (P2).

Some participants referred security being in the DNA of the organisation culture. Having a robust cybersecurity culture in the organisation helps to exceed *"minimal standards-compliance"* [31]. To drive a cybersecurity culture, organisations need to identify key security behaviours, establish security expertise to champion cybersecurity within engineering teams, creating central repository to make security related materials, information and tools in one location, and aligning security. Most participants identified key behaviours such as creating a threat model and defining the appropriate security controls during the design stages of their development process. Participants consistently cited embedding of security champions to support the development teams, with many of them stating they have centralized security capabilities such as Centres of Excellence providing the security

champions. One of the participant (P4) referred to maintaining a central hub that provides the most up-to-date information on security controls, tools and innovative technologies. Specific roles within their organisation were incentivised to provide feedback on the effectiveness of these controls and tools in the central hub. This gives the rest of the organisation feedback on when something is ready for market or not. Furthermore, this helps everyone be more aware of technologies and tools that are new in the market. Another participant cited providing their teams with building blocks and reference architectures to support standardisation. Furthermore, one participant cited that having the right leadership support sets the tone and was critical for building the right security culture within the organisation.

Majority of the participants cited training, readiness and awareness contributing to their SbD approach. Furthermore, mandatory security trainings were required for all employees. There is an ongoing debate about effectiveness of security trainings [32]. Most participants cite employee readiness as a challenge. This could indicate the effectiveness of their security education, training and awareness (SETA) programs.

One participant (P4) shared a view that was different from the rest. He pointed out that with universal access of security tools and training, security domain should not given a special treatment and be compared to other quality attributes. Participant P2 cited a particular reason to contradict that view: "security is about abuse cases and quality does not focus that much on that". Furthermore, there is no empirical evidence to support increasing adoption security tools has led to reduction of vulnerabilities or security incidents. Moreover tools and trainings by themselves do not address the mindset and culture aspects.

4.2.7 CIA Triad

We observed three participants cite CIA triad of Confidentiality, Integrity and Availability in their definition of SbD. They explain that these aspects can be compromised at the application layer, network layer, or host layer and will form the basis of the security requirements and design of the solution – *"I'm worried about the confidentiality aspect of the data on the network layer. So then my design decision is simple. I'll implement a TLS or an SSL or something"* (P8). Furthermore, assessing for vulnerabilities in a system was towards protecting assets that are valuable to the organisation.

4.2.8 Target protection

The final element we observed our participants define SbD is with respect to identifying key assets or targets to protect. We observed two participants discuss protecting specific targets especially digital assets – *"Any solution like you want to safeguard your assets, right, and these are especially in it world they are digital assets"*(P8). Protecting specific assets from threat was cited as primary objective of security. We observed practices that our participants and their organisations implemented for the SbD approach. We will discuss this in the following section with the aim to answer our research question *RQ 1: What are the SbD practices the organisations implement in developing Public Cloud solutions using ADM?*

4.3 SbD practices

With the context of how our participants organisation defined SbD, we seek to further understand specific practices that they implement specifically to support SbD, for the solutions they build for the Cloud. As participants described SbD implementation in their organisation, they provided insights into key practices that form the implementation: (i) Security Education Training and Awareness (SETA) of everyone involved in building, operating and managing the Cloud solution, (ii) Technical capabilities that support SbD practices, (iii) Approach to security requirements, (iv) Architecture and design of the solution, (v) security expertise and how they are organized, (vi) the approach to threat analysis, (vii) choosing appropriate security controls, (viii) assurance processes and methods, and finally (ix) their management approach. We will now cover each of these practices in more details.

4.3.1 Security Education Training and Awareness (SETA)

The first factor reported by our participants was related to SETA. In this sense, we observe that our participants placed importance to people in their approach to Cybersecurity, as much as they would give technology and process – if we quote the often-used triad model of "people, process and technology". Organisations invested on SETA programs as a key strategy to improve their security posture and compliance. Moreover, SETA programs not only influenced employee's intention to comply with organisation security policies, they also influenced their intention to protect their assets[33]. We observed that all participants in our interviews also refer to security related training towards meeting their compliance needs

driven by company policy or other regulations. 12 participants referred to the trainings as mandatory. Basic training such as *"telling why cyber security is important. What are the most frequent attacks? How to react if you receive a phishing email, what are the channel for reaching us, our cyber-SOC. This is the basic training that all the people must follow"* (P9). However, many of the participants referred to other interventions as well, such as monthly forums to discuss security issues, on demand training during project kick-off. This suggests that their organisations can distinguish the need for compliance and the broader intention to improve awareness of individuals.

Furthermore, role specific trainings to bridge any skill and experience gaps, impacts the performance of teams in Agile settings [34]. Participants cited that trainings covered activities such as secure design and coding guidelines, security controls, process related aspects such as ADM and tools like Github[11] that support the process - *"We require everyone to do security application training, so it's going [about] writing code. We have some third parties, some customization of our internal tools. That's like kind of a yearly requirement for all people in a product development role and we audit those things and make sure that content stays fresh."* (P12).

We also observed that various approaches beyond mandatory trainings were leveraged to increase awareness. One such approach was teams getting together on a regular basis to discuss their insights and learnings. Another approach was to have a platform where new technologies and tools are posted with peer review and feedback recorded right into the tool. One of the participant cited using a platform called Cyberbit[12] for simulations: *"This is a platform that basically have a virtual environment that you can configure with server SCADA systems, work station and in this environment, uh simulate this environment simulates cyber security incidents so you must stick what's going on in this environment."* (P9). Furthermore, these tools are part of the broader technical capabilities that organisations build to support SbD.

4.3.2 Technical capabilities

The second factor reported by our participants was their leverage of technology to support their security journey. They considered technology to be a key enabler. There was particular

[11] https://github.com/
[12] https://www.cyberbit.com/

attention on standardisation, especially in the Cloud that provides a plethora of options out of the box: *"increased our ability to monitor and our observability level of this kind of security monitoring, especially a modern technology like policy blueprints monitoring solutions."*(P3). Two participants, notably from startups "born in the Cloud"[13], cited that standardized Cloud capabilities increases their ability to deploy security features faster. A number of participants talked about their DevOps[14] capabilities and the ability to automate their CI/CD[15] pipelines and the ability to integrate certain tools chains that increases the level of automation that teams can achieve in their engineering process. CI facilitates reduced build and test time, increases visibility on build and test results, improves automation in testing and fault detection [35]. This provide teams with increased capabilities to support their agile approach: *"you generally perform a penetration testing of the application, maybe once in six months, once in three months, right? So this has automated pen test which runs twice a day, and there is a manual pen test that runs every quarter."* (P10). Furthermore, participants cited that integrating SAST[16] and DAST[17] tools help mitigate security risks through the engineering lifecycle.

Our participants placed importance to another key element contributing to their technical capabilities – IaC (Infrastructure-as-Code). IaC is considered a foundational technique to increase DevOps maturity of organisations [36]. Furthermore, automation of deployment and environment provisioning automation drives is the biggest driver of maturity in the technology dimension- *"DevOps team which you know, day in and day out, works with AWS[18] portal and Terraform[19] to, bring up instances, bring down instances, change server policies, all of that." (P10)*. Furthermore, participant P13 cited the ability to curate and standardize with IaC. Moreover, this could then be managed by central teams, through centralized repositories that can enable the rest of the engineering teams. This central repository can support various assets and for people who tried something and if its not

[13] Commonly referred to as companies that build their product or services 100% using Cloud technologies
[14] Development (Dev) and Operations (Ops) – "DevOps influences the application lifecycle throughout its plan, develop, deliver, and operate phases. Each phase relies on the others, and the phases are not role-specific. In a true DevOps culture, each role is involved in each phase to some extent." - https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-devops/#areaheading-oc890d
[15] The process of automation to support DevOps journey. https://about.gitlab.com/topics/ci-cd/
[16] Static Application Security Testing tools
[17] Dynamic Application Security Testing tools
[18] Amazon Web Services
[19] Terraform is a tool that provided the capability to automate infrastructure provisioning and management by treating Infrastructure as Code. https://www.terraform.io/

working, *"not ready for market yet, and [feedback is] submitted back so everyone gets aware of the new waves of technologies."* (P4).

A number of participants cited that Cloud providers have tools and frameworks such as the Well Architected Framework, Cloud adoption frameworks and blueprints. These frameworks provide canned processes and predefined approaches that support standardisation and application of best practices. Furthermore, infrastructure can be treated as a gate with the teams managing it can ensure everything being deployed goes through deployment pipelines that can incorporate automation and checks. We observed that infrastructure is being treated and managed similarly to applications as *"these are no longer two different things. Everything is code now."* (P4).

4.3.3 Security Policies and Requirements

The next factor we observed our participants refer to was security requirements. Security requirements reduce vulnerabilities in systems by implementing mechanisms that observe the correct security principles and avoid exploitable defects by guiding the design, construction and verification aspects of the solution [37]. Furthermore, these requirements are result of distinct analysis tasks that cover the intersection of three dimensions goals, design and threats. Risk analysis, security design and threat modelling are the typical activities that support identification of security requirements. We observed that all participants referred to organisation policies and regulations that drive compliance and protection goals. Furthermore, we observed that participants referred to design goals that guide their security design. These design goals can be focused at various levels such as the overall environment the target solution is going to be hosted on such as the Cloud, application level based on specific use of the application or at user or team level depending on how users are expected to interact with the system : *"we have an overall security policy at the cloud level itself, right, like for example, you know we have a very, very strict rule around egress and ingress in the instance side."* (P1).

We further observed different approaches to arriving at security requirements. One participant P9 mentioned that they have a catalogue of requirements that they match with each project and each of the requirements have a standard implementation that goes along with it. Another participant P8 cited that they have a simple matrix that maps Host, Network,

and application versus the CIA triad. All participants except P9 cited they perform threat modelling for their solution.

We observed that security requirements are elicited as part of the overall requirements gathering efforts taking into account not just the policy and guidelines governing the teams building the solution but also taking into account end customer's security stance. Furthermore, some participants cited treating security requirements similar to functional requirements of a product with the goal of embedding these requirements early in the build cycle. Furthermore, we observed security requirements can come outside the engineering teams as mentioned by P13: *"separate team who does more long term planning on what was required and then I input their requirements into the agile planning cycle. So it becomes an input to like okr's or quarterly plans that I expect teams to use to deliver those things on some agreed upon schedule. But the decisions are made external to the teams and they're given to them as nonfunctional requirements."*.

4.3.4 Architecture and Design

Most participants emphasized considering security in the early phases of each project, especially in the architecture and design phases to explore the solution from network, infrastructure, application, integration and data perspectives. Furthermore, they emphasised that understanding of the different layers and components of the architecture as whole helps in better enumerating the attack surface, and model the possible threats even before a getting to the actual construction of the solution - "*Basically you now know the architecture. You actually haven't even written one line of code, but you know by seeing the architecture itself, you know what are all the different entry points for an attack."* (P8). They layers of architecture that was referred in the discussions were Network, Infrastructure, Application and Data. We observed participants refer to architects as a key role in driving security activities during the architecture and design phases of the project.

We observed our participants refer to security design principles they expect the teams to consider. Furthermore, Three participants particularly referred to defence in depth as a design principle being more relevant in developing Cloud solutions compared to traditional On-Premise solutions as the attack surface has increased in the Cloud, due to its inherent architecture of delivering services through the internet. They cited in their past experiences with non-Cloud based solutions, the focus was to secure the perimeter while within the

perimeter the rigor was much lesser. Others referred to other design principles such as establishing secure defaults, principles of least privilege and minimizing the attack surface among some of the key focus for the architecture and design activities. These are among several other design principles appropriate to SbD such as, “fail securely”, “don’t trust services”, “separation of duties”, “avoid security by obscurity”. “ keeping security simple” defined by OWASP[20].

We observed two participants who had a divergent view on the need for ‘Zero trust’. “Zero trust is a paradigm that recognizes that a business’s secrets are no longer kept secure behind the corporate perimeter and protected by firewalls. It takes a data-centric approach to security and assumes a hostile environment so that systems should “never trust, always verify” [38]. Furthermore, while participant P4 cited that not everyone needed ‘Zero trust’ approach, participant P14 stated that ‘Zero trust’ should be the north star. This is an opportunity for further empirical research on relevance of ‘Zero trust’ approach for security by design of Cloud solutions.

We further observed eight participants refer to Data security as a factor to consider during the architecture and design phases. Privacy and impact assessments were quoted as instruments used to determine data security and handling of sensitive data. From a design perspective, two participants discussed techniques such as data masking and data classification. Furthermore, Participant P8 cited the need to design the system with the appropriate controls depending on which state the data is at: “data can actually manifest in three states, like it can be in motion, it can be at rest or it can be in use. So making sure that I'm putting those design controls to safeguard this tangible digital asset as part of all of these three states, is a kind of upfront secured by design thinking” (P8).

We further observed participants referring to architecture and design in the context of ADM. Agile approaches value and prioritize working functional systems in short iterations over activities that can be perceived as not contributing directly to working software. Architecture and design is at the risk of being perceived as such [39]. We observed reference to “due diligence” phase and “Sprint 0” focusing on architecture and design among other activities. Participants make a mention of keeping the architecture updated in each sprint or iteration and govern it with some sort of peer review mechanism. Furthermore, participants cited the need to keep the threat models and other artefacts having dependency on the architecture and

[20] https://wiki.owasp.org/index.php/Security_by_Design_Principles#Security_principles

design updated as the architecture evolves. “Modular and loosely coupled architecture” facilitates continuous architecting and companies need to find the right zone to balance focusing on creating working software to architecture and design activities for the most important characteristics of the system on an ongoing basis [40].

We further observed the emphasis on standardized solutions through *“a cloud security baseline [that] fits into a design.”*(P4) or *“choosing relatively standard solutions from our public cloud vendors and that is actually a change of design thinking,”* (P13). To facilitate standardization, participant P14 referred to a platform engineering approach to create building blocks and reference architectures for to be readily consumed by engineering teams. Other participants supported similar approaches even if they did not refer to it as platform engineering. We observed three other participants P4 and P11 refer to whitelisting. According to NIST[21], whitelisting is the process of pre-authorizing or approving a set of application, infrastructure or services that can be used to build a system that P13 referred to as *“kind of make it like a simple golden path mechanism”* (P13).

