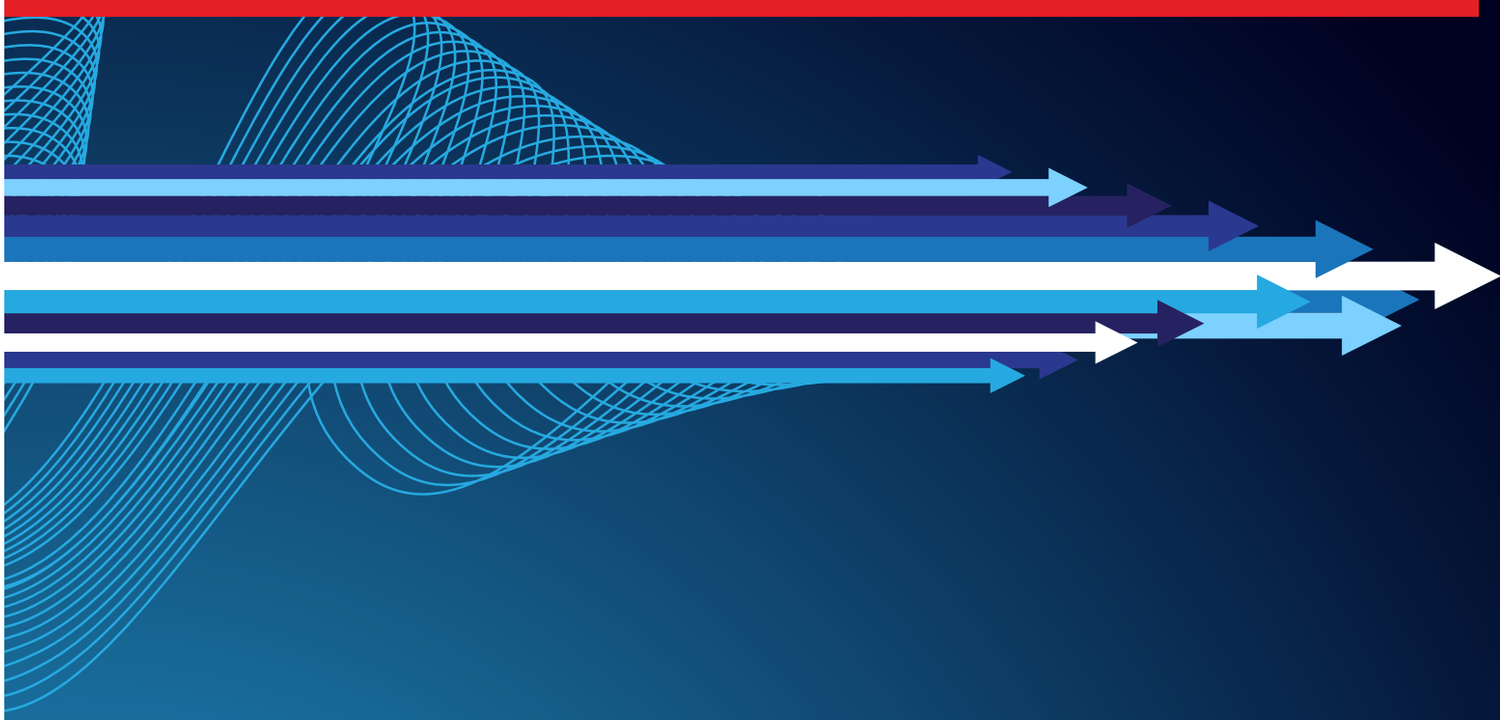
October 2021

Automating for Success

Why Infrastructure Automation is a Prerequisite for Asia's Financial Institutions to Succeed Today and Tomorrow



A report from Kapronasia in collaboration with Red Hat

Contents

Methodology

Kapronasia conducted both primary and secondary research in Asia to obtain the most relevant insights from the industry around Infrastructure Automation.

Secondary Research: Sources included but were not limited to, market intelligence reports and studies by industry experts and professional services networks, white papers, educational materials, media articles, and marketing collateral.

Primary Research: Interviews were secured from relevant players across the ecosystem, including financial institutions and industry experts.

