FINEOS

FINEOS Response to APRA Information Paper:

Outsourcing Involving Cloud Computing Services

Revision: 2.07 - February 2020

FINEOS

FINEOS Corporation Ltd. ("FINEOS") reserves the right to make changes to the information in this document without notice of such changes. FINEOS does not accept any responsibility for any errors or omissions in this document.

The software and policies described in this document are furnished under a licence and may be used only in accordance with the terms of such licence. The documentation is issued in confidence for the purposes only for which it is supplied. It must not be reproduced in whole, or in part, or used for tendering or manufacturing purposes except with the consent in writing of FINEOS Corporation Ltd., and then only on the condition that this notice is included in any such reproduction.

No information as to the contents or subject matter of this document or any part thereof, arising directly or indirectly therefrom, shall be given orally or in writing or communicated in any manner whatsoever to any third party being an individual firm or company or any employee thereof without the prior consent in writing of FINEOS Corporation Ltd.

All URLs given were active at the time of going to press. FINEOS makes no guarantee of their continued validity and takes no responsibility for their content.

Written and published by FINEOS Corporation Ltd.

FINEOS

Contents

Tables and Figures

Introduction

The Australian Prudential Regulatory Authority (APRA) introduced *Prudential Standard SPS 231 Outsourcing (SPS 231)*[1] *and Prudential Standard CPS 231 Outsourcing (CPS 231)*[2] in November 2012 and August 2014, respectively, with CPS 231 being updated in July 2017. A further Prudential Standard - *CPS 234 Information Security (CPS 234)*[3] came into force in July 2019. These Prudential Standards document requirements relating to the risk management of outsourcing arrangements, including cloud services.

In July 2015, APRA produced an information paper, titled *Outsourcing Involving Shared Computing Services (Including Cloud)*[4], with a further cloud-specific information paper released in September 2018 - *Information Paper - Outsourcing Involving Cloud Computing Services*[5].

These, together with APRA's *Prudential Practice Guide on the Management of Security Risk in Information and Information Technology (CPG 234)*[6], provide guidance and outline the key principles that regulated Financial Services Institutions (FSIs) should consider when assessing cloud services.

This whitepaper seeks to assist regulated FSIs in understanding how the FINEOS Platform Software as a Service (SaaS) offering allows them to address the key risks and technology controls set out in the Prudential Standards, Prudential Practice Guides and Information Papers to meet their regulatory requirements.

This whitepaper considers outsourcing involving cloud computing with either a heightened, or extreme inherent risk.

Outsourcing is defined in CPS 234 as when an institution engages another party (in this case FINEOS) to perform on a continuing basis a business activity that either is, or could be, undertaken by the institution themselves.

FINEOS' responses to the APRA Information Paper are consolidated from current FINEOS policies and procedures. If further information is needed, please contact FINEOS.

While this whitepaper looks at risk management as it pertains to FINEOS Platform, it is important for each FSI to understand the wider context of adopting cloud services, considering:

- The organisation's strategy and objectives
- The structure of the organisation
- The cultural readiness of its workforce
- Current technologies and how they will integrate with cloud services
- The organisation's existing approach to risk management

[1] Prudential Standard SPS 231 for Outsourcing
[2] Prudential Standard CPS 231 for Outsourcing
[3] Prudential Standard CPS 234 Information Security
[4] Outsourcing involving shared computing services (including cloud)
[5] Information Paper - Outsourcing Involving Cloud Computing Services
[6] Prudential Practice Guide CPG 234 Management of Security Risk in Information and Information Technology

Using a framework such as the AWS Cloud Adoption Framework (CAF)[7], or Microsoft's Security Assurance Framework for Evaluation, (SAFE)[8] in conjunction with the AWS User Guide to Financial Services Regulations & Guidelines[9], may assist in assessing the overall organisational readiness and risk management approach in adopting cloud services.

FINEOS understands that APRA's standards and guidelines are complex. It is recommended where FSIs have not previously engaged with APRA on this matter, that they utilise the services of an experienced third-party specialist organisation, which can advise and assist with any necessary APRA submission.

Intended Audience

FINEOS has prepared this whitepaper to articulate the FINEOS response to the questions raised by certain APRA requirements, specifically *Outsourcing Involving Cloud Computing Services.*

The intended audience of this whitepaper are those who are familiar with the related APRA information papers. Readers are not required to know all the details of the APRA information papers, however some knowledge would be advantageous.

For ease of reference, the format and structure of this document closely follows that of the information paper *Outsourcing Involving Cloud Computing Service.*

[7] AWS - Cloud Adoption Framework

[8] SAFE Handbook

[9] AWS - User Guide to Financial Services Regulations & Guidelines in Australia

FINEOS

FINEOS Platform Definition

FINEOS Platform is a SaaS offering from FINEOS that provides a flexible, secure and cost-effective way of managing Life, Accident and Health Insurers' claims. The service, which includes Claims, Policy Administration, Billing and other insurance services, is built on Amazon Web Services (AWS) and is managed by FINEOS.

FINEOS Platform has been designed using the AWS Well Architected Framework[10], which uses a structured and consistent approach to designing cloud architectures, based on five pillars:

- Operational Excellence
- Security
- Reliability
- Performance Efficiency
- Cost Optimisation

These five pillars help to reduce or mitigate the risks associated with cloud services and to make informed architectural decisions around resilience, performance and availability of cloud services.

FINEOS successfully completed an AWS Well-Architected Framework review in September 2018.