4.3.5 Security expertise

All participants cited the need for security expertise to support the entire lifecycle of the project. They cited that the expertise was embedded in the engineering teams though a set of organisational practices, with individuals owning the security aspect of the solution or product being built - *“We [security team] ask our colleagues to join a project from the real beginning, so we are usually invited to kick off of the initiative. Then we focus on architectural requirements and then we go on assigning cyber security requirements. Check if the they are implemented well and then if so, the project has some doubts, they need some clarifying. We follow [up with] them.”* (P9). However, they did not imply that other members of the engineering team do not focus on security. While everyone was trained and expected to contribute to the overall security of the product, these champions or security subject matter experts (SMEs) were brought in to perform various activities. In some cases, they owned the security outcomes of the product, whereas in other cases, they provided training to the teams. Security specialists were often cited to be used for reviewing artefacts such as design, code and play a role in gathering information from the customer related to data security, such as the data privacy questionnaire.

[21] https://www.nist.gov/publications/guide-application-whitelisting

Another area that was cited by participants was war gaming or Red and Blue Teaming. These techniques are used to simulate cyberattack and defence scenarios. "The goal of red teaming is to identify vulnerabilities and weaknesses that may have been overlooked by traditional security measures, and to develop more effective defense strategies. Red teaming is a highly effective way for organizations to gain valuable insights into their security posture" [41]. On the other hand Blue Teaming is focused on adopting effective defense strategies based on their "comprehensive understanding of cybersecurity principles, technologies and best practices" [42]. Ultimately, for effective management of an organisation's cybersecurity posture, Security SMEs are critical irrespective of their role in offensive or defensive activities.

One of participants mentioned a new model called Green teaming, where a special team was deployed to address security issues - *"We call it Green teaming. Green teaming is essentially about removing systemic security risk factors through by building automations and solutions rather than security vests. You fund a independent body which takes these systemic security risks, They'll [find] tools, solutions, whatever it takes to actually eradicate those risks without adding significant overhead and debt on the engineering side."* (P11).

We observed that most of the participants cited the need to engage security champions or SMEs early in the engineering cycle to support them across the various security related activities such as gathering security requirements, design, validation and assurance. Furthermore, threat analysis was a key activity cited by the participants, where they leverage specialized security expertise to support building the threat model for the solution.

4.3.6 Threat Analysis

The next practice that we observed 10 of the 14 participants cited was threat analysis or threat modelling. It was the approach engineering teams took to analyse the solution from the attacker's perspective – *"I mean, OK, if I'm an attacker, you know, first of all, who is the attacker?... And then you know what sort of damage can then attack it?"* (P2). This activity was performed to document threats at feature level or functional area of the system being built, with the fundamental assumption to assume breach every single time – *"we record it in different kind of granularity and when we start to define those, we start to work internally as well as with the customer on how we address those"* (P6). The participants cited tools that are used during the process of threat modelling. One such tools cited by participant P8 was the

Microsoft Threat modelling tool[22] that helped them analyse threats across standard buckets called STRIDE (spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege).

We observed teams conceptualize features and threats side by side and feed that into the design of the feature – *"they can start thinking about what are the possible ways that an attacker could compromise it [features or services]. Feed that into the design discussions and then identify those threats early on and factor that in the in their design."* (P11). We observed that teams take an iterative approach with ADM with participants referring to "sprints" to deliver features and functionality. Furthermore, we observed that design and architecture of the entire solution evolves unlike the waterfall approach where you lock the design before moving to the construction phase. This implies threat modelling should also be a continuous activity and not just be done one in the beginning of the project – *"Every Sprint you make the decision, do we update the threat model for the Sprint or not. And that depends on the types of functionality that you add to the application right"* (P2). When they referred to the Cloud, one of the participant cited that ease of provisioning services, self service options, modularity and loose coupling of components, requires them to consider misconfigurations of these components and services as part of the threat analysis efforts – *"it is our model of threat modelling and you know it would be every time looking not just, we are not focusing just on the on the on people with a bad intention, we are really focused about a misconfiguration, misunderstanding"* (P14). These are additional to the abuse or misuse cases based threat analysis they perform on the system.

We further observed that threat modelling was about identifying weaknesses in the architecture and design of the system as well as identifying the right approach to mitigate them. Security controls play a big role in this aspect.

4.3.7 Security controls

The next practice we observed in our discussions with our participants was security controls. NIST defines security controls as "the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a system to protect the confidentiality,

[22] https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool

integrity, and availability of the system and its information." [23] . The focus is on *"understanding the environments, and then defining the right set of controls."* (P1). Furthermore, according to participant P2, Cloud environments provides additional monitoring and controls that are useful. We observed that participants mapped controls to security requirements that can envisioned to meet specific standards, or specific security requirements arising from the customer. Furthermore we observed that controls were applied to mitigate risks. We further observed that applying controls goes beyond mere technical considerations. Participants mentioned the cost of implementing security controls being a key factor in the decision making and this cost will be weighed against the risk factor - *"[Controls are] recorded in different kind of and granularity and when we start to define those, we start to work internally as well as with the customer on how we address those because, some security items might take it high cost to mitigate while the customer might be accepting to take that risk"* (P6). We further observed our participants mention specific focus on data security as a key consideration of their risk assessment.

We observed participants mention specific data related activities such as data classification and assessments such as DPI (data protection impact) and privacy assessments and that every engineer need to have the knowledge to perform these activities - *"So you go in deep for GDPR point of view, we provide those impact assessments from DPI or data protection point of view, and ask the question, you're doing an initiative does it have an impact on your data protection, do you handle any of these flows"* (P7). Furthermore our participants considered data as an asset which needed to be safeguarded in its state of motion, rest or while in use. Moreover, this was an important consideration to identify the right security controls. Furthermore, participant P5 cited certain techniques they have employed such as data masking which protects exposure of data in unintentional ways. We observed that the participants focused on implementing the appropriate security controls with discussions being technically oriented. Moreover, the management and operational aspects were discussed in the context of assurance.

4.3.8 Assurance

The next practice that our participants discussed was assurance. Testing, automation and reviews were frequently cited as assurance related activities. One of the participants P1

[23] NIST SP 800-12 Rev. 1 under Security Controls from FIPS 199, csrc.nist.gov/glossary/term/security_controls

mentioned security testing being mandatory as part of the testing process. Participant P9 elaborated that security tests are defined during the security requirements definition phase. Furthermore he mentioned the need to define the key evidences that need to be collected to support the assurance process. Furthermore, we observed that automation and technical capabilities of organisations support the assurance process - *"Everybody's aware that when you commit a piece of code SONAR cube or SONAR Cloud will scan your code and will tell you very ruthlessly back if you are exposing any security holes and so on."* (P4).

Moreover, we observed that configuration level testing is also performed apart from code level testing. Configuration testing was mentioned by the participants to ensure that services in the Cloud are setup in a secure way factoring in aspects such as multi factor authentication, endpoint protection, segregation of identities. This is further strengthened with outside in perimeter scanning to minimize the risks of unexpected digressions from the intended security posture.

Three of the 14 participants mentioned that automation does not completely take away human interventions. They called out a "two prong" approach of internal and external validations- *"to do code reviews to make sure that code is written securely."* (P5). Furthermore, we observed that organisations leverage external validation to support self reviews - *"a separate team in place to ensure that the right set of penetration testing, vulnerability assessments and code level testing is done before we go live"* (P1). This helps maintaining the separation of "maker – checker" duties.

We further observed participants noting shared responsibilities of the Cloud providers (Figure 8) to support assurance process. Participants called out the partnership needed with Cloud providers to assure security outcomes for the pieces they own and for those services that they are contractually bound to deliver. Many of the participants mentioned this in a positive context where they can depend on the Cloud provider to take care of assurance aspects, while some of them mentioned complexities of the shared responsibility model, when they have to holistically address the assurance needs of a solution – *"doing security testing in Azure is very difficult or it's almost impossible unless somebody is allowing you to do that"* (P5). These complexities have to be factored into the overall management approach.

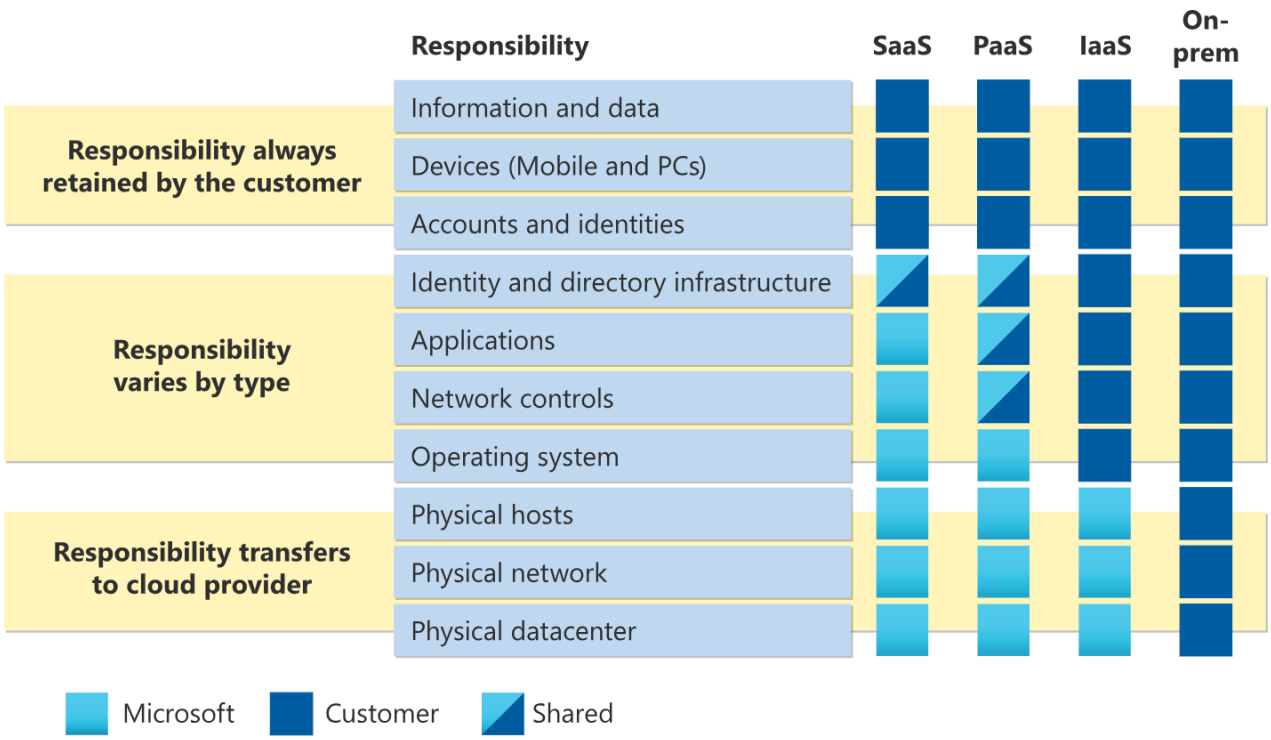


Figure 8: Example of shared responsibility model by Microsoft Azure[24]

4.3.9 Management

The final practice that participants discussed was management. Participants cited that management happens at multiple levels. It happened at an operational level such as staffing of projects, *"in case if someone is not adhering to that I mean we are trying to take them out of the engagement, so that's the level of control that we have with putting in terms of security"* (P1). Furthermore, management happens at a tactical level such as Cloud service whitelisting[25] and deciding what services in the Cloud are permitted to be used within the organisation. Moreover, we observed that participants seek to increase accountability through forums such as Solutions Review Group to perform ongoing reviews– *"so we bring everybody to the kind of monthly call so we have three or four projects going. If they're new change in scope or anything, it goes through the governance process"* (P7). Furthermore, we observed that management was also established at a strategic level where visibility is raised at the executive level to make decisions - *"results are visible to the executive team, [and] we*

[24] Shared responsibility in the Cloud - https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

[25] https://www.csoonline.com/article/569493/whitelisting-explained-how-it-works-and-where-it-fits-in-a-security-program.html

said like this is an acceptable risk. So we have some external validation that we're in need to fix something or we're doing a good job on occasion as well." (P13).

As we discussed SbD practices with our participants, they also cited certain factors that influence SbD practices.

4.4 Factors that influence SbD practices

4.4.1 *Monitoring*:

The first factor the participants cited was monitoring. According to them, there are multiple levels of monitoring. The first among them was monitoring of the solution that was being built. Moreover, this would involve measuring the efficacy of the various security measures being put in place in the engineering lifecycle such as threat modelling, design reviews, code reviews which have human intervention. Furthermore, it covers automated measures as well - "*What's the level of, you know, true positive hits on credentials and SAST (static analysis and security testing) and DAST (dynamic analysis and security testing)? That will give us roughly a good indication of how the application has been built in the life cycle."* (P11). The next level of monitoring is when the solution is live, meaning it is being actively used by the end users and is deployed in a production environment. We observed our participants cite various measures such as endpoint protection, firewalls as well as monitoring for unexpected traffic or other anomalies. These were different to the ones they had used during the engineering cycle. However, once an issue was identified, it feeds back into the engineering cycle for the threat model to be updated. The rest of the engineering process and appropriate security measures were to be followed for fixing the issue. One of the participants P6 noted that the systems were treated as "living organisms" with constant monitoring and nurturing. We further observed in our discussions, that the ability to monitor systems in production depended on the telemetry that was built into the solution. This was further supported by real-time dashboarding and alerting. Two participants cited the ability to engineer telemetry in the Cloud being easier with native tools and open source tools. This combined with the compute and storage flexibility, Cloud enables real-time monitoring of the solutions - *"what insights we could get from the different dashboards and the different alerts, that we have set in place to ensure that it is still secure and if there are any gaps"* (P12).