Executive Summary

Financial institutions (FIs) across APAC are adopting modern, distributed IT architectures, along with **Agile and DevOps practices** in response to widespread disruptions caused by rapid changes in competition, demand, technology, and regulations. Such a response, however, is also dramatically increasing the operational complexity of FIs' infrastructure environments. FIs increasingly complicated IT architectures and environments require continuous updates at the application level, the data level, and the infrastructure level and a multitude of infrastructure configurations at any point in time.

If FIs want to streamline their operations and seamlessly integrate these new and existing IT resources into an optimized, manageable environment, infrastructure automation is a prerequisite. By adopting **infrastructure automation** and applying Agile and DevOps practices at the infrastructure level, FIs ensure that infrastructure changes can be made efficiently and that infrastructure configurations can be spun up quickly, are free of errors, are able to be redeployed, and can be rolled back in case of problems.

FIs across APAC will continue to adopt modern, distributed IT architectures encompassing containerization and the cloud as it enables them to not only better utilize their existing resources, an important driver in an era of pressure to reduce cost-to-income ratios, but to also meet customer expectations for on demand digital services. Such expectations have only increased during the pandemic. To develop cloud-native applications, benefit from the elasticity of the cloud, and deliver a seamless customer journey, infrastructure at scale and on demand is a critical necessity which only infrastructure automation can make feasible.

Moreover, being in a highly regulated and audited industry, FIs are subject to strict compliance, audit, and change control reporting requirements. They need to ensure that they have adequate control over security, access, source control and reporting.

FIs have therefore also started to **apply DevOps practices to security at the infrastructure level**. By embedding security and compliance controls into version control systems and continuous integration and continuous deployment (CI/CD) pipelines, architects can identify and fix errors sooner. This not only helps to reduce the cost of compliance and mundane push button compliance jobs, but it also helps them to become more resilient against cyberattacks. That is going to be especially important as the rise of digital banking and employees working from home increases the vectors of attack.

Finally, as FIs across APAC face greater demands to deliver innovative services faster amid rising competition and customer expectations, the promise of enterprise-wide IT and business automation is appealing. However, getting an entire organization to adopt automation is complex. FIs need a **sustainable automation strategy** and must **create modern IT with new approaches to process and collaboration**.

As FIs embark on automation they are going to need a framework for managing an organization-wide automation adoption journey. That journey will encompass multiple facets from introducing new technology to aligning teams on standard practices to orchestrating powerful workflows that fit with FIs evolving business objectives.

Key Findings

FIs' business environments are becoming increasingly complex and volatile making it more important than ever for organizations to be able to respond and adapt quickly.

In response FIs across APAC are adopting hybrid/multi-cloud architectures, along with Agile and DevOps practices. These are dramatically increasing the operational complexity of FIs' infrastructure environments.

DevOps and automation below the line at the infrastructure layer has become a critical, non-negotiable competency just as it has at the application layer.

Infrastructure automation is a prerequisite if FIs want to streamline their operations and seamlessly integrate these new and existing IT resources into an optimized, manageable environment.

Applying DevOps practices to security at the infrastructure level not only helps to reduce the cost of compliance and mundane push button compliance jobs, but it also helps FIs to become more resilient against cyberattacks.

FIs facing greater demands to deliver innovative services at faster intervals amid rising competition and customer expectations need a sustainable automation strategy. They will need a framework for managing an organization-wide automation adoption journey.

The Case for Infrastructure Automation

Financial Institutions Across APAC are Adopting Modern Agile and DevOps Practices

Financial Institutions (FIs) across Asia-Pacific are experiencing widespread disruptions caused by rapid changes in competition, demand, technology, and regulations. As their business environments become increasingly complex and volatile it has become more important than ever for organizations to be able to respond and adapt quickly.

To overcome the challenges and deliver results, incumbents are developing greater business agility to respond quickly to changes in customer needs and stay ahead of the competition. Underpinning this agility is digital transformation, that is, the automating of manual, time-consuming processes and deploying modern application platforms that adapt easily to changing requirements.