As an AWS Financial Services Independent Software Vendor (ISV) Partner[11], FINEOS is required to demonstrate considerable expertise in AWS within the financial services industry, and to meet several demanding requirements - such as providing use case-specific public client references - as well as successfully completing a comprehensive audit by AWS of its Financial Services solution.

FINEOS holds AWS - Financial Services Competency status. This designation recognises FINEOS for delivery of effective solutions to help insurers manage critical issues pertaining to the industry, such as core systems implementations, data management, navigating compliance requirements, and establishing governance models.

[10] AWS - Well-Architected Framework

[11] Introducing the AWS financial services competency

Risk Management Considerations

FINEOS understands that using a hosted solution may bring associated risks. The aim of this whitepaper is to ensure that any FINEOS client has full trust in the FINEOS Platform solution and to show how FINEOS Platform can help them to meet their regulatory obligations, including:

- Continuing to operate and meet obligations following loss of service and other disruption scenarios
- Preserving the integrity of both critical and sensitive data
- Complying with legislative and prudential requirements
- Ensuring that APRA can fulfil its duties as prudential regulator

Strategy

FINEOS engages in a comprehensive sales process with prospective FSI clients to ensure that the FSI fully understands the FINEOS Platform offering, and that it is a good fit for their business and strategic needs.

Governance

Once an FSI has completed its internal governance process to select FINEOS as its preferred vendor, FINEOS engages in a detailed scoping process outlined in the section of this whitepaper.

It is imperative for FSIs to engage with APRA once the FINEOS Platform solution has been selected so they can elicit any areas of potential concern from APRA prior to proceeding.

FSIs may engage with APRA earlier in the solution selection process where the solution involves extreme inherent risk to provide APRA with feedback on any potential areas of concern.

Solution Selection Process

For FSIs that have no prior relationship with FINEOS, the initial engagement between the FSI and FINEOS is via a competitive tender process.

As part of this process, FINEOS will provide detailed answers to a series of questions, some of which will cover topics such as application and cloud architecture, service operation, solution maintenance and enhancement, as well as more general questions about FINEOS itself, e.g. history, financials, culture, etc.

The competitive tender process will also normally include presentations and showcases to the prospective client, which is another opportunity to evaluate FINEOS. Existing FINEOS clients will typically not require a competitive tender process, for example when moving from an on-premises deployment to a cloud hosted FINEOS Platform.

Prior to starting an implementation project, FINEOS undertakes a process called an Implementation Scoping Study (ISS). The ISS activity has two main purposes:

- From an FSIs point of view, the ISS provides the opportunity to ensure the proposed solution is in alignment with the FSIs enterprise architecture, as well as confirmation of implementation scope and estimates
- From a FINEOS point of view, the ISS allows for a better understanding of the FSIs business context, requirements and technical context; this supports more accurate project scoping and estimation

The ISS is a time-boxed, collaborative activity with the prospective client, and is led by a team of FINEOS Senior Consultants.

Workshops between FINEOS Consultants and the client take place over the course of an ISS. These can cover a wide variety of topics, but are typically grouped into two broad categories:

- Business workshops, focusing on how the business requirements can be met by the solution
- Technical workshops, which focus on security, integration requirements, non-functional requirements and any relevant architecture considerations

The technical workshops are an opportunity for prospective FINEOS clients to better understand the technical detail of the proposed solution and explore areas of additional complexity and/or risk. FINEOS plans the schedule of workshops in collaboration with the client, allowing both parties to table relevant topics.

FINEOS recommends that a Solution Architect from the client be actively involved for the duration of the ISS activity, with support from roles including, but not limited to:

- Business Architect
- Enterprise Architect
- Cloud Architect
- Integration Architect
- Security Architect

As well as roles from within the client's own organisation, the client may also choose to include external resources to support due diligence activities and ensure alignment with the client's architecture.

Transition Approach

FINEOS adopts a staged approach to transitioning clients to FINEOS Platform, this approach is applicable for both new FINEOS clients adopting FINEOS Platform for the first time as well as existing FINEOS clients transitioning to a FINEOS hosted solution.

The approach, which comprises four stages, allows the client to gain a greater understanding of how FINEOS Platform works and how it will enable the client to meet its business needs at each stage, while also helping FINEOS to shape the delivery of the project and transition of the client to FINEOS Platform.

FINEOS follows a predictable approach to onboard all clients, leveraging the speed and agility of cloud technologies to allow FINEOS and client teams to begin the transition earlier than would have been possible with traditional on-premises implementations.

Figure 1 – Staged Approach to Transitioning a Client to FINEOS Platform

Implementation Scoping Study

At the beginning of all client engagements, FINEOS conducts an ISS process with the client. This allows FINEOS to fully understand the client's business needs and for the client to understand the capabilities of FINEOS Platform.

During the scoping study, FINEOS also engages in a *Cloud Launch* exercise which gathers client-specific information for integrations, data migration, security requirements and configuration.

The outputs of the ISS are presented back to the client for review by relevant client governance authorities, including, but not limited to:

- Architecture/strategy governance
- Program Management Office (PMO)
- Financial control

Following the governance review, the ISS outputs are typically incorporated into the business case presented to the client's board or executive committee for approval.

Project

An implementation project is usually commenced following approval to proceed by the client.

FINEOS uses an agile project implementation approach, leveraging industry-standard agile techniques. The project is a collaboration between the client and FINEOS teams and uses visual agile practices and regular software deliveries/reviews.

A core part of the FINEOS implementation approach is to engage with the client's business representatives and end users. They provide regular feedback and acceptance as part of the evolution and delivery of the solution.

This approach maintains a clear focus on business benefits and value when discussing backlog refinement, sprint planning and change management.