Finally, the third level of monitoring we observed was at the organisation level where executives look at scaling security efforts with scorecards that was being reviewed

holistically on regular frequency, such as monthly or quarterly. These are used by executives to determine the overall security posture and risk. Further more it was used to review if they were on track towards their business goals. One of the participant mentioned level of leadership support determined what was being reviewed and also determined the investments and focus of the organisation. Participant P13 cited external validation for particular security related topics that might be of interest – "*we actually run some classic tools that we do pen testing several times per year, and I also have some external auditors who will come in and spend focus time on a particular topic."* (P13). Furthermore, we observed Automation being cited by many of our participants having an impact on the ability to monitor as well as other practices.

4.4.2 Level of Automation:

The next factor we observed our participants cite was the level of automation that supports the various SbD activities and practices. DevOps, Infrastructure as Code (IaC) and Artificial Intelligence (AI) has been cited by participants as areas of strong focus. We observed participant cite automation of activities in the DevOps cycle to support their security by design approach. Tools such as code scanners, SAST and DAST tools were quoted to be used to automate some of the security related activities. Furthermore one of the participant P10 quoted using a tool called Indusface[26]. According the provider's website, the tool can provide web application scanning, mobile application scanning, API Scanning and asset discovery (Figure 9). According to the participant these tools provided a robust way to monitor solutions and especially Cloud based solutions that have internet facing assets and endpoints.

[26] https://www.indusface.com/

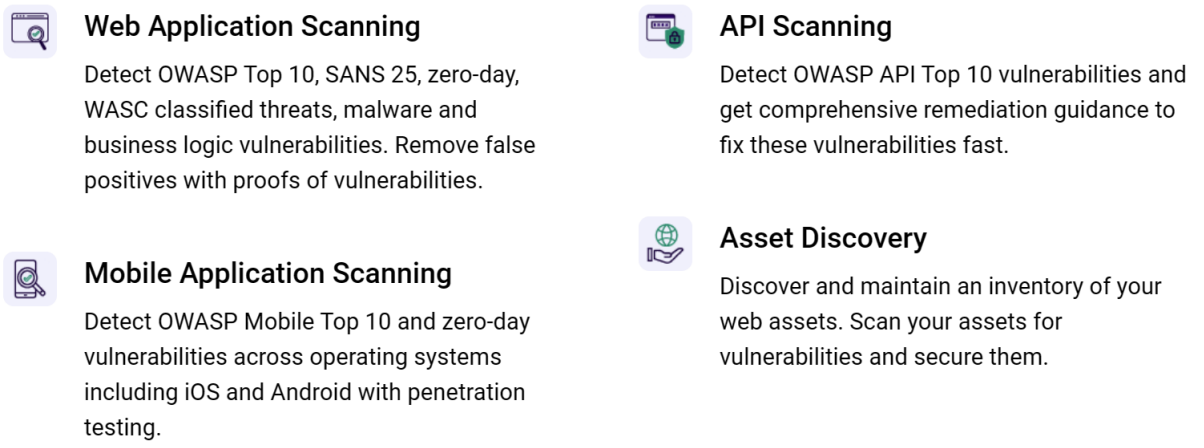


Figure 9: Indusface WAS overview. Source: Indusface.com

Furthermore, we observed that automation was also being deployed to improve collaboration between engineering and security teams. The participants cited that several teams are involved in engineering, securing and operating these solutions. For instance, there were separate teams responsible for the infrastructure aspects and dedicated security SMEs supporting security aspects. One of the participant P11 cited they were using automation to trigger engagement of these teams at the appropriate time. The automation integrates various systems like their ticketing system that monitors engagement, to code repositories that can be linked automatically to each request or ticket. According to our participant, this helps the teams work closely together without losing too much context – *"it connects the repo from which the code is being pulled into. It connects the deployment config so that like the security engineer, and always have the context around what exactly this is being actually attempting to do, and then feed that back into the engineering manager and the product owner"* (P11).

Another topic that surfaced by five participants in the interviews was Artificial Intelligence, specifically Generative AI. As one of the participants P4 calls out: *"we are probably one of the most aggressive engineering organizations using generative AI for coding. And of course also when it comes to using generative AI to do the code generation or code scanning, all of our teams are very well aware."* Furthermore, they expect AI's impact to be much broader across the ecosystem and developers - *"the ecosystem has evolved in all of these security capabilities that we expect the developers to know about. With the advent of AI and copilot and everything. Now it's going to the next level." (P11).* Further more participants cited that monitoring and automation support individuals and teams in their decision making.

4.4.3 Prioritisation in Agile Decision making:

The third factor we observed influencing SbD practices was prioritization in Agile in Decision making. Participants cited that agile teams work in short cycles and the decision making process has implications on security. Typically agile teams prioritise items based on customer value [16]. Security related backlog items would get the appropriate priority *"if you have risk as the number one triaging dimension."* (P4). Participants cited treating security requirements as features and some of them referred to it as non-functional requirements. Furthermore, we observed many of the participants refer to using Scrum[27] as the methodology in their organization. They cited that there were daily calls to review progress and also a retrospective meeting at the end of each sprint[28]. One participant P10 cited that there are dedicated sections in these forums where security related aspects are discussed including security incidents that needs addressing. Sometimes, the decisions can be top down driven objectives and the teams are expected to deliver on these on an agreed upon schedule- *"[security] becomes an input to like okr's (objectives and key results) or quarterly plans"* (P13). We observed that these forums are key to making security related decisions. Furthermore, we observed that decisions and practices are influenced by the context in which they operate.

4.4.4 Business Model:

The last factor we observed from our discussions with the participants was that the approach to security was largely influenced by the business model[29] of the organisation that is building the solution. The participants can be categorized broadly based on their employer's business: (i) companies that create products and services, (iii) companies that provide technical services such as consulting or engineering services and (iii) startups, which are companies in early stages of their operations. Participant P13 from a well established product company, cited linking security and their proposition to their customers - *"in terms of the customer centricity, that security is a customer trust promise"* (P13). He further emphasized creating awareness among his teams around why the customers trust them with their sensitive data and

[27] https://www.scrumalliance.org/about-scrum#!section1

[28] Sprint is fixed timeline iteration spanning 1-4 weeks. A project runs multiple sprints to complete the requirements of the system.

[29] The way organisations plan to make money - https://www.investopedia.com/terms/b/businessmodel.asp

the obligation to protect that trust. On the other hand, services oriented organisations that provide skills and capabilities to build Cloud solutions had a different take on the subject of satisfying their customers. We observed that their focus was to provide specific services being requested. While they could challenge their customer's asks, it finally came down to the decision by the customer - *"because number one reason we exist is to actually make customers happy. And if customer wants a dog house, we'll make a dog house. We'll explain why dog houses are not the best for humans to live in, but at the end of day we understand what you told us that we still want a dog house. We will build a doghouse."* (P4). This is unlike the first instance where as a product company, engineering teams had a lot more direct influence of security in the product roadmap. We observed participants representing professional services companies, cite the influence this has on security practices during the construction and operations of the solution, as it has a dependency on the customer's awareness and how much they value security.

The third business model we observed were participants who came from startups that believe in an inherently agile organisation, focused on challenging the status quo - *"modern definition of startup should be an agile organization looking at disrupting things"* (P10). Participants cited their approach to Cloud and security were more nimble, as they had the opportunity to start from a clean slate most of the times and did not have to deal with the baggage of an existing setup, or what they referred to as 'legacy'. Along with business models and other factors influencing SbD practices, we further observed challenges and barriers that also influenced SbD implementation in organisations.

4.5 Challenges and Barriers

Participants cited several challenges when implementing security within their organisations, including Cloud operating model, people, process, methods, changing threat landscape, tools and technologies. This will support answering our second research question *RQ 2: What are the barriers and challenges that prevent effective implementation of SbD practices in developing Public Cloud based solutions leveraging ADM?*

Figure 10 illustrates our observations of the response categories from our participants. 100% of participants discussed challenges in the process, methods, people and organisation categories. Furthermore, 93% of our participants cited challenges with tools and technologies and 86% of them mentioned they faced challenges with Cloud operating model. The final

category of threats related challenges garnered responses from 57% of participants. We will further explore each of these categories in the following sections.

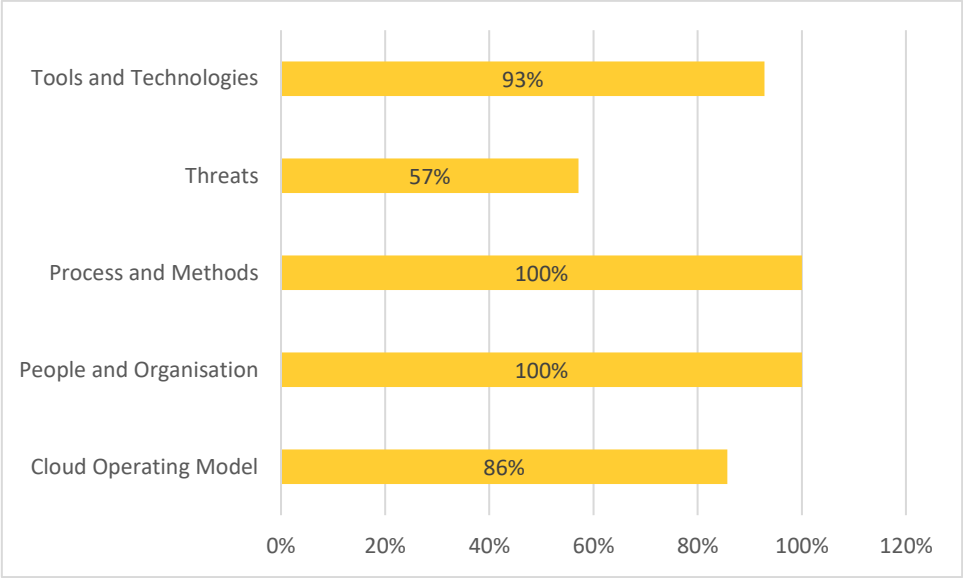


Figure 10: Challenges and Barriers, N=14. Source: created by the author

4.5.1 Cloud Operating Model

The first category of challenges participants cited was with Cloud Operating Model. Participants noted challenges across seven areas as shown in Figure 11 : (i) Cloud Architecture, (ii) Ease of provisioning new services, (iii) shared responsibility model, (iv) Costs and ROI, (v) Security capabilities, (vi) Enforcing regulatory requirements, and (vii) vendor lockin. We observed 79% of the participants shared challenges with security and the cloud architecture. The top challenges they shared with respect to cloud architecture were increased complexity with cloud infrastructure and integrating with other cloud software and services. Furthermore, integrating with legacy systems was also cited as another area that can degrade security. Moreover, participants cited that cloud based resources require increased granularity and security measures. Since the cloud is inherently a platform shared across multiple customers, participants cited a need to shift the security principles and practices and pushed for clear boundaries and isolation between applications and tenants – "*In the public cloud environment, I think it's actually even more challenging to apply security design in this space compared to the traditional. Well, let's say there are more surface area for the cloud resources and cloud offerings and there are more things to consider from application, from networking for identity to the non technical expert of security operations team*" (P3).

We observed that different approaches were required based on the type of Cloud services being consumed such as, IaaS, PaaS or SaaS. Moreover the level of granularity with which individual services needed to be designed and secured varied by the type of service. This was cited to drive more effort and complexity in securing these services individually, with potentially different security controls. Furthermore, 43% of the participants cited the ease of provisioning services in the Cloud as another challenge area. Participants cited the flexibility and increased focus on usability provides users, who typically would depend on IT operations people to provision resources, could now do it themselves in the cloud directly. This changed the level and type of controls that needed to be in place to secure cloud resources – *"by virtue of it being a public cloud and you know you know again due to the teams being agile, it's very easy to you know bring up bring something's down or get things wrong. You know the reason being, it's easier to create server, softwares, run patches in this public cloud infrastructure. It's a click of a button and you can deploy a new software there"* (P10).

We further observed from the discussions with our participants that there could be a potential dissonance in the speed at which the end users adopt new cloud services versus the speed at which security professionals can keep policy, controls and guidance updated. They cited the increased security risk due to this dissonance – *"majority of the breaches actually happen because the people are adopting the public cloud faster than the best practices to actually host safely and securely on public cloud infrastructure"* (P11). We further observed that organisations that follow agile approaches provide higher degree of freedom for their teams and this provides them the opportunity to leverage these new services which may not be pre-curated by their IT and security teams.

Another layer of complexity that 29% of our participants cited was the shared responsibility model, where the CSP is responsible for security aspects depending on the type of service being consumed such as IaaS, PaaS or SaaS (see Figure 8). Moreover, some participants stated that lack of accurate understanding of the shared responsibility model for each of the services being consumed could potentially lead to unmitigated risks – *"most of them [business decision makers], the way that they perceive the cloud is, it is secure by design. So we need to really make sure that we they understand, why we are adding these security things on top and what's the cost and make the informed decision."* (P6). We observed that costs and ROI were an important consideration. We observed 14% of our participants cited justifying the costs for security controls in the Cloud as a challenge. They cited that Cloud provided a variety of first party and third party options that could be free or paid. There is a

need for a detailed understanding of functionality and sufficiency of each of the controls before making the decision – *"It's a great challenge. How to define and to explain to clients that we can do it with a free first party given controls but you are not going to get XY and Z or we can go a level above. Are you using things that are free but good enough, or are you going to start looking into professional grade security tools?"*(P4). The perception that the cloud is secure by design needs to be balanced with informed decision-making and understanding the risks involved. These decisions are made by people, and is done within the organisation context and culture.