A key step in the digital transformation journey is the adoption of Agile and DevOps. Agile methodology is aimed at enhancing the quality and speed of software and services development. DevOps, meanwhile, blends software development and IT operations to shorten the development lifecycle and provide continuous delivery of applications with high quality.[1]

The adoption of Agile and DevOps practices along with modern, distributed architectures across a hybrid/multi-cloud environment enables FIs to develop and release applications to market much faster, meeting customer demand for new products and services at higher frequencies. The result is increased revenue generation and faster time to value.

Such modern constructs also enable the move to online applications. That has been especially pertinent during the pandemic. Stay-at-home notices saw an increase in the demand for digital applications such as payments, peer-to-peer transactions, and online SME lending. By utilizing the elasticity of the cloud, FIs are able to handle spikes in demand for their digital services, providing a better customer experience by maintaining performance even during times of heavy traffic.

Modern, distributed architectures also bestow another benefit. They help FIs optimize and increase the efficiency of their existing resources. FIs no longer have to provision for additional capacity on premise, which for the most part remains underutilized. Instead, access to additional computing capacity is delivered via the cloud on demand. This is critical at a time when FIs across APAC are facing increased pressure to address their cost-to-income ratios and to keep costs on a downward trajectory.

Modern IT Architectures Require Infrastructure Automation

However, FIs' adoption of hybrid/multi-cloud architectures, along with Agile and DevOps practices are dramatically increasing the operational complexity of FIs' infrastructure environments. If FIs want to streamline their operations and seamlessly integrate these new and existing IT resources into an optimized, manageable environment, infrastructure automation is a prerequisite.

Provisioning and configuring infrastructure manually is a time-consuming and costly process. Historically, it required the physical setup of hardware, the installation and configuration of operating system software, and connection to middleware, networks, and storage etc. by professionals. With dramatically shorter software development lifecycles, FIs can no longer afford to wait for servers to be deployed. In addition, if FIs want to manage their complex, diverse environments and capitalize on the cloud's benefits – namely, to have infrastructure at scale, on demand – having developers manually configure and manage complex cloud infrastructures at speed is not feasible. The only option is to have consistent and scalable automation.

1 Bob Violino, "Scaling agile and DevOps for digital transformation," CIO, https://www.cio.com/article/3531389/scaling-agile-and-devops-for-digital-transformation.html

This is where infrastructure automation comes into play. Infrastructure as Code (IaC), a subset of infrastructure automation, is a combination of standards, practices, tools, and processes to provision, configure, and manage IT infrastructure using code and other machine-readable files.[2] Instead of manually setting up on premise and cloud environments, administrators and architects can automate infrastructure provisioning and configuring with IaC.

IaC, therefore, seeks to eliminate the pain points of system configuration, especially the significant time element of configuring a new environment. Each environment needs to be configured individually, and when something goes wrong, it can often require starting the process all over again.

Fully documented, versioned infrastructure is spun up by executing a script rather than having to manually make configuration changes or use one-off scripts to make infrastructure adjustments. Once a team has committed infrastructure configuration to version control, they can apply Agile and DevOps practices such as continuous integration and continuous deployment (CI/CD) pipelines to infrastructure changes. Infrastructure updates can follow a DevOps workflow.[3] Applying DevOps practices to automation scripts ensures they are free of errors, are able to be redeployed on multiple servers, can be rolled back in case of problems, and can be engaged by both operations and development teams.[4]

Infrastructure Automation is Also Required for Security and Compliance

Administrators are also using DevOps for security and compliance. As mixed environments grow, risk correspondingly increases with reduced visibility and control into each system, making manual security and compliance monitoring increasingly difficult. In addition, relationships are often strained between development, operations, and security teams – with security personnel often the last to know about configuration changes and issues.[5]

These tensions have given rise to DevSecOps and the Shift Left movement. DevSecOps sees security teams working closely with the DevOps teams to address security concerns as early in the development lifecycle as possible. Shifting Left meanwhile means information security is built into the application process from the beginning of the development lifecycle. By performing security checks and audits earlier in the development lifecycle it becomes easier to find flaws and potential issues.