As part of the implementation project, FINEOS provisions several environments in the cloud. These are created using Infrastructure as Code

(IaC) to allow for a repeatable, consistent approach to environment provisioning. These environments have lesser security controls than production environments and do not leverage High Availability (HA). No Personally Identifiable Information (PII) data is stored within these environments.

Rigorous governance is a key tenet of FINEOS project implementations. The following items ensure proper control of the project:

- Budget management
- Scope and change management
- Communication plans
- Project schedule
- Project control log
- Project and steering committee reporting
- Account and relationship governance meetings

Service Transition

The service transition stage helps FINEOS and the client jointly plan and manage the move to FINEOS Platform.

Change management is a key component of this, allowing FINEOS and clients to make informed decisions and manage risk.

FINEOS assigns a Release Manager to each FINEOS Platform client for all change management. This allows for a defined engagement model for ongoing change to the client's FINEOS Platform system.

In controlled environments such as production, the Release Manager works with both client and the FINEOS Change Advisory Board (CAB) to ensure that any change is fully understood, and all risks are documented and accepted prior to any change being made.

FINEOS also assigns an Application Support Engineer to each FINEOS Platform client, as the primary contact for any support issues. The FINEOS Application Support Engineer collaborates with the client's own support teams to document and agree a support charter which:

- Outlines the application support processes
- Explains the roles of FINEOS support and related teams
- Outlines the services that FINEOS support can provide
- Defines client responsibilities with respect to production support
- Signifies agreement between the client and FINEOS about these roles, responsibilities, and processes

The Application Support Engineer also works with the client's own teams to help transition users to FINEOS Platform, introducing knowledge, incident management tools and processes to ensure a smooth change-over to FINEOS Platform.

Production/BAU

Production/Business as Usual (BAU) considers both the operational health of FINEOS Platform and the delivery of on-going change via a continuous improvement/BAU process.

Automated infrastructure and application monitoring, together with manual daily checks ensure that the FINEOS Platform service is operating as expected. Any exceptions are automatically raised to the appropriate team for resolution.

Change is divided into three types:

- **Software** - FINEOS application / configuration
- **Platform** - FINEOS middleware / database components
- **Infrastructure** - AWS Infrastructure components

Each change type is further categorised as:

- **Material** - Change that will potentially impact the client either technically, contractually or commercially and requires FINEOS to inform the client of the proposed change
- **Non-Material** - Change that will not impact the client either technically, contractually or commercially and therefore does not require FINEOS to inform them of the change

A change can be either applied through the regular maintenance schedule or via an emergency change process:

- **Planned Changes** - These are presented at the weekly CAB meeting by the Release Manager for approval. Requests must be presented to the CAB at least one week in advance of the change deployment date
- **Emergency Changes** - For emergency changes, the Release Manager contacts the Head of Cloud Operations or VP Cloud Services and an emergency CAB will convene to review the changes

The FINEOS Release Manager presents all proposed changes to the CAB and communicates the CAB decision to the FSI.

Access and Ability to Act

In Australia, FINEOS Platform clients that are APRA-regulated will have an "APRA access clause" within their contract to meet requirements in both *Prudential Standard CPS 231 Outsourcing* (*section 34.)* and *Information Paper – Outsourcing Involving Cloud Computing Service* (APRA access and ability to act).

This clause is in place to allow APRA to fulfil its duties as a prudential regulator.

FINEOS will comply with APRA requirements for access and onsite visits and will also facilitate unobstructed access to relevant documents on request and in a timely manner.

Risk Assessments and Security

FINEOS met the requirements of the AWS Well-Architected Framework in September 2018 in an audit conducted by AWS.

The framework provides a consistent approach to evaluating systems against the qualities required by modern cloud-based systems, and the remediation that would be required to achieve these qualities.

Principles

Strict access controls are in place for FINEOS Information Systems, the FINEOS Network and FINEOS Platform which store FINEOS and/or Client Confidential Information or FINEOS Confidential Restricted Information. Managers are accountable for the access rights of the users under their supervision.

All access controls must support:

- Users agreeing to the acceptable use policy before they are given access to FINEOS Network, FINEOS Platform and/or Information Systems
- Access being controlled using a combination of usernames and passwords, and where required, Multi-Factor Authentication (MFA)[12]
- Access control rules and rights to Information Systems, FINEOS Network and FINEOS Platform are defined in standard user profiles and granted based on business need
- The Principle of Least Privilege (PoLP)[13], which enforces the minimal level of user rights, or lowest clearance level to allow the user to perform his/her role
- Least privilege being applied to processes, applications, systems and devices, in that each should have only those permissions required to perform an authorised activity
- The requirement for authentication credentials to be encrypted during transmission across any network
- Segregation of duty existing between the request, approval and delivery of access
- User access requests being subject to formal authorisation, periodic review and removal
- Enhanced access controls and monitoring for Highly Privileged Access (HPA) accounts
- Four-eyes (two-person) rule being required for change implementation or break-glass, which is described in the Break Glass section of this whitepaper

[12] AWS - Multi-Factor Authentication

[13] Best Practices - Grant Least Privilege

Access Monitoring and Alerting

FINEOS uses real-time alerts to highlight when Identity and Access Management (IdAM)[14] privileges are changed. This will alert FINEOS cloud teams to un-authorised access or when raising of privilege levels occurs.

In the event of an alert, the FINEOS cloud team extracts all relevant Cloud Service Provider (CSP) logs to begin investigation.

On discovering any unauthorised changes within the account, the FINEOS cloud team will immediately roll back the unauthorised changes to the previously valid state and will launch an investigation.