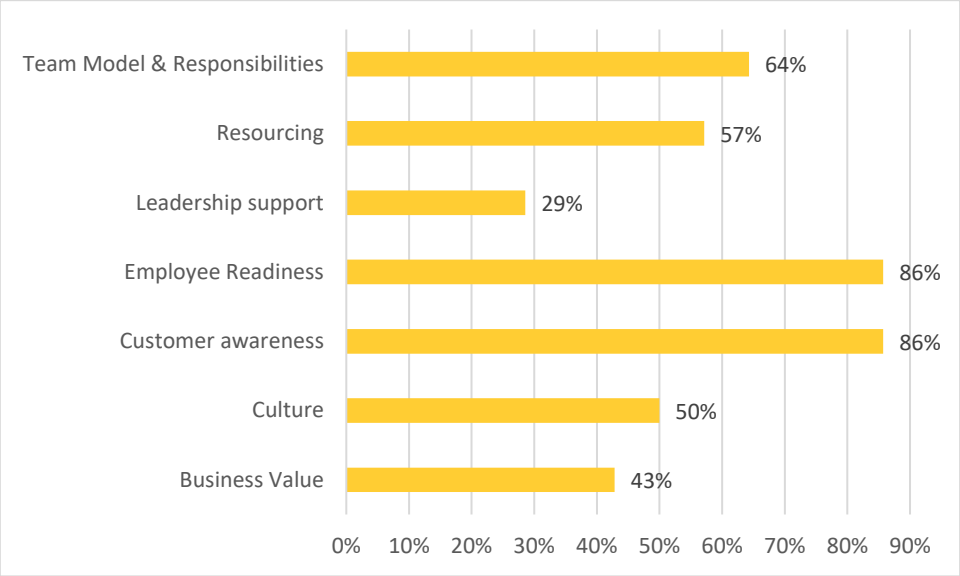


Figure 11: Challenges – Cloud Operating Model, N=14. Source: created by the author

4.5.2 People and Organisation

The next category of challenges that our participants cited were in the area of people and organisation. 100% of the participants cited challenges in one of the following topics: (i) Employee Readiness, (ii) Customer awareness, (iii) Business value of security, (iv) Resourcing, (v) Culture and (vi) leadership support. We observed 86% of the participants cite challenges with employee readiness. They cited that rapid growth of technology and lack knowledge and awareness was a key challenge. We observed that there was a shift in the what is expected from individuals when they build Cloud solutions where a developer is expected to know more about infrastructure and networking aspects, compared to the past, where they just could focus on the application aspects – *"if you're a developer who's historically used to just writing code and you're moving to the cloud, you must understand*

basic networking" (P2). Moreover, they cited that security landscape is changing rapidly as well and security professionals are playing catch-up with more sophisticated attacks. Furthermore, the other related challenge that participants cited was maintaining security and best practices in a fast paced and evolving environment. While they acknowledged there is focus on security related training in their organisations, participants cited employee skills as being a key challenge. One participant cited the need to not just focus training efforts on security related features and controls, but also inherently helping them imbibe fundamentals of building secure products through their design and coding. Participants also cited the need for continuous training that focuses on keeping employees skills fresh and not just have security training just once a year. The need for this arises due to the rapid change in the Cloud and security landscape – *"we want every developer to have full awareness of security, but it's probably difficult to train and educate people on the technology and the risks, that are probably more relevant to what we call full stack developer, that's just a scarce talent in the industry as well."* (P13).

The next area of challenge in the people and organisation category was customer awareness. After employee readiness, 86% of participants cited challenges with customer awareness and lack of understanding of security. Furthermore, they cited that customers may also have different levels of maturity, which affects their approach to security. We observed from our conversations that balancing security with customer expectations and budget to be complex. They cited that educating customers and reinforcing the importance of security is crucial in promoting a secure development mindset. Customer awareness and maturity on security influences their investments into security – *"fundamentally the biggest blocker ends up becoming the customer 1st, and 2nd the team that you have, why the customer? Because the customer tends to spend all of their money to build features"* (P6).

This is also a reflection of the customer's appreciation of the business value they perceive from security, which 43% of our participants cite as challenge – *"So we're gonna spend $1,000,000 on hardening our product. What is that actually buying us and the customer versus spending $1,000,000 on a fantastic new feature. It's gonna bring in a whole bunch of extra revenue. And that, and that's the battle we face a lot now."* (P2). Participants cited organisation culture and leadership support influences priorities of teams. 50% and 29% of participants cited challenges in culture and leadership support respectively. They cited that agile culture was focused on delivering customer and business value. Furthermore in that context, prioritising security will require strong leadership support to set the right tone at the

top and the rest of the organisation to follow that up to embed security mindset in the teams and ways of working – *"the main challenge for us because you, you know, the application and importance, the timeline for having production application is is very important for our business. Sometimes go-live milestones is shared with our CEO. So if we you share [a] milestone of production with our CEO, it's very important to meet the milestones"* (P9).

The next area of challenge we observed was 64% of participants cited with team model and responsibilities. We observed this was especially true in agile settings where participants cited embedding security expertise within agile engineering teams as a challenge. Furthermore, even if they manage to embed security expertise, there was a question on whether they will be positioned as a core part of the team versus a supplemental member of the team. This could determine the focus security receives within the team. One of the participant challenged the need to have a dedicated security expertise in the team - *"It is a cultural shift and we need to explain that when we are talking about security, it is not a matter of security architect. It is a matter of architect. It is a matter of developer. It is a matter of project manager. All are picking a part of this story of security like everyone is taking part of the success of a project"* (P14). This raises the question on how security mindset and expertise can be effectively spread across a broader base, versus being focused on a few dedicated resources.

The final area of challenge within the people and organisation category mentioned by 57% of our participants is resourcing and skill gap. They cited there was pressure in the system to staff projects. Furthermore, they don't have the time to fill any security related skill gaps individuals may have. Moreover, there is further inconsistency in skills when they have to depend on third parties or subcontractors to address project staffing needs. Furthermore, increased use of subcontractors adds another complexity of misaligned culture and values between the hiring and subcontracting companies – *"A barrier or friction point is resourcing. I think you know we're we are under budget pressure like probably everyone. So I'd say if I were to increase the depth and awareness, I would probably spend more money on security application consulting."* (P13).

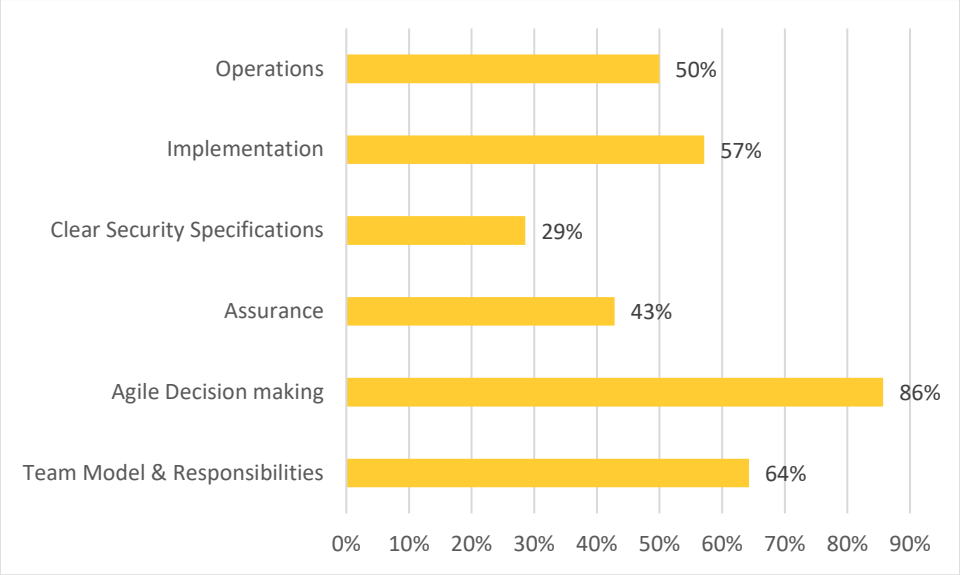


Figure 12: Challenges: People and Organisation, N=14. Source: created by the author

4.5.3 Process and Methods

The next category of challenges that our participants cited as challenge was in the area of process and methods. 100% of the participants mentioned challenges in at least one of following areas: (i) velocity and agile decision making, (ii) implementation, (iii) operational aspects, and (iv) assurance. We observed 86% of the participants cite challenges in the area of agile decision making and velocity. We observed a lack of clarity in terms of how security should be treated within the context of decision making and prioritisation including the trade-off between adding new functionality and improving existing functionality. Furthermore, they cited that when there is a focus on speed to market, there is an increased risk of missing out on implementing best practices and guidance. The other aspect one of the participant mentioned with agile is the risk of architecture taking a different path with every iteration and security not keeping up - *"on the on the grassroots level, there is still a lot of friction of productivity or agility versus security"* (P11).

The next area we observed 57% of participants citing challenges in the process and methods category was in the area of it s implementation. One participant cited aspects such as vendor lock-in, supply chain and third party risks, when it comes to integrating security in to DevOps cycle, especially in the Cloud. Participants cited that there could be a "problem of plenty" with the number of available options, and the time and effort required to find the right option for the particular situation, Furthermore, one participant cited the common practice among

developers to use public tools such as StackOverflow[30] and the risk it introduces if you don't have additional measures in place – *"I was mentioning most of our developer folks. They tend to just code the feature as fast as they want to be, and if they for example, find something in Stack Overflow that does the job, they use it and then suddenly what we end up finding is for example some secrets being checked in into our repository, where somebody can just grab it and then have full access to our databases and all this kind of stuff"* (P6).

One in two participants mentioned challenges with managing and operating security within cloud environments and cited various factors such as the freedom and ease of provisioning of services that is provided in the Cloud, less focus on documentation in agile leading to traceability issues. While on one hand they cited control and traceability issues with what is being implemented, another participant cited the ease of provisioning and integrating security tools into the engineering process created noise in the system due to the number of alerts it generated. Furthermore he cited that if these tools were not tuned to reduce the number of false positives, it could cause fatigue, leading to developers triaging the wrong issues to focus on – *"You got 400 security bugs to deal with now. They will start to triage five of them. Now they will ignore the security debt actually, the real issues are there. #8 and #12 are the real issues, but now since they spent 25 minutes in tracing the first five and it's like, OK, this is nonsense noise. They've moved on"* (P11). We further observed participants mention that ease of doing things lead to engineers turning off security controls intentionally or unintentionally – *"somebody wanted to do a quick testing. So they kind of, you know, let's say remove that [security control] do the testing and you know they forgot to turn it on"* (P12). This could lead to making the systems vulnerable due to unmitigated threats.

[30] Public platform where people share knowledge specifically on technical issues - https://stackoverflow.com/

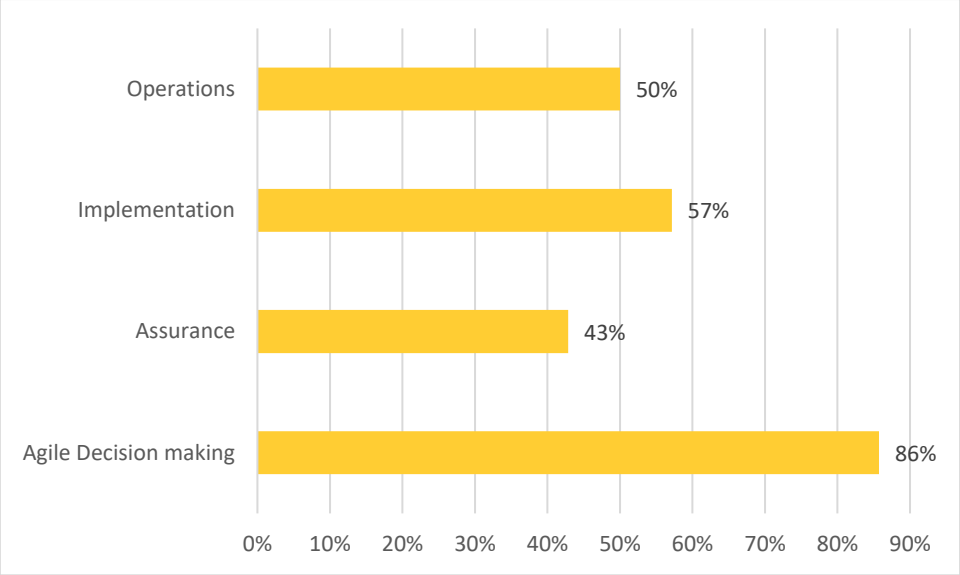


Figure 13: Challenges - process and methods, N=14. Source: created by the author

4.5.4 Threats

The next category of challenges we observed from our interviews was threats. Our participants cited that Cloud environments have increased exposure to attacks compared to traditional on-premise environments. We observed two areas of challenges within this category: (i) Sophistication of attacks, and (ii) increased surface area. They cited that each component in the cloud environment can be potential target for attacks, both internally and externally. The inherent distributed nature of cloud architectures and the introduction of microservices and PaaS services has made security more complex and challenging. 43% of the participants cited that the surface area for attacks have increased with the Cloud – *"That's a challenge, and these teams are always under pressure and we're worried I use frequently the surface area, the surface area of a product team running independent service is quite high for all the places that touches endpoints"* (P13). Moreover, 21% of the participants cited attacks have become more sophisticated, especially with bad actors leveraging cutting edge technologies like AI.