As regulators across APAC tighten their oversight over FIs the complexity and cost of compliance is increasing. Being in a highly regulated and audited industry, FIs are subject to strict compliance, audit, and change control reporting requirements. They need to ensure that they have adequate control over security, access, source control and reporting.

Applying DevOps practices to security at the infrastructure level not only helps to reduce the cost of compliance and mundane push button compliance jobs, it also helps FIs to become more resilient against cyberattacks. That is going to be especially salient as the rise of digital banking and employees working from home increases the vectors of attack.

By embedding IaC security and compliance controls into version control systems and CI/CD pipelines, architects can start identifying and fixing errors earlier, optimizing the use of resources. Using infrastructure automation can help FIs to provision resources, make configuration changes, and run commands across multiple environments, consistently and reliably. Financial services firms need automation capabilities to deploy applications and to ensure that distributed architectures are consistent and compliant with the required security.

2 Tomas Fernandez, "What is Infrastructure as Code?," Stackpath, https://blog.stackpath.com/infrastructure-as-code-explainer/

3 Ian Buchanan, "How Infrastructure as Code (IaC) manages complex infrastructures," Atlassian, https://www.atlassian.com/continuous-delivery/principles/infrastructure-as-code

4 Christopher Null, "Infrastructure as code: The engine at the heart of DevOps," TechBeacon, https://techbeacon.com/enterprise-it/infrastructure-code-engine-heart-devops

5 Red Hat, "Automated security and compliance for financial services," https://www.redhat.com/en/resources/automate-security-compliance-overview-financial-services

Modern Infrastructure for a Modern World

Capitalizing on the Benefits of Modern IT Architectures, Agile and DevOps

FIs across APAC are responding to pressures in their environment by adopting the DevOps philosophy for getting code into production fast, reliably, with a lower lead time, and with lower change failure rates; the success of which is measured against the DORA four key metrics.[6] As well as applying such a model at the application layer, it has become increasingly apparent that applications and data systems also need an Agile infrastructure to scale with them. That requires the implementation of DevOps at the infrastructure layer as well.

Case Study: Asia Development Bank (ADB) (Part 1)

The ADB illustrates how FIs are indeed starting to apply Agile and DevOps practices at the infrastructure level. Krista Lozada, Senior IT specialist, Innovation & Engineering at the Bank says, "Agile methodologies and DevOps are not usually associated with the infrastructure layer. As principles, these have been matured and perfected at the application level for application development. We were not used to thinking about DevOps as a clear answer to our infrastructure challenges. Our team had to adapt."

In terms of the approach taken, ADB's core team has broken the infrastructure down into modules, which, Ms. Lozada says, is critical to ensuring that a set of configurations are always followed. She likens these modules to Lego blocks. If someone wants, for example, three virtual machines (VMs) with a load balancer in front and a public IP attached they do not need to build the configuration from scratch. They can attach the modules like Lego blocks to achieve the automation use case required.

Ms. Lozada says it is very "software development like." Her team have CI/CD pipelines that run every day to conduct unit tests on the new modules that the team have created to validate them to a certain state. Ms. Lozada says that they use "real DevOps people" who understand DevOps principles to apply software development practices, such as unit testing, to be sure that they have written something that is not going to introduce breaking changes.

Ms. Lozada explains that because their philosophy is to only write code once and to make sure that everything is reusable, they have a DevOps pipeline to tokenize everything. The environment, therefore, is a variable that the pipeline can inject. Likewise, they have a stage for Test, User Acceptance Testing (UAT), and Production. They also have a stage for regions. While it is currently hard coded to be SE Asia, it is a variable as well. If they were asked to change the region to Australia, they would only have to change one variable – which would take five seconds – to spin up the same infrastructure without any repercussions. That is because, Ms. Lozada says, they have "abused" CI/CD and how they handle stage files. "We know we can reuse the same code against 10,000 environments," she says.