FINEOS Platform leverages AWS tooling to automatically remediation any unauthorised changes at the AWS services layer.

Additional Controls for Highly Privileged Access

Use of HPA credentials must be logged, reviewed and protected from unauthorised use. HPA audit logs must include:

- The resource being accessed
- Any access to FINEOS Confidential Restricted or FINEOS Confidential and/or Client Confidential Information
- User accounts that have system-level privileges granted through group memberships or programs must have unique credentials

Break-Glass

In the unlikely event that a FINEOS employee requires access to a client's confidential information within FINEOS Platform, authorisation must be received from the client's named approvers and the FINEOS Security Council.

Access requires four-eyes principle (two-person) which involves approved FINEOS and client representative(s), all access is time based.

Break-glass is used for access to the following information:

- Client's production database in FINEOS Platform
- Client's data extracts in AWS Simple Storage Solution (S3)[15] buckets or other Client Confidential Information uploaded to S3 buckets
- Client's FINEOS Platform logs which could contain Client Confidential Information (PII)

At the completion of the activity which required the break-glass policy to be invoked, privileged access is immediately revoked.

Vulnerability and Penetration Testing

FINEOS will regularly test for security weaknesses in its systems to establish the current security posture. This can include social engineering exercises and phishing email tests. Penetration testing tools and techniques will be run against systems to identify any potential weaknesses in the security configuration. Penetration testing is performed by independent consultants.

Remediation Management

Once vulnerabilities have been identified, a remediation plan is immediately developed by FINEOS and communicated to the FSI via the Release Manager. The plan includes:

[14] AWS - Multi-Factor Authentication
[15] AWS - Simple Storage Service

- A business information security leader accountable for treatment decision
- Treatment recommendations
- Remediation actions
- Re-test results and any further actions

Testing after Security Incidents

Security Incidents are managed by the FINEOS Security Incident Response Team (SIRT).

The SIRT is established to provide a quick, effective and orderly response to security related incidents.

The SIRT establish an incident response plan and ensure an effective and timely response to incident.

While the SIRT is focused on investigation, containment and remediation, a Crisis Management Team is responsible for communications with personnel outside of the SIRT, including Data Protection Office, Insurance Brokers, Customers, third parties and FINEOS staff.

Any system that has been involved in a cyber-security incident must be re-tested before being re-instated to production status. If already live, testing must be scheduled immediately.

FINEOS has a dedicated global Security Council, which meets regularly to proactively manage information security risks and strategies.

FINEOS provide reports to the client on service risks, incidents, or weaknesses within a contractually defined timeframe. This allows the regulated FSI to fulfil its obligations to notify APRA once aware of any security incidents or weaknesses.

APRA Observed Weakness	FINEOS Response
Inappropriate access rights	FINEOS Platform uses AWS Identity and Access Management (IdAM), and Multi-Factor Authentication (MFA). This aligns with the FINEOS policy to use Role-Based Access Control (RBAC) to grant or deny access to information and data services of the underlying system. User access is restricted based on business needs. FINEOS follows AWS best practices by employing the concept of least privilege. FINEOS actively monitors and audits user accounts and ensure that they are disabled (where applicable) in a timely manner. All access rights and alerts are configured with Infrastructure as Code (IaC) to enforce consistency.
Admin console access and monitoring	All FINEOS Platform AWS accounts utilise Amazon Cloud Trail[16], CloudWatch[17] and GuardDuty[18] to monitor and report on all aspects

[16] AWS - CloudTrail
[17] AWS - CloudWatch
[18] AWS - GuardDuty

APRA Observed Weakness	FINEOS Response
	of system access (console, API etc.). This is managed by the FINEOS Cloud Operations Team.
Encryption Key Management	AWS Key Management Service (KMS)[19] is used for all available services. KMS uses envelope encryption which provides symmetric encryption of data. KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect encryption keys. The service is integrated with services such as AWS CloudTrail to provide logs of all key usage.
Encryption of data in transit and at rest	FINEOS treats all client data as critical information. FINEOS Platform uses AES-256 encryption for all data stored at rest. All data in transit is encrypted using Transport Layer Security (TLS; formerly Secure Socket Layer, or SSL) an industry-standard AES-256 cipher, including connections between FINEOS applications and databases. Connections between FINEOS applications and databases are encrypted using TLS. AWS Config[20] enforces Infrastructure as Code (IaC) created key policies within FINEOS Platform, ensuring that all configured services enforce encryption as standard.
Isolation from 3rd parties	FINEOS Platform separates clients' cloud environments into separate AWS accounts to ensure isolation. Within these accounts, environments run within a Virtual Private Cloud (VPC)[21]. FINEOS applications within the VPC have further logical isolation using application defined subnets.