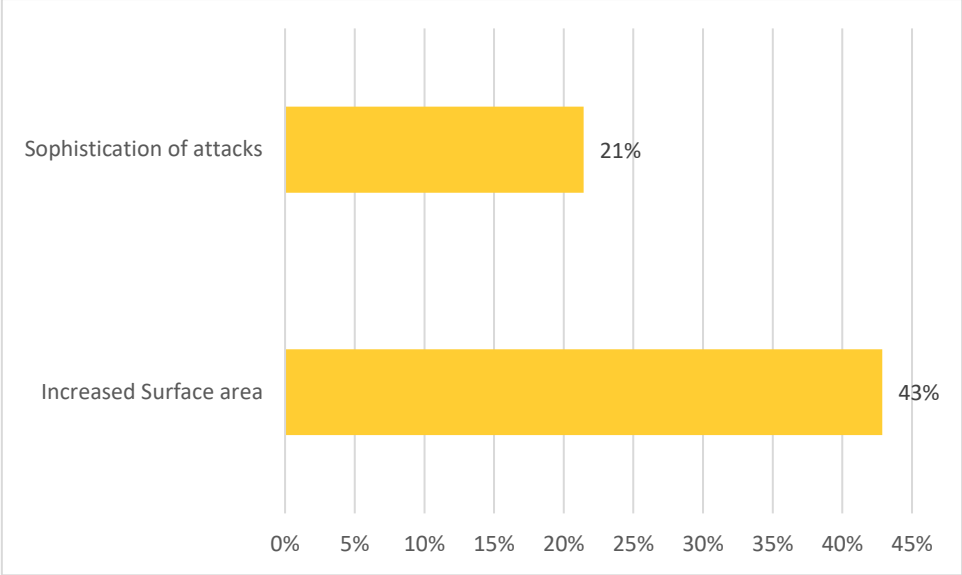


Figure 14: Challenges – Threats, N=14. Source: created by the author

4.5.5 Tools and Technologies

The final category of challenges we observed from our discussions with the participants was around tools and technologies. 57% of participants cited challenges with the pace of change of technologies. Our participants observed a gap in knowledge and awareness. Furthermore, they cited that security approaches require a different mindset and understanding of emerging technologies. They cited the need to stay ahead of the curve to provide the right solutions and establish customer trust. Furthermore, they noted that abundance of tooling and confusion in implementing security controls within the CI/CD pipeline can be overwhelming. Participants cited lack of skilled cloud security professionals who are current with the latest features and security measures. Furthermore, participants cited challenges with rapidly changing environment that leads to a lack of understanding of the overall threat - *"the overall environment is changing so rapidly, right, the kind of security threats that were there, you know that are there today, people have not even thought about it maybe a month back, maybe two months back"* (P10). Furthermore, 43% of the participants cited increased complexity as a challenge. They cited that the complexity and challenges of implementing security in Cloud environments are greater than in traditional environments, with more factors to consider such as application, networking, and identity. Additionally, integrating different security models with Cloud and traditional on-premise systems can degrade security. They noted that complexity is further increased by the need to understand the entire user journey and the dependencies between different components – *"Old systems that we always integrate with*

will typically not integrate well with a modern fine grained security elements that are available. So integrate new with old, usually on that integration boundary security always suffers" (P4). Furthermore, 50% of the participants cited challenges with establishing standards patterns and practices in an environment that is fast changing and has high complexity. One participant P9 particularly called out that, while coming up with standards and policies in such an environment could be a challenge, there was also a gap in teams implementing and operating Cloud systems. This was due to the gap in interpreting and understanding of the policy and standards by teams implementing solutions being and than the ones who defined it. He cited that Cloud is further accentuating this challenge, with the complexity and pace of change. Furthermore, the key was to find the glue between the teams that define the policies and standards, and the ones who implement it - *"If I have to say where I suffer more today is because we are not able to transfer and be sure our colleagues are getting the meaning of what was defined, and the issue is not the friction between the parties but the issue is that you start with two different line that take different direction because who have to operate is trying to do their best based on what they think is the meaning of the references"* (P9).

Another challenge 29% participants cited was with supply chain and third party risks. They cited that challenges in security automation in cloud environments include supply chain and third-party risks. The cited the need to understand why something was created and how it was secured, as well as how different components connected to each other. They called out that lack of training or disregard for licensing requirements of open source libraries can lead to uncontrolled risks. While the public cloud ecosystem has made it easier to build secure products, legacy code bases still pose challenges. Finally, participants cited challenges with fragmentation with the abundance of tools being available with each of them catering to specific aspects of the security journey with their own set of rules that may not be homogenized.

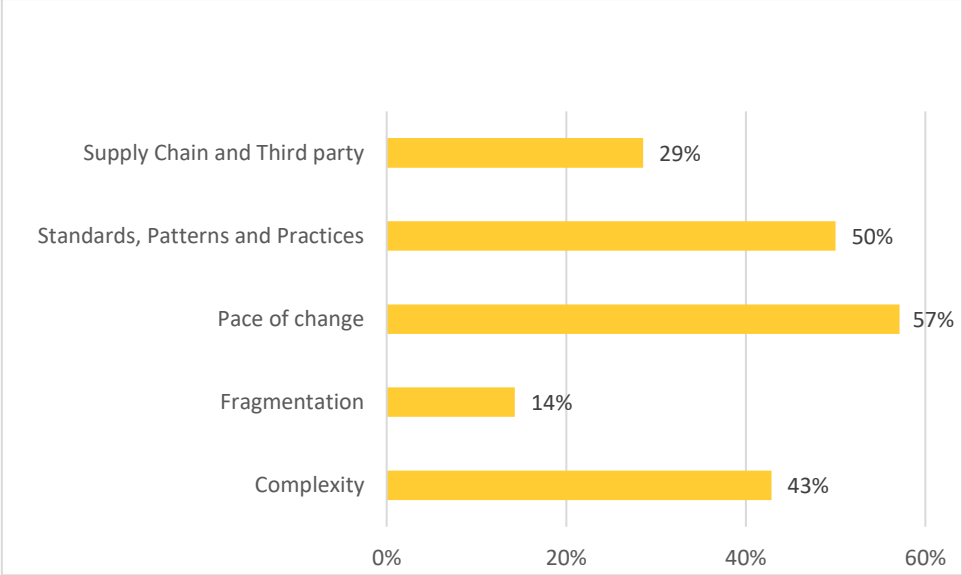


Figure 15: Challenges – Tools and Technologies, N=14. Source: Created by the author

4.6 Respondents practical recommendations

We observed a few practical recommendations from some of our participants they leverage in their organisation. We have summarised this in the below Table 3.

Participant	Practical Recommendation
P4	Focusing a team that scans the open source market, venture capital market and startups for creating an encyclopaedia of emerging technologies. Furthermore, encourage and simulate the rest of the organisation to leverage and provide their feedback based on their experiences using the tools.
P7	Setup a Solutions Review Group that governs, reviews and approves architecture changes of solutions.
P8	Create a simple matrix of HNA (Hosts, Network, Application) versus CIA (Confidentiality, Integrity and Availability) to identify threats and deduce security requirements for each of the cells. The example cited was the case of confidentiality being an issue in the network layer, the solution for this would be to use encryption such as SSL.
P9	A central team of security SMEs curates a catalog of security requirements. At the beginning of each project, based on the project outcomes, a set of security requirements from the catalog is matched based on the needs of the project.
P10	Leverage tools such as Indusface to perform automated way to test against top vulnerabilities published by OWASP or similar organisations. These tools support

	automated pen (penetration) testing that support organisations perform such testing more frequently, even as many as twice a day compared to manual pen tests that are typically done once in few months.
P11	Green teaming – funding an independent body that systematically reviews security risks and works on eradicating those without burdening engineering team who could be focused on business functionality. Another participant referred to this as special spike teams that focus on special security topics. The outcomes of the teams can be leveraged by rest of the engineering teams.
P12	Curated and standardized security related activities created as backlog items. These are integrated into engineering teams backlog of tasks that needs to completed within a sprint or iteration. These can act as a checklist for the teams as well and be integrated into the tools they would use to support their agile processes.
P13	Whitelisting and mandatory use of services within cloud environments. Furthermore, leveraging services that are standard from the cloud provider or other vendors and not getting fixated on creating fit for purpose solutions for security related aspects. Focus should be on differentiating around it.
P14	Platform Engineering that leverages anything that can be written as code to be brought together in the form of a platform or curated central repository that provides the necessary resources, infrastructure, application or tools in the form of building blocks and reference architectures for the teams to leverage as they build their solutions. This platform provides the opportunity to be integrated into the code development tools and processes of development teams.

Table 3: Practical recommendations. Source: created by the author.

5 Discussion

5.1 Discussion results

5.1.1 Shifting Left in the Cloud

All participants referred to establishing secure development lifecycle approach and referred to moving appropriate security related activities earlier in the lifecycle or what some of them referred to as “shifting left”. According to The Cyber Security Book of Knowledge, secure software development lifecycle process is defined as “proactive approaches to building security into a product, treating the ‘disease’ of poorly designed, insecure software at the source, rather than ‘applying a band aid’ to stop the symptoms through a reactive penetrate and patch approach. These processes work software security deeply into the full product

development process and incorporate people and technology to tackle and prevent software security issues.” [43]

CLASP, Microsoft SDL and Touchpoints are popular Secure software development lifecycle models [44]. Each of the models provide guidance and activities across the typical phases of the development lifecycle: `Education and Awareness', `Project Inception', `Analysis and Requirements', `Architectural Design', `Detailed Design', `Implementation' , `Testing', `Release and Deployment', and `Support' and support embedding security related activities earlier in the lifecycle. While security requirements play a key role in these processes, there was a confusion on how security requirements should be handled.

Security requirements was often termed as non-functional requirements such as performance. While you can explicitly call out what acceptable performance levels are, stating acceptable security levels is a challenge, as security is about the absence of vulnerabilities and threats, and not the presence of something that can be easily measured. For instance you can measure performance of a website as a measure of number of concurrent users being able to access it, or you can validate the presence of a functional feature by testing explicitly for those. However, that will not be true for security, as testing for a security control does not necessarily mean you can be assured of removal of all vulnerabilities or threats. Hence a risk based approach is often followed when it comes to security, as you reduce the chance of a breach.

Software development processes tend to handle typical functional and non-functional requirements well as there is good traceability from requirements to validated outcomes, where you can be sure if something is completed or not. This is also referred to as “definition of done” in ADM. There is no easy way of clearly defining when you are “done” with security, as requirements management process need to address incorporating misuse cases and a mitigation case for each of the misuse cases [45]. However, there is no established standard as to what level depth or breadth one needs to get to. This can be time consuming and is more granular than threat models that are performed at an overall architecture or design perspective. This can be especially challenging in Agile environments that are often time constraint and focused on delivering functional value, unless the business value of security is well understood, and is supported by the required expertise along with tools and automation.

5.1.2 Tooling, automation to cope with agile needs

We observed in our discussions that the participants focused a lot on the technical aspects of their approach to SbD especially in the context of Agile development. This could be due to the very nature of their jobs which was to build technical products and solutions. We observed tooling and automation was cited to be used in multiple ways to support SbD. One was security controls that actually does the job of protecting, such as end point protection, web access firewalls, etc. The other was tooling and automation that acted as enablers. A good example of this is Infrastructure as Code. While infrastructure that is needed to host the solutions in the Cloud could be deployed manually, having the options to deploy it as Code using technologies such as Terraform, provides the opportunity to perform automated checks and change management and provides and additional layer of assurance against introducing vulnerabilities either intentionally or unintentionally. Another enabler is DevOps with the focus on automating the process of solution building and deploying to the target environment. The focus of DevOps is continuous integration of code that is being written or modified, into a master branch that is used for the deployment to a target environment. This ensures the team building the solution and the team deploying the solution, which are typically separate teams, are well aligned and helped reduce time and effort spent on deployment activities. Furthermore, it helps improve the velocity of deployments which is a one of the main focus of agile development methodologies. We observed that participants focused their efforts on (i) automating the code integration and code deployment pipeline and (ii) integrating security such as code checkers, and various security testing tools. The number of false positives and efficiency of these tools making it difficult for developers to get to the actual security issues to address was one of the challenges cited. Furthermore, our participants cited the number of tools they have to contend with and the integration of these tools as challenges . This aligns with a systematic literature review of 54 peer reviewed articles conducted by Rajapakse, e.t.al [21] explored these among the 21 challenges and 31 solutions to those challenges. The study highlights the challenges arising from complexity and limitations of tools leveraged in the DevOps. Furthermore they also highlight the inability to fully automate security practices into DevOps. The study further highlight the challenges in adopting DevOps in regulated environments, constrained environments such as embedded systems or Internet of Things (IoT), or complex heterogenous cloud environments such as multi cloud environments. To mitigate the challenges in adopting DevOps, they recommend continuous security assessments while recognising that automation and tool support could be lacking to support such ongoing assessments.

The use of AI to generate code is another area that will require deeper investigation. Generative AI (GenAI) is a relatively new technology popularised by the release of ChatGPT in November 2022 [46]. ChatGPT became the fastest growing internet service to reach a 100 million users in January 2023 [47]. Through the year 2023 multiple companies like META, Google and Anthropic released their version of Large Language Models (LLMs) which are the foundational models for GenAI. GenAI as its name indicates is a form of AI which leverages its large corpus of data it has been trained on to generate new content. One of the applications of GenAI is to generate code [48]. Microsoft launched GitHub CoPilot which featured AI coding assistant that can perform a number of tasks to assist developers including generating code based on the prompt provided [49]. Companies could increase their dependence on GenAI for code generation or other forms of AI provided they carefully consider the various paradoxes AI brings along with it, such as (i) automation paradox: where you need human involvement to validate AI output, (ii) transition paradox: with new roles will be needed while other roles get displaced, (iii) creativity paradox: offering new opportunities in the creative process while taking control of process, and (iv) security paradox: system created using AI can be used for offense and defence mechanisms [50].

Human skills and intervention will be required to address gaps and to monitor the impact of the tools, automation and AI on the engineering process. Moreover, investments in people, process and tools are required to mature DevOps and automation practices. These investments could be quite significant depending on the complexity of the environment or the solution. Furthermore, organisations with their limited training budgets have to contend with AI and other new emerging areas to train their organisation. Moreover, there could be a risk of security related investments getting de-prioritised with unsubstantiated assumptions about AI's impact on their security posture such as AI generated code being secure by design.

Customer's awareness and their assessment of business value of security was cited as challenges by our participants. If that is indeed the situation, underinvesting in automation, assurance and building security into DevOps practices could have a detrimental effect on the security of the solutions. While this is true for all types of solutions, the increased attack surface area and the sophistication of attacks observed by our participants makes this of particular relevance in Cloud scenarios.