Ms. Lozada explains why IaC is now such a prerequisite. Before automation, she says, if someone wanted infrastructure, they would have to file a ticket. Somebody on the other end would then have to process it while probably also needing to talk to network, storage, and the OS teams as well. Historically, when VMs lived for a very long time and FIs did not manage a lot of infrastructure, that model worked. However, as FIs move more workloads into the cloud, infrastructure teams are required to spin up more VMs and that would require the processing of thousands of tickets a day. There is also a cost impact because FIs are no longer paying for a VM that sits in their datacenter. They are paying by the hour for it. That means, Ms. Lozada says, "that somebody has to spin up the infrastructure that is needed and then discard it at the end of the day. So, it is definitely a model that cannot scale."

6 The DevOps Research and Assessment (DORA) framework essentially looks at four key metrics divided across the two core areas of DevOps. Deployment Frequency and Mean Lead Time of Changes are used to measure DevOp speed, while Change Failure Rate and Mean Time to Recovery are used to measure stability.

Case Study: Ascend Money[7]

Ascend Money, a fintech, operates across the APAC region, with headquarters in Thailand and offices in Vietnam, Philippines, Cambodia, Myanmar, and Indonesia. Its mission is to help customers do more with their money and improve the lives of the region's underbanked population.

Rapid growth through acquisitions meant that Ascend Money's teams in each country had different approaches to developing and deploying digital applications, preventing efficient collaboration. The company sought a way to improve collaboration and delivery times for new products and features while also providing customized services for each local population. Each day, Ascend Money builds and releases around 100 applications - and this number is growing.

To further ensure consistency across teams and locations, Ascend Money has used Red Hat's OpenShift Container Platform and Red Hat Ansible Tower to automate many repetitive manual tasks, including deploying new environments and making global configuration changes.

OpenShift includes built-in automation capabilities that help Ascend Money's teams focus on creating and updating new, valuable services, rather than routine tasks. In addition, Ansible Tower helps support consistent automation through Ansible Playbooks shared between different countries' teams.

As a result, tasks that previously took one week can now be completed in just 2-3 days, and the company can now support nearly 200 developers with a technology operations team of only six people.

Compliance and Security

As regulators around the globe tighten their regulatory oversight over already highly regulated industries such as the financial services industry (FSI) and the world becomes more digitally native with digital-first financial institutions, security, compliance, and governance have risen to the top of the agenda at FIs across APAC.

That has led to an explosion of security tools with a concomitant growth in security orchestration, automation, and response (SOAR). That is the orchestration and automation of security compliance across a plethora of tools, providing FIs with a level of resiliency, adaptability, and agility to alleviate the constraints imposed on them by ever more onerous compliance requirements. As regulatory oversight increases, it will be essential for FIs to adopt security automation and tie-up all their different security

7 Red Hat, "Ascend Money builds applications with Red Hat OpenShift and Ansible," https://www.redhat.com/en/resources/ascend-money-case-study

tools within their architecture. To do this successfully, FIs can integrate these tools into their existing playbooks to help them enhance and extend the level of compliance and automation that they have with a security focus.

With security, compliance, and governance now a major subcommittee on every board across APAC, the requirement for a standardized operating environment has never been more important. The need to apply DevOps and automation below the line at the infrastructure layer has therefore become a critical, non-negotiable competency just as it has at the application layer. With containerization, container platforms, and all the components that make a container platform work, infrastructure updates are now occurring almost weekly. Multiple interdependencies are needed, updates are deployed on premise and in the public cloud, all while FIs try to ensure that their applications continue to work together seamlessly. If these organizations are not using automation and applying a DevOps model of CI/CD for infrastructure as code, then it becomes exceptionally challenging to be able to manage that standard, secure, reliable, and compliant platform.

In order to achieve consistency, reusability, standardization, compliance and provide an audit trail of what changes have been made at the infrastructure level, DevOps and automation at the infrastructure layer has now become a necessity for orchestrating and deploying those updates, certifying them, ensuring that they are patched, that everything works together and enabling a roll back if it fails. Using playbooks to orchestrate different infrastructure components to be configured, deployed, integrated, and then tested, while also providing a record of review reduces change failure rates, improves uptime, reduces downtime, and catches errors earlier when changes are being made.

Case Study: Global insurer with a Singapore presence

The Chief Data Officer of a global insurer based in Singapore says that in the past, when infrastructure was configured, it would have to be checked manually by security engineers or vendors. However, with automation and DevSecOps, the company can codify compliance rule sets into IaC as early as possible, when the infrastructure is being set up. The code or the container can be checked all the way to the end of the pipeline where it is being deployed and going into Production.