[19] AWS - Key Management Service
[20] AWS - Config
[21] AWS - Virtual Private Cloud

FINEOS

APRA Observed Weakness	FINEOS Response
Production data in non-production environments	FINEOS Platform separates each client's production and non-production cloud environment at account level. Any data moving between production level accounts is run through an automated data scrubbing process to ensure that all PII data is de-identified before the data is available for lower level (non-production controlled) accounts. This process is automated ensuring that FINEOS staff never have access to PII data outside the Break Glass process detailed in the *Risk Assessment and Security* section of this whitepaper.
Secure posture of disaster recovery environments versus production	FINEOS Australia clients are restricted to using the AWS Sydney region (ap-southeast-2). AWS technology provides multiple distinct locations (availability zones)[22] within this region which are designed to be geographically insulated from each other. FINEOS Platform leverages all the AWS Sydney region (ap-southeast-2) availability zones to protect applications from the unlikely event of failures. AWS Cloud Formation[23] and Code Commit[24] are used to enable automated infrastructure creation and recreation. Should a client need additional backup systems over and beyond what AWS high availability services provide, FINEOS can work with that client to design a solution that meets the specific data storage and recovery requirements.
Misunderstanding of the shared responsibility model	AWS has provided clear guidance on what AWS see as the shared responsibly of clients and service providers using AWS services. FINEOS has applied an additional layer to the model to ensure that FINEOS Platform clients are aware of their responsibilities when using FINEOS Platform. The full shared responsibility model is discussed throughout the Implementation of Controls section of this whitepaper and a graphical view is available in *Appendix 1 – Shared Responsibility Model*.

Table 1 – Technology Risk Controls Associated with Access Controls

[22] AWS - Regions and Availability Zones
[23] AWS - CloudFormation
[24] AWS - CodeCommit

Implementation of Controls

FINEOS has a range of protocols, policies, standards, guidelines and strict practices, aligned to the ISO 27000 family of standards and designed to ensure the rigorously enforced confidentiality, integrity and availability of all client and client's customer information.

These policies govern all access, storage and transmission channels for information both online and offline. The policies are supported and reinforced by an extensive range of supporting systems management and auditing solutions.

FINEOS is undertaking a System and Organisation Controls - Type 2 (SOC 2) attestation. Three trust services - 'Security', 'Availability' and 'Confidentiality' - are being targeted.

Audits

Audits will be initiated on a regular basis by FINEOS. Findings from audits are presented to the appropriate group for remediation or justification.

FINEOS leverages cloud provider and third-party tools for ongoing auditing and monitoring.

FINEOS has completed several client-initiated audits ranging from security questionnaires and score cards to on-site workshops with independent assessors. In addition, FINEOS schedules regular cyber assessments with one of the top five independent consultancies.

Shared Responsibility Model

Responsibility for the cloud service is shared between the client, FINEOS and the CSP (AWS).

Please see Appendix 1 – Shared Responsibility Model for more information.

Ongoing Oversight

FINEOS Platform ongoing oversight is supported by three types of activities:

- Incident and Problem Management
- Change Management
- Service Levels and Reporting

Incident and Problem Management

FINEOS Platform Incident and Problem Management procedures are designed to resolve disruptive or potentially disruptive events with maximum speed and minimum disruption. As part of this, FINEOS Operational Management also identifies root causes of past incidents and seeks to identify and prevent future occurrences.

The goal of Incident and Problem Management is to allow FINEOS to adhere to service availability, meet Service Level Agreements (SLAs), manage client communications and notifications.

With the use of cloud technologies, the resiliency of the system helps make sure that faults, if they occur, have minimal impact on service availability. Resilient design promotes rapid restoration of service in the unlikely event of disruption.

FINEOS drives predictability and resilience through automation and the minimising of human involvement.

Change Management

FINEOS assigns a Release Manager to each FINEOS Platform client for all change management – this allows for a defined engagement model for ongoing change to the clients FINEOS Platform system.

The FINEOS CAB meets on a weekly basis to review and approve / reject any production changes that have been planned for an individual client.

The FINEOS Release Manager presents all proposed changes to the CAB and communicates the CAB decision to the FSI.

Service Levels

The FINEOS Regional Operations Manager has the responsibility of ensuring FINEOS Platform service meets SLAs and performance and operational targets.

On a regular basis, they provide reports to the client on SLA adherence, performance metrics, service risks and issues.

Business Disruption

Financial

FINEOS is a well-respected company recently listed on the Australian Stock Exchange (ASX: FCL) that has been in business for over twenty-five years.

Whilst FINEOS is financially sound, it expects that each new client contemplating buying FINEOS platform or services will complete its own due diligence, which may involve the review of financial records as are required to be disclosed to the ASX.

The FINEOS Platform service is offered on a subscription basis, with a multi-year initial term agreed with each client, under a detailed and comprehensive contract.

Subscriptions, paid annually in advance, are based on the number of users on the system, or some other business volume-related metric as may be agreed between the client and FINEOS.

FINEOS is not aware of any specific financial risks posed by these agreements that would impede its ability to deliver the contracted service.

Technological

FINEOS leverages high-availability solutions for all material components of its cloud architecture while meeting data sovereignty requirements in Australia and New Zealand (ANZ); all data and data backups are stored in the AWS Sydney region data centres.

The FINEOS Platform architecture is designed to minimise business disruption through:

- Being designed to be self-healing where the available AWS service(s) exist
- Leveraging high-availability solutions for all business-critical components of the cloud architecture
- Having a pre-defined automated backup schedule in place for client production data
- Automated database backups occurring daily during a pre-defined backup window
- Database backups having a pre-defined backup retention period

APRA-regulated clients are restricted to using the AWS Sydney region (ap-southeast-2). Within this region, AWS provides multiple distinct locations (availability zones) which are designed to be insulated from each other. FINEOS Platform leverages all the availability zones in the ap-southeast-2 region to protect applications from the unlikely event of failure.

Should a client need additional backup systems over and above what AWS high availability services provide, FINEOS can work with that client to design a solution that meets the specific data storage and recovery requirements.

Recovery Planning

FINEOS has contractually defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Recovery is tested on a regular basis to ensure FINEOS can meet these obligations.

FINEOS Platform uses AWS to deliver its enterprise solutions. AWS provides SLAs to FINEOS for a core set of services, which FINEOS leverage to provide clients highly available, durable and secure solutions.