5.1.3 Key actors – who is accountable for security?

We observed several actors being involved in security through the entire lifecycle of solution. We observed software architects, engineers within the development teams have to design and build security into the products and solutions they build. Dedicated security expertise residing in external teams are often engaged with the engineering teams during the lifecycle to provide the focus on security aspects of the solution. While some participants mentioned these security SMEs own security of the solution, others mentioned they were in an advisory role, and the actual engineering teams were ultimately accountable for security. Furthermore, if there is a reliance on tooling and automation, there is dependency on the team providing these services, that further influence security outcomes. As many actors from the engineering teams, security SMEs, tooling and DevOps teams work together, there needs to be a clear framework and engagement model on who monitors, orchestrates and owns the security outcomes for the solution. The size and distributed nature of teams can add further complexity to this equation. Furthermore, shared responsibility model of Cloud providers need to be factored into this accountability model. Clarity of roles and responsibilities and skill levels of individuals involved, will impact security outcomes of Cloud solutions.

5.1.4 Security skill gaps

We observed employee skills and awareness was a consistent challenge in our interviews. While there was a focus on training, the pace of change in technology has an impact on keeping the content of the trainings current. Furthermore, knowledge retention from trainings, especially technical knowledge was to wear off within weeks in an experimental study on college students based on simulated phishing emails and attacks [32]. While the study has its limitations with its direct applicability on the topic of SbD, it is directly related to security and SETA programs, that organisations rely on. With long term effectiveness of training programs not being assured, organisations should regularly assess their continuous training needs and identify the right frequency of trainings that best suits their particular needs.

The World Economic Forum in their Future of Jobs 2023 [31] report state that *"cybersecurity is among the top strategically emphasised skills for the workforce. Yet, there is a shortage of 3.4 million cybersecurity experts to support today's global economy. This number is only*

[31] https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf

expected to grow as the impact of emerging technologies is felt across organizations. To illustrate, while the rise of large AI language models has its benefits, it also heightens cyber threats such as phishing and identity fraud which add to the workload of overstretched cyber teams". Given the shortage of security talent, organisation will have to focus their efforts in training their existing workforce on security and cultivate a security mindset to help bridge the talent gap.

5.1.5 Security mindset

A study of 21 cybersecurity professionals, describe "security mindset" as a psychological phenomenon or "unconscious habit" of evaluating weaknesses in systems, even when not being required to do so [51]. Furthermore, it is about taking conscious actions based on their probing of the system, and impact assessment done in a larger context. For individuals to cultivate a security mindset, the organisation culture needs to be supportive of providing the knowledge, experience and most important motivation to build competency around the three interrelated aspects of "monitoring, investigating and evaluating". It is inconclusive to what extent this mindset can built intentionally. However, it does posit that as long as habits form the foundations, it should be somewhat trainable. This might require different approaches to training such as lab based training programs, that addresses the motivational aspects required for individuals to put in the "substantial effort and perseverance for conceptual understanding to be gained" [52]. In the context of Cloud and other emerging technologies, creating a security mindset will help address some of the shortcomings of tools, automation, trainings and policies not keeping up with the pace of change and help improve the situational awareness of employees.

5.2 Situation Awareness in effective agile decision making

We observed teams operate in dynamic environments contending with constant change either with respect to the technologies they work on, customer requirements, people they work with or threats to the systems they are building. They are under pressure to deliver value in short two or three week iterations, when they adopt Agile methods. These require teams and individuals to make decisions under stressful conditions. Agile teams face several challenges across "decision process, decision intelligence and decision quality" [53]. Short term focus, incomplete understanding, lack of support system to present data in easily consumable view,

data inconsistencies, lack of visibility of information to the team, are some of the challenges that can lead to poor decision making that affect security. Moreover, short iteration cycles and undue pressure on the teams to deliver, create workload pressures leading to inferior performance in error detection and correction, taking short-cuts that lead to mounting technical debt[32] and poor quality of the solution over time [54]. Situation Awareness (SA) and the Endsley 1995 SA Model is "widely recognised by practitioners to be critical in effective decision making" [55]. It is often applied in scenarios where decisions have to be made under constraint environments. Time is often the constraint where actors have to decide quickly based on information available to them at that point, the way the information is presented to them, the context they are operating under such as stress and difficulty of the situation and finally the level of automation available to them. Individual factors such as their training, abilities, and overall experience along with their alignment to mission goals influence effective decision making. The highest level of SA in Endsley's model the is the ability to project the future status and take the appropriate decisions and actions based on that. Figure 16 provides an overview of the various factors from Endsley's original SA model.

Building secure Cloud solutions require individuals to make good decisions consistently such as performing continuous risk assessments and threat modelling, making the right design choices and choosing the right security controls. The quality of their decisions and the outcomes of their actions depends on capabilities such as DevOps implementation maturity, the usability of the interface design of various tools used in the engineering process, business awareness and prioritisation of security within the organisation. Furthermore, it depends on the complexity of their Cloud environments, especially if there is a need to integrate with legacy systems or span across various Cloud deployment models or Cloud providers. Moreover, the skills of the individuals to perform their task in securing Cloud solutions and stated org mission and expectation of security influences their SA.

[32] When taking short cuts and delivering code that is not right for the programming task of the moment, a development team incurs Technical Debt. This debt decreases productivity. This loss of productivity is the interest of the Technical Debt. (source: https://www.agilealliance.org/introduction-to-the-technical-debt-concept)

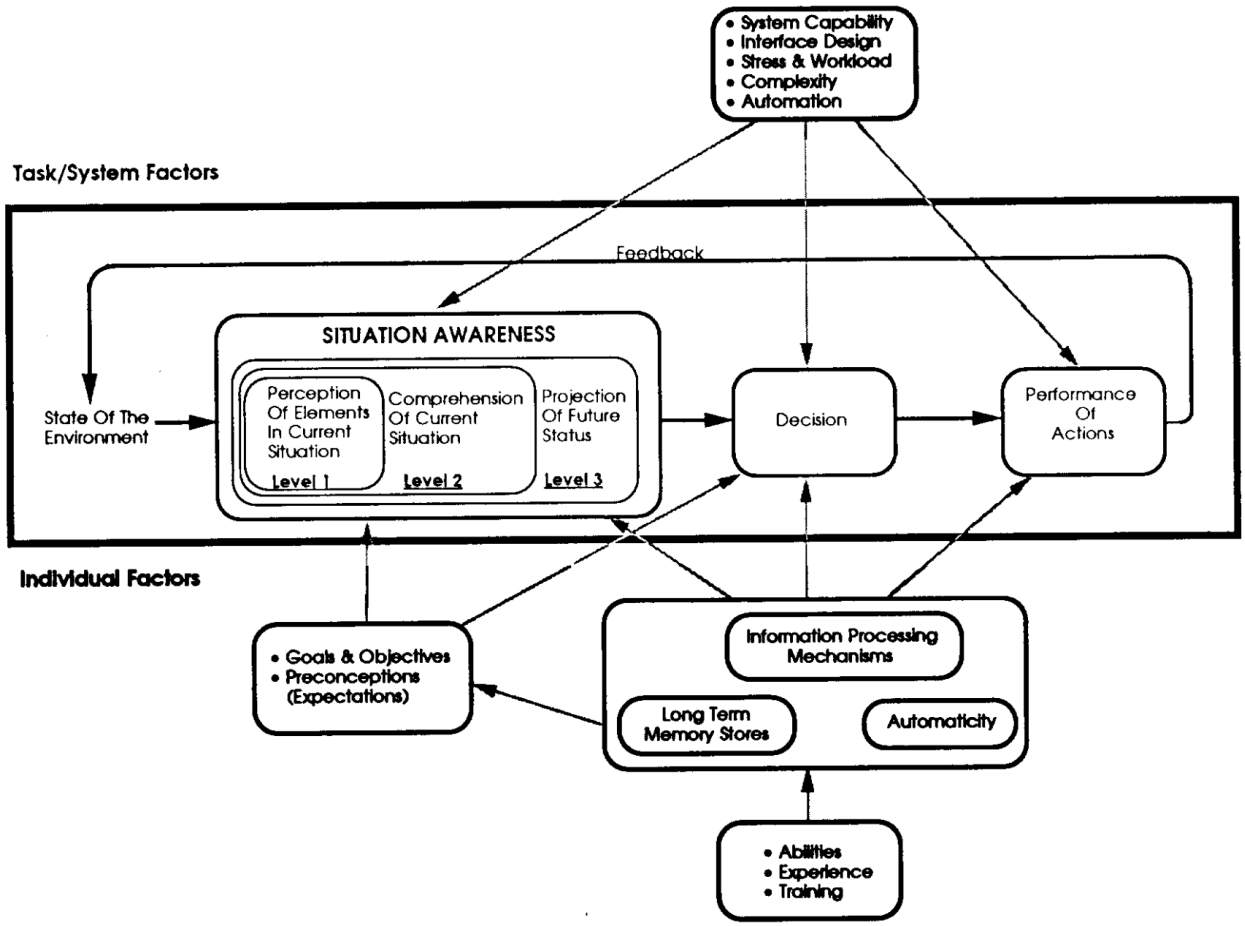


Figure 16: Endsley SA model in dynamic decision making [56]

5.3 Practical recommendations

5.3.1 Organisations should focus on improving SA of key actors

SbD is only going to be achieved when actors consistently make the right decisions by continuously assessing the impact of their decisions, and making the necessary course corrections before bad actors can exploit them. While technology is a big enabler to achieve this, human factors and the environments under which actors operate should be a focus. This requires the automation efforts organisations are investing as part of their SbD practices, to be more human-centred. It means that systems that key actors use should provide them the right insights at the right time, and in a form that is designed to help them take action. This human-centred automation efforts needs to be supported by innovative readiness approaches that can help build technical skills, the required cognitive skills and the security mindset to look for abuse cases. Adopting more formal assessments and measurement of SA using

frameworks such as Situation Awareness Global Assessment Technique (SAGAT) [57] can help improve SA in agile teams.

5.3.1 Standardisation and Curated assets

Automation, systems capability and intuitive design for engineers influence their SA level [56]. One of our participants P11 referred to "developer empathy", meaning designing SbD approaches with the end user in mind. These will be all the key actors who are involved in the engineering process. While they could be experts in their functional or technical areas, they are likely not security experts. Standardised process, tools and curated assets are part of the system capabilities that teams can leverage to improve their SA and make the right decision in a fast paced agile environment.

5.3.2 Holistic risk assessments

Agile teams as part of their iterations or sprints should incorporate continuous risk assessments. These risk assessments should cover all technical and non-technical aspects such as people risks and skill gaps. Furthermore, they need to factor in maturity of their DevOps implementation including automation and assurance and last but not the least organisational risks such as customer security awareness and maturity, leadership support and timeline risks. The outcome of the risk assessment should help set realistic sprint goals and manage expectations of their key stakeholders to prioritise security.

5.4 Limitations of this research

This is an exploratory study of organisation's practices and the challenges they face in building Secure by Design Cloud solutions. We should discuss several limitations that leads to recommendation for future work. The first notable limitation is the recruitment strategy employed. Majority of the interview participants were identified through direct connections in the existing workplace or contacted with the help of known connections. Out of the sixteen participants, we have had the opportunity to interact or work directly with six of them in the past. The rest of the participants were referred by known connections as practitioners or experts. All efforts were made to diversify the pool by recruiting people working for different profiles of companies such as startups, professional services and product companies.

However, the sample is still skewed towards people who have a professional services background and this will have to be factored in when generalizing the findings to non professional services environments. We believe the findings are still relevant as the business model for professional services is only one of the many factors influencing SbD practices and many organisations use professional services in some shape of form through their supply chain. However, it is important to acknowledge this key limitation.

Secondly, due to the limited sample size, we could not observe any industry specific aspects or the impact of regulations on SbD practices. Regulated industries have specific requirements and deeper studies would be required on SbD practices in that context.

Another limitation of the study is the lack of gender diversity of participants. While efforts were made to recruit female candidates, the referrals of senior architect and practitioners were primarily male. While the participants were diverse from geographical, cultural, ethnicity and experiences, we have to acknowledge the significant limitation.

Finally, since my long association with a leading Cloud provider, there could be a bias and predisposition among the candidates recruited based on my connections.

5.5 Future research

The aim of our study was to observe SbD practices in Agile Public Cloud environments in an exploratory manner and open up ideas for further research. While SbD has vast opportunities for further research, there are three areas we identify from this study that requires further deeper empirical research. The first one being the impact of the shared responsibility model with Cloud providers on security. There are technical and non-technical areas that needs further empirical research such as complex hybrid or multi-cloud scenarios, impact of stakeholder understanding of the shared responsibility model on investments and organisation capability development. Another opportunity for research is the effectiveness of organisation policy and compliance programs in Agile Cloud environments. The next opportunity for future research is the impact of security mindset in Agile teams delivering Cloud solutions. Specifically, determining the best suited training approach to cultivate this mindset can help bridge the cybersecurity talent shortage, organisations face continue to face. Finally, the next area of research is the impact of individual and team SA on SbD practices. Since its origins with fighter pilots and military, the model has found successful applications

in other fields that operate in a constraint environment. While there has been some work done in this space, they have been narrowly focused such as how a user-centric visualisation can support data exfiltration anomalies in the Financial industry [58], or identify relationship between drivers knowledge and awareness and their response to cybersecurity attacks in autonomous vehicles. There is an opportunity to study impact of SA in the broader context of SbD . Given that SA has its roots in cognitive sciences, it supports an interdisciplinary approach to future work in SbD.

6 Conclusion

Our study explored the practices and challenges organizations face when implementing Security by Design (SbD) in delivering Cloud-based solutions. Through semi-structured interviews with 16 practitioners of varying seniority levels, we identified nine key practices that support SbD in organizations, including Security Education Training and Awareness (SETA), technical capabilities, security requirements, and solution architecture and design. Our participants also highlighted challenges and barriers, such as the Cloud operating model, changing threat landscape, tools, processes, and security skills shortage. From an organizational, technical, and behavioural perspective, we discuss these results and provide ideas for future work. Future research opportunities include exploring the effectiveness of different approaches to SETA, the impact of SA on SbD practices, and the development of tools and processes to support SbD in the Cloud.