The checks make sure that the team can go live properly and securely and if there are any deviations or non-adherence it will be flagged to the security, application, or project team to let them know so that they can get it fixed or if it warrants a development approval, the team can go through the identification process within the automation tool itself to have the security risk or compliance owner approve the deviation.

The Chief Data Officer says, “number one, I think it has definitely helped to make us more secure and to make sure that we comply with the requirements. Number two, it has made us more efficient, in terms of being able to respond and approve these requests very quickly. Most importantly perhaps, there is also a central audit trail all the way end-to-end. We can see exactly where the problem is, how it is being resolved, who approved it, and at what date and time so that in case the MAS [Monetary Authority of Singapore] comes to check, it is just a download page report that we can share with them.”

According to the Chief Data Officer, while automation is powerful and allows you to codify compliance requirements, there are two associated risks, which they have discovered as a company. The first is that it can lead to a lot of false positives. The codified rule sets are cascaded out to the entire platform, but one size does not fit all. That is because you have different business severity and applications of different criticality. The risk is of over complicating it by having very granular rule sets which cause a lot of false positives that will end up creating more inefficiencies for the project team, the application team, and the compliance security owner that have to review and resolve these. The solution adopted by the company

was to create more granular rules at the beginning and then loosen these over time.

On the flip side, the second risk, according to the Chief Data Officer, is that the company found that there were teams who were purposefully creating rule sets that were too generic. As an example, the Chief Data Officer highlighted a rule set that was created to track whether Port 22 was still open for solid-state hybrid drive (SSHD). While tracking open ports is a good rule, this one is too simple, he says. Other ports need to be checked as well. However, because of the information asymmetry between compliance and the security engineer, the former will think that the latter is doing their job by checking the correct ports, but in actual fact they are not. The engineer in this case made the rule set too loose because it resulted in less work and quicker approvals but resulted in a high level of attacks. The Chief Data Officer says that their rule set is constantly evolving and there is now an approval process, whereby the security team, the risk team, and the compliance officer, as well as the architecture team need to review the new rule sets that come into play, to make sure that these make sense.

Case Study: Asia Development Bank (ADB) (Part 2)

Krista Lozada at ADB explained why it was critical for the financial service industry to apply DevOps at the infrastructure level. "Automation is very powerful," she says. It can be written and abused in such a way that would be antithetical to FIs like ADB because of the onus on compliance and security. She says, "that is where DevOps comes in, because you can Shift Left and catch the errors such as security issues at the gates as early as possible."

Ms. Lozada says that one of their biggest mandates is that their IT people must use the modules to spin up infrastructure. To that end the team have certain mechanisms in place to ensure that people do so. By using the enterprise version of Red Hat's Ansible, for example, Ms. Lozada and her team were able to introduce governance. By using modules, certain configurations are hard coded, meaning that developers cannot override those configurations.

Ms. Lozada says that they want to Shift Left as much as possible. So, for a static configuration of the VM, Ms. Lozada and her team will make sure that the first instance of the image has all the security agents in there if possible. If a developer wants to have a Linux server, for example, it is going to fetch the image that the team has created in Alpaca, which has already been configured and hardened. The IaC platform is then going to apply all the security and monitoring agents such as CrowdStrike and DataBlock and then do all the necessary policies. That means that all the security elements have already been baked in at the moment the developer gets the VM. Ms. Lozada makes the point that if a person was manually spinning up the infrastructure, there is a possibility that they might forget to add the security or monitoring agents. Ms. Lozada says, "we are not leaving anything up to chance."

That is for immutable infrastructure, that is infrastructure that does not change and once provisioned will be in the desired state with all the required standards included. However, Ms. Lozada and her team also recognize that some of the new workloads that ADB have will require mutable infrastructure, that is infrastructure whose state does need to be changed. In these cases, Ms. Lozada says, that is where configuration management comes in. Ms. Lozada illustrates with an example. What will often happen, she says, is that if a process is not working with a VM, the developer will turn off a security agent in order to troubleshoot, but then forget to turn it back on.