Should a database restoration be required; AWS' database restoration technology[25] allows for two types of restoration:

- Automatic periodic data backups in conjunction with transaction logs to enable the ability to restore the database instance to any time during the backup retention period
- User-initiated snapshots or automated backups that enable the backup and restoration of database instances to a known state

Both restoration techniques restore to new and separate database instances to ensure physical segregation from the original database instance.

All database restorations are performed in the same AWS account and Virtual Private Cloud (VPC) database-specific subnets to ensure that existing security and encryption configuration is adhered to.

Any FINEOS Platform database instance recovery requires formal sign-off and approval from appropriate client and FINEOS representatives.

The FINEOS Release Manager assigned to the client manages the process, submitting the following information to the FINEOS CAB:

- Reason for artefact restoration and duration of artefact restoration
- Components being rolled back
- Risk and impact of any rollback
- Runbook and rollback strategy
- Validation of the completed rollback in production
- Rollback checklist

Any restoration or data recovery process brings risk. Before any change is implemented to systems, FINEOS will make backups of all code and database artefacts. This is to allow rollback to a known previous working state in the event of a restoration problem.

Disaster Recovery

FINEOS has defined a Disaster Recovery Plan which allows the client to continue to operate in the event of complete failure of the CSPs geographical region.

FINEOS platform can be run on any FINEOS-supported technology stack. This enables clients to have an alternative plan in place to meet critical business and regulatory obligations. FINEOS can consult with clients to help design and size an alternative plan.

Service Monitoring

AWS utilises automated monitoring systems to provide a high level of service performance and availability. Proactive monitoring for both internal and external use is available through a variety of online tools.

FINEOS applications within AWS are designed to extensively monitor key operational metrics. Alarms are configured to notify operations and support personnel when early warning thresholds are crossed on key operational metrics.

Audit and Assurance

FINEOS has a defined audit and assurance model which enables internal and third-party independent audits to be performed.

FINEOS works collaboratively through the client's assigned Release Manager, reporting monthly on contractually agreed aspects of FINEOS Platform. This auditing process is to ensure clients maintain a high level of trust in FINEOS Platform.

[25] AWS - Disaster Recovery

FINEOS has an ongoing responsibility to implement AWS best practices as part of its AWS Well-Architected Framework certification.

Materiality and Notification

Based on APRA's outsourcing Prudential Standards, timing of consultation is based on the regulated entity's inherent risk assessment:

For arrangements with low inherent risk not involving off-shoring, APRA does not expect an APRA-regulated entity to consult prior to entering into the arrangement

For arrangements with heightened risk, APRA would expect to be consulted after the APRA-regulated entity's internal governance process is completed

For arrangements involving extreme inherent risk, APRA encourages earlier engagement as these arrangements will be subjected to a higher level of scrutiny

FINEOS aims to engage with the client's security and risk teams as early as possible to define a risk profile and understand any risk impacts to the client.

This early engagement helps to ensure that the correct risk categorisation is in place and any potential obstacles can be mitigated and reduce potential project delays.

Consultation

It is important to note that APRA requires prior consultation for outsourcing arrangements where offshoring is involved *(CPS 231)*[26].

FINEOS Platform APRA-regulated clients are restricted to using the AWS Sydney region (ap-southeast-2) meaning FINEOS Platform is not considered an offshoring arrangement.

All data and data backups are stored in the AWS Sydney region data centres.

It is imperative for regulated entities to engage with APRA once a solution has been identified so that APRA can provide feedback on areas of potential concern as per notification requirements within CPS 231.

[26] Prudential Standard CPS 231 for Outsourcing

Conclusion

Outsourcing involving cloud computing services is now mainstream, driven by the ever-increasing number of services available from Infrastructure as a Service (IaaS) providers such as AWS and SaaS providers like FINEOS and many more organisations, including Australian FSIs are now seeing the benefits of cloud migration.

Regardless of the IT strategy that organisations choose to follow, they need to adopt an IT security risk management posture that is commensurate with the risks involved.

While this whitepaper provides an assessment of how FINEOS Platform utilises AWS and other services to meet risk management considerations outlined by APRA, FSIs must satisfy themselves that their business operations meet the necessary guidelines, standards and regulatory requirements relevant to its business.

FINEOS will support FSIs on this journey and furnish any additional information to support FSIs who are looking to adopt FINEOS Platform.