For practitioners in organizations, it is crucial to embrace a culture of security and invest in the development of technical and behavioural capabilities to support SbD. With an ever-changing threat landscape in the Cloud, taking a proactive approach to security should become an imperative. This means shifting away from a "penetrate and patch" approach and towards a more proactive "shifting left" approach. This is important for society at large as more systems are leveraging the Cloud and protecting these systems helps protect against attacks and data breaches that can have a broader consequence. Organizations must anchor their SbD approach on the value they place on security, informing key decisions such as investments in training, tools, and automation. This is particularly important in an environment where there is shortage of skills and an increased competition for available investments. The flexibility of innovative security controls and the ease of provisioning of services in the Cloud can become a double-edge sword that needs to be handled with care.

While Cloud providers have some responsibility for security, companies that use their services share a large portion of the responsibility and are ultimately accountable to their customers and stakeholders. In fast paced environments, these organisations may struggle to keep up with the pace of change, especially when it comes to policies and compliance. Ultimately, it will come down individuals and their awareness of the risks, and their ability to make the right decisions in support of SbD practices. With the security skills shortage in mind, we have an opportunity to broaden our perspective on "shifting left" and consider the role of educational institutions in cultivating a security mindset and promoting security awareness on a larger scale.

7 Acknowledgements

A number of people have significantly contributed to this work. I would like to start off by thanking my interview participants, who have taken time out of their busy schedule to support my thesis. My supervisors Els and Cristina for their valuable guidance, patience and availability throughout the process. My managers, collegues and my company for their flexibility in accommodating my classes and course schedules. Last but not the least, my wife Suja, daughter Sneha and son Abhi, who have been relentlessly cheering me on.

8 References

[1] "Accelerating digital transformation through cloud | McKinsey." Accessed: May 08, 2023. [Online]. Available: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/how-cios-and-ctos-can-accelerate-digital-transformations-through-cloud-platforms

[2] "Public cloud computing market size 2023," Statista. Accessed: May 26, 2023. [Online]. Available: https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/

[3] "Flexera 2023 State of the Cloud | Report." Accessed: May 04, 2023. [Online]. Available: https://info.flexera.com/CM-REPORT-State-of-the-Cloud

[4] "Cloud assets the biggest targets for cyberattacks, as data breaches increase | Thales Group." Accessed: Jan. 06, 2024. [Online]. Available: https://www.thalesgroup.com/en/worldwide/security/press_release/cloud-assets-biggest-targets-cyberattacks-data-breaches-increase

[5] H. Jahankhani, G. Me, D. L. Watson, and F. Leonhardt, "Secure by Design: Considering Security from the Early Stages of the Information Systems Development Haralambos Mouratidis," in *Handbook Of Electronic Security And Digital Forensics*, Singapore: World Scientific Publishing Company, 2009.

[6] S. Kang and S. Kim, "CIA-level driven secure SDLC framework for integrating security into SDLC process," *Journal of ambient intelligence and humanized computing*, vol. 13, no. 10, pp. 4601–4624, 2022, doi: 10.1007/s12652-021-03450-z.

[7] "Microsoft Security Development Lifecycle." Accessed: Jan. 05, 2024. [Online]. Available: https://www.microsoft.com/en-us/securityengineering/sdl

[8] “The CLASP Application Security Process.” Accessed: Jan. 05, 2024. [Online]. Available: https://cwe.mitre.org/documents/sources/TheCLASPApplicationSecurityProcess.pdf
[9] M. Haranas, “Microsoft, AWS, Google Cloud Market Share Q3 2023 Results | CRN.” Accessed: Jan. 06, 2024. [Online]. Available: https://www.crn.com/news/cloud/microsoft-aws-google-cloud-market-share-q3-2023-results
[10] J. Surbiryala and C. Rong, “Cloud Computing: History and Overview,” in *2019 IEEE Cloud Summit*, Aug. 2019, pp. 1–7. doi: 10.1109/CloudSummit47114.2019.00007.
[11] martinekuan, “Azure Application Architecture Fundamentals - Azure Architecture Center.” Accessed: May 04, 2023. [Online]. Available: https://learn.microsoft.com/en-us/azure/architecture/guide/
[12] A. Singh and K. Chatterjee, “Cloud security issues and challenges: A survey,” *Journal of Network and Computer Applications*, vol. 79, pp. 88–115, Feb. 2017, doi: 10.1016/j.jnca.2016.11.027.
[13] H. Tabrizchi and M. Kuchaki Rafsanjani, “A survey on security challenges in cloud computing: issues, threats, and solutions,” *J Supercomput*, vol. 76, no. 12, pp. 9493–9532, Dec. 2020, doi: 10.1007/s11227-020-03213-1.
[14] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, “A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies,” *IEEE Access*, vol. 9, pp. 57792–57807, 2021, doi: 10.1109/ACCESS.2021.3073203.
[15] T. Bullock, “2022 State of Agile Report - 5 Takeaways,” Scrum Inc. Accessed: Jan. 14, 2024. [Online]. Available: https://www.scruminc.com/2022-state-agile-report-takeaways/
[16] P. Spagnoletti, N. Kazemargi, and A. Prencipe, “Agile Practices and Organizational Agility in Software Ecosystems,” *IEEE Transactions on Engineering Management*, vol. 69, no. 6, pp. 3604–3617, Dec. 2022, doi: 10.1109/TEM.2021.3110105.
[17] G. Lee and W. Xia, “Toward Agile: An Integrated Analysis of Quantitative and Qualitative Field Data on Software Development Agility,” *MIS Quarterly*, vol. 34, no. 1, pp. 87–114, 2010, doi: 10.2307/20721416.
[18] M. Fowler and J. Highsmith, “Facilitating change is more effective than attempting to prevent it. Learn to trust in your ability to respond to unpredictable events; it’s more important than trusting in your ability to plan for disaster.”.
[19] “15th State of Agile Report.” Accessed: Jan. 05, 2024. [Online]. Available: https://info.digital.ai/rs/981-LQX-968/images/SOA15.pdf
[20] A. Elbanna and S. Sarker, “The Risks of Agile Software Development: Learning from Adopters,” *IEEE Software*, vol. 33, no. 5, pp. 72–79, Sep. 2016, doi: 10.1109/MS.2015.150.
[21] R. N. Rajapakse, M. Zahedi, M. A. Babar, and H. Shen, “Challenges and solutions when adopting DevSecOps: A systematic review,” *Information and software technology*, vol. 141, pp. 106700-, 2022, doi: 10.1016/j.infsof.2021.106700.
[22] V. Casola, A. De Benedictis, M. Rak, and E. Rios, “Security-by-design in Clouds: A Security-SLA Driven Methodology to Build Secure Cloud Applications,” *Procedia Computer Science*, vol. 97, pp. 53–62, Jan. 2016, doi: 10.1016/j.procs.2016.08.280.
[23] V. Casola, A. De Benedictis, M. Rak, and U. Villano, “A novel Security-by-Design methodology: Modeling and assessing security by SLAs with a quantitative approach,” *Journal of Systems and Software*, vol. 163, p. 110537, May 2020, doi: 10.1016/j.jss.2020.110537.

[24] R. Arizon-Peretz, I. Hadar, and G. Luria, “The Importance of Security Is in the Eye of the Beholder: Cultural, Organizational, and Personal Factors Affecting the Implementation of Security by Design,” *IEEE Transactions on Software Engineering*, vol. 48, no. 11, pp. 4433–4446, Nov. 2022, doi: 10.1109/TSE.2021.3119721.
[25] “What is a CI/CD pipeline?” Accessed: Jan. 07, 2024. [Online]. Available: https://about.gitlab.com/topics/ci-cd/cicd-pipeline/
[26] “What is FMEA? Failure Mode & Effects Analysis | ASQ.” Accessed: Jan. 15, 2024. [Online]. Available: https://asq.org/quality-resources/fmea
[27] “About NIST,” *NIST*, Jul. 2009, Accessed: Jan. 07, 2024. [Online]. Available: https://www.nist.gov/about-nist
[28] “ISO/IEC 27001:2022(en), Information security, cybersecurity and privacy protection — Information security management systems — Requirements.” Accessed: Jan. 07, 2024. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en
[29] “Ebios,” ENISA. Accessed: Jan. 07, 2024. [Online]. Available: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_ebios.html
[30] “SOC 2® - SOC for Service Organizations: Trust Services Criteria.” Accessed: Jan. 07, 2024. [Online]. Available: https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2
[31] M. Alshaikh, “Developing cybersecurity culture to influence employee behavior: A practice perspective,” *Computers & Security*, vol. 98, p. 102003, Nov. 2020, doi: 10.1016/j.cose.2020.102003.
[32] D. Sikolia, D. Biros, and T. Zhang, “How Effective are SETA Programs Anyway: Learning and Forgetting in Security Awareness Training,” *Journal of Cybersecurity Education, Research and Practice*, vol. 2023, no. 1, Jul. 2023, doi: 10.32727/8.2023.13.
[33] A. J. Burns, T. L. Roberts, C. Posey, R. J. Bennett, and J. F. Courtney, “Intentions to Comply Versus Intentions to Protect: A VIE Theory Approach to Understanding the Influence of Insiders’ Awareness of Organizational SETA Efforts,” *Decision Sciences*, vol. 49, no. 6, pp. 1187–1228, 2018, doi: 10.1111/deci.12304.
[34] T. D. Oyetoyan, D. S. Cruzes, and M. G. Jaatun, “An Empirical Study on the Relationship between Software Security Skills, Usage and Training Needs in Agile Settings,” in *2016 11th International Conference on Availability, Reliability and Security (ARES)*, Aug. 2016, pp. 548–555. doi: 10.1109/ARES.2016.103.
[35] M. Shahin, M. Ali Babar, and L. Zhu, “Continuous Integration, Delivery and Deployment: A Systematic Review on Approaches, Tools, Challenges and Practices,” *IEEE Access*, vol. 5, pp. 3909–3943, 2017, doi: 10.1109/ACCESS.2017.2685629.
[36] I. S. E. Souza, D. P. Franco, and J. P. S. G. Silva, “Infrastructure as Code as a Foundational Technique for Increasing the DevOps Maturity Level: Two Case Studies,” *IEEE Softw.*, vol. 40, no. 1, pp. 63–68, Jan. 2023, doi: 10.1109/MS.2022.3213228.
[37] S. Türpe, “The Trouble with Security Requirements,” in *2017 IEEE 25th International Requirements Engineering Conference (RE)*, Sep. 2017, pp. 122–133. doi: 10.1109/RE.2017.13.
[38] M. Shore, S. Zeadally, and A. Keshariya, “Zero Trust: The What, How, Why, and When,” *Computer*, vol. 54, no. 11, pp. 26–35, Nov. 2021, doi: 10.1109/MC.2021.3090018.
[39] Muhammad Ali Babar, Alan W. Brown, and Ivan Mistrik, *Agile Software Architecture : Aligning Agile Processes and Software Architectures*. Amsterdam: Morgan Kaufmann, 2014. Accessed: Apr. 22, 2023. [Online]. Available: https://login.ezproxy.leidenuniv.nl:2443/login?URL=https://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=516109&site=ehost-live

[40] T. Mårtensson, D. Ståhl, A. Martini, and J. Bosch, “Continuous Architecture: Towards the Goldilocks Zone and Away from Vicious Circles,” in *2019 IEEE International Conference on Software Architecture (ICSA)*, Mar. 2019, pp. 131–140. doi: 10.1109/ICSA.2019.00022.
[41] K. L. McLaughlin, “Offense for Defense: The Art and Science of Cybersecurity Red Teaming,” *EDPACS*, vol. 67, no. 5, pp. 18–24, May 2023, doi: 10.1080/07366981.2023.2210013.
[42] K. L. McLaughlin, “Defense Is the Best Offense: The Evolving Role of Cybersecurity Blue Teams and the Impact of Soar Technologies,” *EDPACS*, vol. 67, no. 6, pp. 35–41, Jun. 2023, doi: 10.1080/07366981.2023.2212484.
[43] A. Rashid, H. Chivers, G. Danezis, E. Lupu, A. Martin, and S. Schneider, “The Cyber Security Body of Knowledge”.
[44] “Similarities and differences between CLASP, SDL, and Touchpoints: the activity-matrix - KU Leuven.” Accessed: Dec. 07, 2023. [Online]. Available: https://kuleuven.limo.libis.be/discovery/fulldisplay/lirias1655460/32KUL_KUL:Lirias
[45] M. Ficco, F. Palmieri, and A. Castiglione, “Modeling security requirements for cloud-based system development,” *Concurrency and Computation: Practice and Experience*, vol. 27, no. 8, pp. 2107–2124, 2015, doi: 10.1002/cpe.3402.
[46] “Introducing ChatGPT.” Accessed: Dec. 30, 2023. [Online]. Available: https://openai.com/blog/chatgpt#Iterative%20Deployment
[47] “ChatGPT is everywhere. Here’s where it came from | MIT Technology Review.” Accessed: Dec. 30, 2023. [Online]. Available: https://www.technologyreview.com/2023/02/08/1068068/chatgpt-is-everywhere-heres-where-it-came-from/
[48] M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, “From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy,” *IEEE Access*, vol. 11, pp. 80218–80245, 2023, doi: 10.1109/ACCESS.2023.3300381.
[49] “GitHub Copilot Chat launches into general availability,” SiliconANGLE. Accessed: Dec. 30, 2023. [Online]. Available: https://siliconangle.com/2023/12/29/github-copilot-chat-launches-general-availability/
[50] K. Michael, R. Abbas, and G. Roussos, “AI in Cybersecurity: The Paradox,” *IEEE transactions on technology and society*, vol. 4, no. 2, pp. 104–109, 2023, doi: 10.1109/TTS.2023.3280109.
[51] K. Schoenmakers, D. Greene, S. Stutterheim, H. Lin, and M. J. Palmer, “The security mindset: characteristics, development, and consequences,” *Journal of Cybersecurity*, vol. 9, no. 1, p. tyad010, Jan. 2023, doi: 10.1093/cybsec/tyad010.
[52] H.-J. Kam, P. Menard, D. Ormond, and R. E. Crossler, “Cultivating cybersecurity learning: An integration of self-determination and flow,” *Computers & Security*, vol. 96, p. 101875, Sep. 2020, doi: 10.1016/j.cose.2020.101875.
[53] M. L. Drury-Grogan, K. Conboy, and T. Acton, “Examining decision characteristics & challenges for agile software development,” *Journal of Systems and Software*, vol. 131, pp. 248–265, Sep. 2017, doi: 10.1016/j.jss.2017.06.003.
[54] “Under Pressure: The Effects of Iteration Lengths on Agile Software Development Performance - Kim E. van Oorschot, Kishore Sengupta, Luk N. Van Wassenhove, 2018.” Accessed: May 05, 2023. [Online]. Available: https://journals-sagepub-com.ezproxy.leidenuniv.nl/doi/full/10.1177/8756972818802714
[55] M. R. Endsley, “Situation awareness: operationally necessary and scientifically grounded,” *Cogn Tech Work*, vol. 17, no. 2, pp. 163–167, May 2015, doi: 10.1007/s10111-015-0323-5.