"That is where Ansible comes in," Ms. Lozada says. If developers are causing infrastructure to drift from the desired state that is required, Ansible's configuration management tool will return the infrastructure to the desired state by switching the security agent back on again. That enables Ms. Lozada and her team to be certain that everything is going to be one hundred percent compliant all the time. Ms. Lozada and her team know that at any point in time all of their workloads, on all of their infrastructure, are following certain compliance or security postures that are expected.

Conclusion: How ANZ Bank Adopted an Organization-Wide Automation Strategy

The pressure on FIs across APAC to respond and adapt quickly to an evolving complex and volatile business environment will remain for the foreseeable future.

However, FIs today face what first glance appears to be a trilemma or impossible trinity. That is, they need to be **resilient, innovative, and secure** all at the same time. In a traditional world these three imperatives would counteract against each other. Traditionally, an organization could be resilient and secure but not innovative, or if they wanted to be innovative, they would have to sacrifice security. But with automation FIs can achieve the Holy Grail of all three.

For FIs facing greater demands to deliver innovative services at faster intervals amid rising competition and customer expectations the promise of enterprise-wide IT and business automation is appealing. However, getting an entire organization to adopt automation is complex. FIs need a sustainable automation strategy and must create modern IT with new approaches to process and collaboration.

As FIs across APAC embark on automation they are going to need a framework for managing an organization-wide automation adoption journey. That journey will encompass multiple facets from introducing technology to aligning teams on standard practices to orchestrating powerful workflows that fit with FIs evolving business objectives. It is always about focusing on three things: **people, process, and technology**.

This report ends with ANZ New Zealand as a case in point of how the convergence of people, process, technology, culture, and policies can come together to institutionalize automation as a culture and a practice across the entire organization:

The Bank worked with Red Hat to increase productivity and time to market through the adoption of agile practices and automation. Through a residency with Red Hat Open Innovation Labs and use of Red Hat Ansible Automation Platform, ANZ New Zealand reduced the time required for end-to-end DNS provisioning from six days to five minutes, a time savings of 99.4%.

Faced with time-consuming routine and repeatable network operations tasks, ANZ New Zealand decided to transition to a cloud-first approach focused on automation and site reliability engineering. However, many of these IT business processes, including patching and provisioning servers, require a manual governance process around technical work. Automating these tasks can depend entirely on

the adoption of new technology tools, IT processes and behavioral changes, which can be difficult to accomplish. Additionally, ANZ New Zealand sought to develop and establish a culture of new ways of collaborative working in order to support its commitment to talent acquisition and retention.

To help address its transition to a more agile, cloud-first strategy, ANZ New Zealand turned to Red Hat, specifically Red Hat Open Innovation Labs. The immersive residency program aims to help organizations **integrate people, practices, and technology to increase agility** in the development of software and products, **catalyze innovation** and **solve internal challenges** in an accelerated time frame. During the six-week engagement, ANZ New Zealand's teams gained a new understanding of how modern automation technologies like Red Hat Ansible Automation Platform can transform complex IT landscapes. They also became well-versed in Agile development practices, including CI/CD, culminating in the team finding new ways to connect with other corporate groups for more effective work, establishing a new culture of collaboration and community.

As a result, ANZ New Zealand built automation skills through e**xpert-led training on network automation and Agile development approaches.** The skills and tools gained from the Red Hat Open Innovation Labs engagement have enabled the project team to expand the use of Red Hat Ansible Automation Platform and their newfound practices across the wider organization and business units. In addition, since completing the residency, engineers at ANZ New Zealand have been using Red Hat Learning Subscription to continue to grow their skill sets.

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

Please visit https://www.redhat.com

Kapronasia

Kapronasia is a leading provider of market research covering fintech, banking, payments, and capital markets. From our offices and representation in Shanghai, Hong Kong, Taipei, Seoul, and Singapore, we provide clients across the region the insight they need to understand and take advantage of their highest-value opportunities in Asia and help them to achieve and sustain a competitive advantage in the market.

Please visit https://www.kapronasia.com