FINEOS

Appendix 1 – Shared Responsibility Model

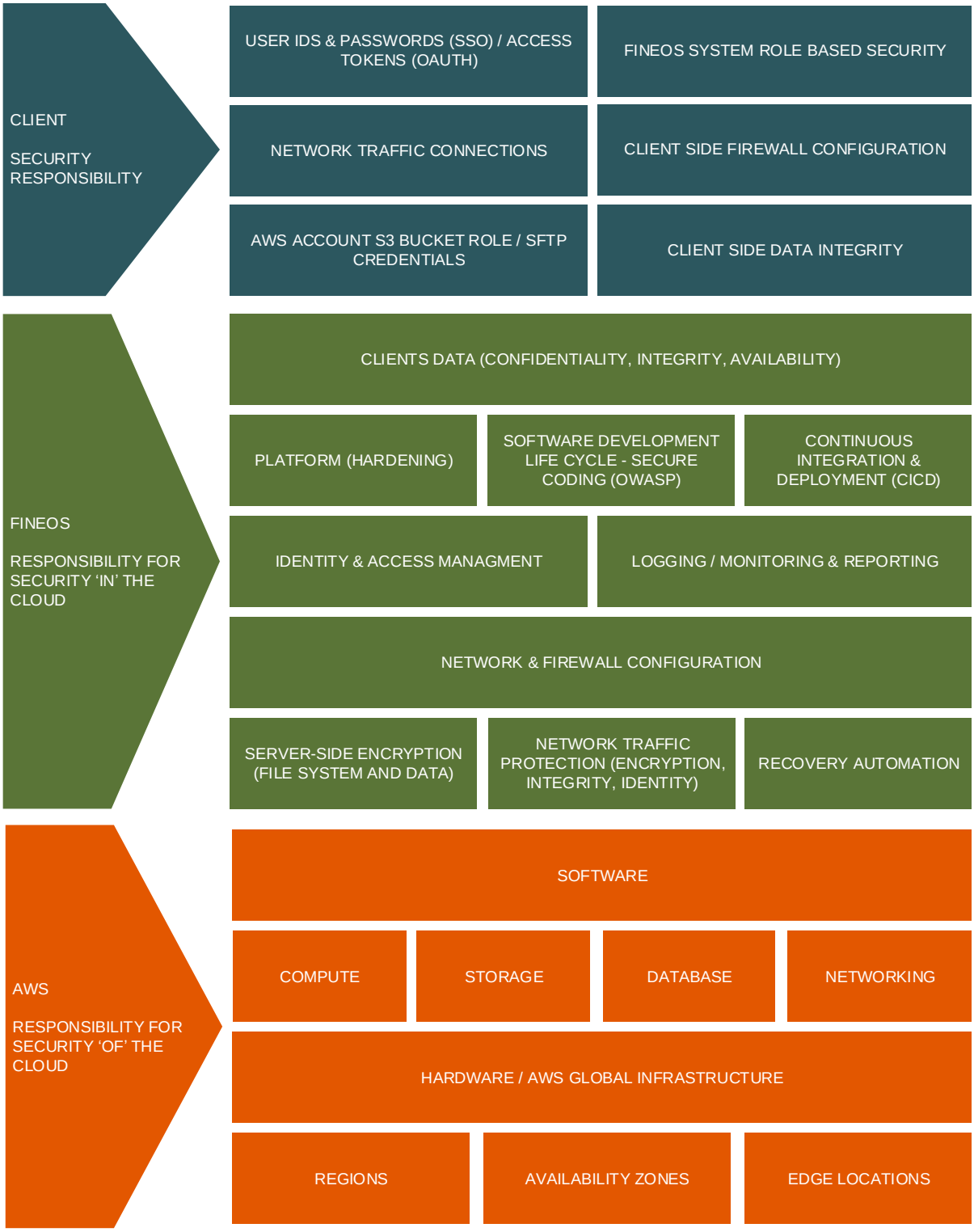

Figure 2 – Shared Responsibility Model

User IDs & Passwords (SSO)	*Client Identity Provider (IDP) user authentication which will be used to authenticate with the FINEOS system via Single Sign On (SSO). Clients must ensure a strong password policy and user lifecycle management.*
Access Tokens (OAUTH)	*FINEOS Platform – Application Programming Interface (API) Gateway supports oAuth 2.0 client credentials grant for Ingress (Client to FINEOS) Integrations. Client applications requesting data must ensure valid tokens are used to access a given set of resources.*
FINEOS System Role Based Security	*Clients' fine-grained user permissions are configured within the FINEOS system.*
AWS Account S3 Bucket Role	*Clients' AWS account role which has access to specific FINEOS S3 buckets. FINEOS S3 buckets require clients' AWS account id to build secure bucket policies. Clients are responsible for AWS role creation and credentials.*
SFTP Credentials	*Clients with Secure File Transfer Protocol (SFTP) access to specific FINEOS S3 buckets are responsible for connection credentials.*
Client-Side Data Integrity	*Client files loaded into AWS S3 for ingestion into FINEOS Platform must be of the specified format (ensuring accuracy and consistency).*
Client-Side Network Traffic Connections (VPN or Direct Connect)	*Clients' Virtual Private Network (VPN) endpoints need to be kept alive to ensure the VPN tunnel is always active.*
Client-Side Firewall Configuration	*Clients are responsible for the configuration of internal firewalls – these firewalls need to allow access to FINEOS Platform systems and ensure that any communication traffic from FINEOS Platform to client systems is unimpeded.*

Table 2 – Client Security Responsibility

Client Data	*FINEOS is responsible for the Confidentiality, Integrity and Availability of Client Data. This includes insuring only authorised FINEOS staff have access.* *All client data is managed to ensure consistency, accuracy and trustworthiness over the entire life cycle of the data. All data is encrypted at rest and in transit.* *Data is stored in multi availability zones to ensure high-availability solutions for all business-critical components.* *Automated database backups occur daily during a pre-defined backup window. Database backups have a pre-defined backup retention period.*
Platform	*FINEOS is responsible for management of:* • *The guest operating system (including updates and security patches)* • *Application software or utilities installed by FINEOS on the infrastructure* • *Configuration of the AWS-provided firewall*
Software Development Life Cycle	*FINEOS commits to developing software in a way that eliminates any potential vulnerabilities in our product software before deployment. Secure coding practices, including security education and training, are incorporated into our software development life cycle and our processes.* *Penetration (PEN) testing is undertaken to test, measure, and enhance established security measures on information systems and support areas*
Continuous Integration & Deployment	*As part of FINEOS Continuous Integration (CI), static source code analysis takes place to identify sub-optimal coding patterns across numerous fronts, including coding practice, maintainability, scalability, coding style, and vulnerabilities.* *For change involving FINEOS artefacts, FINEOS enforces the testing of each change of its application codebase(s) automatically. Once testing has passed, FINEOS deploys the changes to a staging environment.* *Changes are subsequently promoted to higher-level environments based on continued successful testing.* *The FINEOS change process is outlined in the "Production/BAU" section of this whitepaper.*
Identity and Access Management	*FINEOS Platform uses AWS Identity and Access Management (IdAM), and Multi-Factor Authentication (MFA). This aligns with the FINEOS policy to use Role-Based Access Control (RBAC) to grant or deny access to information and data services of the underlying system.* *FINEOS is responsible for managing the Identity and Access Management for all client AWS accounts.* • *Access being controlled using a combination of usernames, passwords and Multi-Factor Authentication (MFA)*