[56] M. R. Endsley, “Toward a Theory of Situation Awareness in Dynamic Systems,” *Human factors*, vol. 37, no. 1, pp. 32–64, 1995, doi: 10.1518/001872095779049543.
[57] M. R. Endsley, “A Systematic Review and Meta-Analysis of Direct Objective Measures of Situation Awareness: A Comparison of SAGAT and SPAM,” *Hum Factors*, vol. 63, no. 1, pp. 124–150, Feb. 2021, doi: 10.1177/0018720819875376.
[58] M.-H. (Miles) Chung *et al.*, “Enhancing cybersecurity situation awareness through visualization: A USB data exfiltration case study,” *Heliyon*, vol. 9, no. 1, p. e13025, Jan. 2023, doi: 10.1016/j.heliyon.2023.e13025.

APPENDIX

1. *Interview questions*

a. How often does your organisation use Agile development methodologies to develop
b. public cloud-based solutions?
c. What Agile methodologies do you leverage for building these solutions?
d. Do you define security by design in your organisation/department/teams?
e. How do you define security by design in your organisation/department/teams?
f. How do you approach Security by design when you build Public Cloud solutions, especially using Agile delivery?
g. What are the factors from security by design perspective that have significantly changed in public cloud-based solutions vs any other solution like traditional on-premises solutions?
h. What are the key barriers and challenges to effectively implementing security by design in Cloud based Solutions?
i. Does Agile culture affect security by design practices when you build public Cloud
j. solutions?
k. How does Agile culture affect security by design practices when you build public Cloud solutions?

2. *Interview schedule*

Participant	ID	Role	Business	Geography	Interview Date
P1	INT019	CISO	Professional Services	Asia	20/09/2023
P2	INT009	Principal Engineer	Product	North America	19/09/2023
P3	INT022	Software Architect	Professional Services	Europe	20/09/2023
P4	INT001	Cloud Architect	Professional Services	North America	25/08/2023
P5	INT004	Architect	Professional Services	North America	04/09/2023
P6	INT005	Architect	Professional Services	Europe	30/08/2023

P7	INT007	Chief Architect	Professional Services	Europe	15/09/2023
P8	INT015	Security SME	Professional Services	Asia	13/09/2023
P9	INT011	CISO/Security SME	Product	Europe	05/09/2023
P10	INT018	CTO	Startup	Asia	31/08/2023
P11	INT014	Cyber Security Executive	Startup	North America	05/09/2023
P12	INT017	Architect	Professional Services	Asia	13/09/2023
P13	INT003	CTO	Product	Europe	18/08/2023
P14	INT021	Cloud CTO	Professional Services	Europe	10/01/2023
P15	INT011	Security SME	Product	Europe	05/09/2023
P16	INT019	Security SME	Professional Services	Asia	20/09/2023

3. *Information sheet shared with participants ahead of the interviews*

Participant Information Sheet

Security by Design in an Agile Public Cloud world: Factors that impact security by design of public cloud-based solutions using Agile development methodologies.
Department: Faculty of Governance and Global Affairs, University of Leiden, Netherlands
Name and Contact Details of the Researcher: Ramshanker Gopal Krishnan,
r.gopal.krishnan@umail.leidenuniv.nl

You are being invited to take part in a research project. Before you decide it is important for you to understand why the research is being done and what participation will involve. Please take time to read the following information carefully and discuss it with others if you wish. Ask me if there is anything that is not clear or if you would like more information. Take time to decide whether you wish to take part. Thank you for reading this.

1. **What is the project's purpose?**
   Software plays a crucial role in cyberspace. More organizations are becoming increasingly digital. They leverage innovative technology to create new experiences for their customers and transform their own businesses. The availability of storage, network, and compute resources on demand through the public cloud infrastructure has helped fuel this Digital Transformation journey. As organisations transform, there is an increasing need for speed to stay competitive in the market. This has led to them to adopt Agile methodologies to develop their digital platforms and solutions. These platforms and solutions make up a critical part of cyberspace and the security of these solutions impact beyond the organisations that create them. Public cloud and Agile methodology adoption requires a cultural and behavioural change within organizations, including how decisions are made, as it tries to address two dynamic aspects that of business requirements as well as rapidly evolving Public Cloud components. The aim of the study is to understand from experts and practitioners how security by design works in the real world for public cloud-based solutions that are built with Agile development methodologies.
   The study is a part of my master's thesis project and will conclude in December 2023. For the research, key experts in the industry who build public cloud bases solutions leveraging agile methodologies will be interviewed for their insights.

2. **What will happen to me if I take part?**
   You will be asked to attend an interview to share with the researcher your experiences on the following questions:
   - How often does your organisation use Agile development methodologies to develop public cloud-based solutions?
   - What Agile methodologies do you leverage for building these solutions?
   - Do you define security by design in your organisation/department/teams?
   - How do you define security by design in your organisation/department/teams
   - How do you approach Security by design when you build Public Cloud solutions, especially using Agile delivery?
   - What are the factors from security by design perspective that have significantly changed in public cloud-based solutions vs any other solution like traditional on-premises solutions?
   - What are the key barriers and challenges to effectively implementing security by design in Cloud based Solutions?
   - Does Agile culture affect security by design practices when you build public Cloud solutions?

- How does Agile culture affect security by design practices when you build public Cloud solutions?

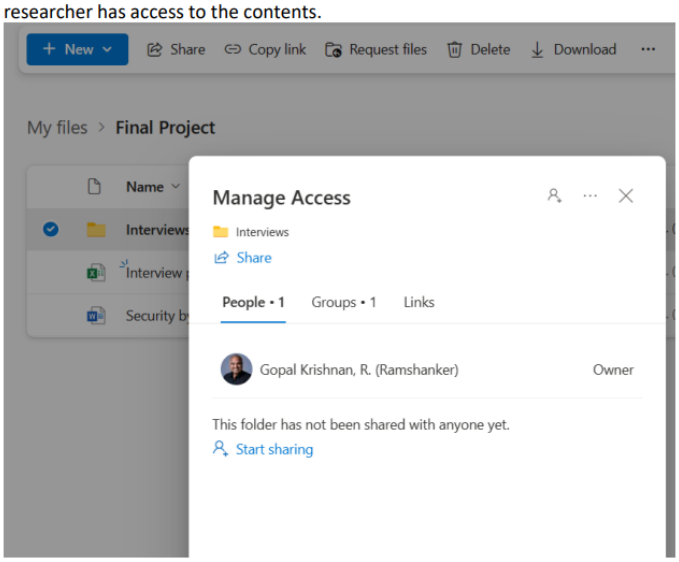
The duration of the interview could be 60-90 minutes and will be scheduled at your convenience preferably before September 15th, 2023, to provide the researcher time to analyse and author the report. There could be a short follow up call if required for any clarification post the analysis phase.

3. What kind of data will be collected and how will it be handled?

Three types of data are collected within the project

1) Personal data of the interviewees and individuals involved in the observation. These data will be textual (in doc format) and will be stored separately in an anonymized form;
2) Non personal data: relevant concepts and insights. These data will be audio (recorded interviews) and textual (transcripts and notes from observation).
3) Meta data such as demographics, and whether the interview was done on location or by phone/online. These data will be textual (in doc format)

Interview audio/video recordings and transcripts will be stored solely in the resercher's OneDrive that is specifically alloted to every individual by the University. By default, only the researcher has access to the contents.



One important addition to the general GDPR (General Data Protection Regulation) data security and protection rules is that the names and functions of interviewees should be available for the thesis supervisor and 2nd reader (to be able to assess how appropriate the interviewees were for the research) and for the university accreditation committee (they assess whether the supervisors do a proper job offering education). In practice, this means that when thesis is submitted, an annex including the names and functions of interviewees will be added, but that annex is removed before the thesis is sent to the OSC for publication in the public thesis repository. That also means that in the body of the thesis interviewees will be referred by numbers (interviewee 1, interviewee 2, etc.)

On successful defense of the thesis and acceptance by the University, the recordings and all raw data collected as part of the interview process will be deleted from the repository. Only the anonymised data and transcripts will be retained for further research purposes.

4. **Will I be recorded and how will the recorded media be used?**
   The audio and/or video recordings of your interview made during this research will be used only for analysis and for illustration purposes only. No other use will be made of them without your written permission, and no one outside the project will be allowed access to the original recordings. The transcript of the interview will be shared with you for validation.
   All personal data will be anonymised, and data will be handled in compliance with GDPR.

5. **Will my taking part in this project be kept confidential?**
   All the information that we collect about you during the research will be kept strictly confidential and in compliance with GDPR. You will not be identified in any ensuing reports or publications. No end customer name, people reference that are specific to your organisation will be shared. If there is a specific need with your permission, only anonymised references will be made

6. **How will data security and protection of sensitive data be taken care of during the research?**
   No sensitive data are to be collected during the project. Personal data will be anonymized before storing the interview and observation data in the secure OneDrive storage. For verification purposes, the relevant researchers will have access to the pre-anonymization data. The latter will be stored separately from the anonymized data in a secured place with limited access rights. Anonymizing the personal data will be done in accordance with the best practices of the Leiden Centre for Digital Scholarship. This means that: - Identifiers such as the name of the interviewee will be removed and replaced by numbers; - The precise function of the interviewee in the organization will be replaced by the larger category; - The precise organization will be replaced by the size of the organization (SME or large enterprise) and an indicator of the sector (public or private and the larger category in order not to make the data traceable to the individual); - An anonymization log containing all removals and replacements will be created and stored separately from the anonymized data files in a secure place with limited access rights.

7. **What are the possible disadvantages and risks of taking part?**
   We do not foresee any risks in taking part in this academic research.

8. **What are the possible benefits of taking part?**
   Whilst there are no immediate benefits for those people participating in the project, it is hoped that this work will help create clarity on the key factors that impact cybersecurity in public cloud and identify potential areas for further research to support broader cybersecurity efforts. The outcomes of the research and the paper will be made available to you for your consumption.

9. **What if something goes wrong?**
   Your concerns and complaints can be raised with the research supervisor Dr. Els de Busser at e.de.busser@fgga.leidenuniv.nl

10. **Limits to confidentiality**
    Confidentiality will be respected subject to legal constraints and professional guidelines.

11. **Will you process and/or store personal data during your project?**
    The limited amount of personal data that will be collected during the project (see above) will be anonymized and the individuals involved will be informed of this prior to their cooperation to the project. As a matter of precaution, the data will only be collected after obtaining the informed consent of the person involved. Obtaining consent will be done in compliance with the requirements of the GDPR.

12. **What will happen to the results of the research project?**
    The results of the research will be presented as part of the master's program and will be shared with you directly by the researcher for your consumption.

13. **Do I have to take part?**
    It is up to you to decide whether to take part. If you do decide to take part, you will be given this information sheet to keep (and be asked to sign a consent form). You can withdraw at any time without giving a reason by emailing me to the address above. if you decide to withdraw you will be asked what you wish to happen to the data you have provided up that point.

Thank you for reading this information sheet and for considering taking part in this research study.

---

4. *Code Book*

Cloud Operating Model
Cloud Operating Model: Cloud Architecture
Cloud Operating Model: Costs and ROI
Cloud Operating Model: Ease of provisioning new services
Cloud Operating Model: Enforcing regulatory needs
Cloud Operating Model: Security Capability
Cloud Operating Model: Shared responsibility model
Cloud Operating Model: Vendor lockin
Definition of SbD
Definition of SbD: CIA Triad
Definition of SbD: Compliance
Definition of SbD: Culture and Mindset
Definition of SbD: DevOps
Definition of SbD: Frameworks
Definition of SbD: Lifecycle Approach
Definition of SbD: Risk Management
Definition of SbD: Target protection
Factors influencing practices
Factors influencing practices: Automation
Factors influencing practices: Business model
Factors influencing practices: Monitoring
Factors influencing practices: Prioritization in Agile Decision making
Factors influencing practices: Team Model
People and Organisation
People and Organisation: Business Value
People and Organisation: Culture
People and Organisation: Customer awareness
People and Organisation: Employee Readiness
People and Organisation: Leadership support
People and Organisation: Resourcing
People and Organisation: Team Model & Responsibilities
Process and Methods
Process and Methods: Agile Decision making
Process and Methods: Assurance
Process and Methods: Clear Security Specifications
Process and Methods: Implementation
Process and Methods: Operations
SbD practices
SbD practices: App and Data Security
SbD practices: Architecture & Design
SbD practices: Assurance
SbD practices: Dedicated Security team
SbD practices: Governance
SbD practices: Security controls
SbD practices: Security Policy & Requirements
SbD practices: Security Training
SbD practices: Technical Capabilities

SbD practices: Threat Analysis
Sentiment
Sentiment: Challenge
Sentiment: Enabler
Threats
Threats: Increased Surface area
Threats: Rapidly changing environment
Threats: Sophistication of attacks
Tools and Technologies
Tools and Technologies: Complexity
Tools and Technologies: Fragmentation
Tools and Technologies: Pace of change
Tools and Technologies: Standards, Patterns and Practices
Tools and Technologies: Supply Chain and Third party

5. *Quotations per code*