	• *Access control rules and rights to FINEOS Cloud accounts are granted based on business need* • *The Principle of Least Privilege (PoLP), which enforces the minimal level of user rights, or lowest clearance level to allow the user to perform his/her role* • *Least privilege being applied to processes, applications, systems, and devices, in that each should have only those permissions required to perform an authorised activity* • *Segregation of duty existing between the request, approval and delivery of access* • *User access requests being subject to formal authorisation, periodic review and removal* • *Enhanced access controls and monitoring for Highly Privileged Access (HPA) accounts* • *Four-eyes (two-person) rule being required for change implementation or break-glass, which is described in the Break Glass section of this whitepaper*
Logging / Monitoring & Reporting	*FINEOS leverage both AWS and 3rd party monitoring tools.* *All FINEOS Platform AWS accounts utilise Amazon Cloud Trail[27], CloudWatch[28] and GuardDuty[29] to monitor and report on all aspects of system access. This is managed by the FINEOS Cloud Operations Team.* *AWS automated logging and monitoring systems provide a high level of service performance and availability.* *FINEOS applications within AWS are designed to extensively monitor key operational metrics. Alarms are configured to notify operations and support personnel when early warning thresholds are crossed on key operational metrics.* *3rd party tools are used to provide an addition layer of monitoring across the FINEOS Platform infrastructure.* *FINEOS provide reports to the client on service risks, incidents or weaknesses within a contractually defined timeframe. This allows the regulated FSI to fulfil its obligations to notify APRA once aware of any security incidents or weaknesses.*
Network & Firewall Configuration	*FINEOS is responsible for the configuration of the networking and firewalls within the FINEOS Platform* *These responsibilities include AWS Web Application Firewall (WAF), Security Groups and Network Access Control Lists (NACLs) – these configurations need to allow access to the FINEOS Platform systems from trusted client sources and ensure that any communication traffic between FINEOS Platform applications are secure and encrypted using TLS (formerly Secure Socket Layer, or SSL).* *Where the use of a VPN is required, FINEOS is responsible for setting up and*

[27] AWS - CloudTrail
[28] AWS - CloudWatch
[29] AWS - GuardDuty

	configuring the AWS side of the service. This involves creating the Client VPN endpoint, associating the target network, and configuring the authorisation rules and routes.
Server-Side Encryption	*FINEOS Platform uses AES-256 encryption for all data stored at rest. AWS Key Management Service (KMS) is used to manage the keys for all available services. KMS uses envelope encryption which provides symmetric encryption of data.* *Infrastructure as Code (IaC)* provisions *keys and key policies within FINEOS Platform, ensuring that all configured services enforce encryption as standard.*
Network Traffic Protection	*All data in transit is encrypted using TLS which is an industry-standard AES-256 cipher, including connections between FINEOS applications and databases.*
Recovery Automation	The FINEOS Platform architecture is designed to minimise business disruption and ensure secure recovery through: • *A self-healing design (where the available AWS services exist)* • *Leveraging high-availability solutions for all business-critical components of the cloud architecture* • *Having a pre-defined automated backup schedule in place for client production data* • *Automated database backups occurring daily during a pre-defined backup window* •

Table 3 – FINEOS Security Responsibility

FINEOS

Appendix 2 – Links

[1] https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf

[2] https://www.legislation.gov.au/Details/F2012L02223/Download

[3] https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf

[4] https://www.apra.gov.au/sites/default/files/information-paper-outsourcing-involving-shared-computing-services.pdf

[5] https://www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services.pdf

[6] https://www.apra.gov.au/sites/default/files/Prudential-Practice-Guide-CPG-234-Management-of-Security-Risk-May-2013_1.pdf

[7] https://aws.amazon.com/professional-services/CAF/

[8] http://aka.ms/safehandbook

[9]https://d1.awsstatic.com/whitepapers/compliance/AWS_User_Guide_to_Financial_Services_Regulations_and_Guidelines_in_Australia.pdf

[10] https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf

[11] https://aws.amazon.com/blogs/apn/introducing-the-aws-financial-services-competency/

[12] https://aws.amazon.com/iam/details/mfa/

[13] https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege

[14] https://aws.amazon.com/iam/

[15] https://aws.amazon.com/s3/

[16] https://aws.amazon.com/cloudtrail/

[17] https://aws.amazon.com/cloudwatch/

[18] https://aws.amazon.com/guardduty/

[19] https://aws.amazon.com/kms/

[20] https://aws.amazon.com/config/

[21] https://aws.amazon.com/vpc/

[22] https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

[23] https://aws.amazon.com/cloudformation/

[24] https://aws.amazon.com/codecommit/

[25] https://d1.awsstatic.com/whitepapers/aws-disaster-recovery.121b65092f931567af5370b47dd12cb18866089c.pdf

[26] https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf