White Paper

RECONCILIATION ACTION PLAN
REFLECT

FINEOS

FINEOS Response to APRA: Prudential Standard CPS-230 Operational Risk Management

Introduction

The Australian Prudential Regulation Authority (APRA) CPS - 230 Operational Risk Management, outlines a minimum set of expectations to ensure that APRA regulated entities are resilient to operational risks and disruptions. CPS230 sets out requirements to effectively manage operational risks, maintain critical operations through disruptions, and manage risks arising from service providers.

Core systems are examples of 'critical systems' which need to be assessed for risk. In this document, FINEOS provides an assessment of how clients can understand and mitigate against these risks through using the FINEOS Platform powered by Amazon Web Services (AWS)

Four key areas:

Operational Risk Management

Business Continuity

Management of Service Provider Arrangements

Monitoring, Notifications and Review

Intended Audience

The intended audience of this document are Chief Information Officers (CIO), Chief Technology Officers (CTO), Chief Risk Officer (CRO), Chief Security Officers (CSO), Chief Information Security Officer (CISO), workload owners, service owners, governance, risk, and compliance (GRC) specialists and other stakeholders who engage in cloud adoption. Readers are not required to know all the details of the APRA information papers; however, some knowledge would be advantageous.

FINEOS understands that APRA's standards and guidelines can appear complex. For Financial Service Institutes (FSIs) who have not previously engaged with APRA on cloud adoption, it is recommended to seek guidance from specialists who can advise and assist with any necessary APRA engagement. In addition to FINEOS, clients may engage AWS and consulting partners within AWS Certified Partner Network (https://partners.amazonaws.com/)

FINEOS Platform Definition

The FINEOS Platform is a Software-as-a-Service (SaaS) offering from FINEOS that provides a flexible, secure, and cost-effective way of managing Life, Accident and Health Insurers' operations. The service, which includes New Business and Underwriting, Policy Administration, Billing and Claims is powered by AWS and is managed by FINEOS.

Operational Risk Management

As described throughout this document, FINEOS policies and procedures are benchmarked against industry standards including International Organisation for Standardisation (ISO), System and Organisation Controls (SOC) and National Institute of Standards (NIST) Cybersecurity Framework (CSF). These in addition to the FINEOS Business Continuity Plan (BCP) enable FINEOS to identify, assess and manage its operational risk.

Business Continuity Management

The FINEOS Platform has defined standard Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Recovery is tested on an annual basis to ensure FINEOS can meet these obligations.

Results of the High Availably/Disaster Recovery (HA/DR) testing/attestation are provided to clients; these results document the test/actions and status of those tests ensuring that severe but plausible/valid scenarios are covered.

FINEOS will actively test, review, and update the Business Continuity (BC)/DR Plan on at least an annual basis using industry best practices. FINEOS will provide the client with copies of any relevant and material updates to the BC/DR Plan.

Where requested, FINEOS may provide consultancy for DR and BC best practice.

To ensure data quality, FINEOS has automatic periodic data backups in conjunction with transaction logs to enable the ability to restore a database instance to any time during the backup retention period.

The FINEOS Platform Incident and Problem Management procedures are designed to resolve disruptive or potentially disruptive events with maximum speed and minimum disruption.

Production instances of the FINEOS Platform have databases deployed over multiple AWS Availability Zones within the clients' geographic AWS Region, this ensures clients data maintains integrity and is highly available.

FINEOS regularly tests for security weaknesses in its Platform to establish the current security posture. Penetration testing tools and techniques are run against the Platform to identify any potential weaknesses in the security configuration. Penetration testing is performed at least annually by independent third-party consultants, tests are performed against each generally available major release of the FINEOS Suite. Results can be shared with clients on request.

The FINEOS Platform Incident and Problem Management procedures are designed to resolve disruptive or potentially disruptive events with maximum speed and minimum disruption. The procedures align to the NIST and CSF, these are organised into five core Functions also known as the Framework Core (Identify, Protect, Detect, Respond and Recover).

Business Continuity Management (continued)

The functions are organised concurrently with one another to represent a security lifecycle. Each function is essential to a well-operating security posture and successful management of cybersecurity risk.

As part of this, FINEOS Operational Management also identifies root causes of past incidents and seeks to identify and prevent future occurrences (pre-event and post-event awareness).
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.

Management of Service Provider Arrangements

FINEOS is a well-respected company listed on the Australian Stock Exchange (ASX: FCL) that has been in business for over thirty years. Whilst FINEOS is financially sound, it expects that each new client contemplating subscribing to the FINEOS Platform will complete its own due diligence, including the review of publicly available financial records as disclosed to the ASX.

For FSIs that have no existing relationship with FINEOS, initial engagement between the FSI and FINEOS is typically via a competitive tender process. As part of these processes, FINEOS provide detailed answers allowing FSIs to understand any potential risks of moving workloads to the FINEOS Platform.

Existing FINEOS FSI clients will typically not require a competitive tender process, for example when moving from an on-premises deployment to a cloud hosted FINEOS Platform. FINEOS can provide detailed answers for FSIs to understand potential risks of moving workloads from an on-premises environment to a cloud hosted FINEOS Platform.

Management of Service Provider Arrangements (continued)

Platform clients that are APRA-regulated will have formal agreements which contain an "APRA access clause" to meet requirements (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.

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.

FINEOS is undergoing ISO 27001:2002 certification, stage 1 completion is targeted for late 2024 and stage 2 is targeted for completion mid-2025. All protocols, policies, standards, guidelines, and strict practices are aligned to the ISO 27000 family of standards. They are 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.

As a service provider, FINEOS maintains its own BCP with clear objectives, roles, and responsibilities. The "Business Continuity Team" is responsible for annually reviewing the complete plan and procedures. The plan includes key suppliers and relevant contact details for key vendor services (fourth party to a regulated entity). FINEOS holds a (SOC 2 – Type 2) attestation. Three trust services - 'Security', 'Availability' and 'Confidentiality' – are validated. The attestation period is between October and September with a publish month of December annually.

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

Clients using the FINEOS Platform powered by AWS inherit the most comprehensive compliance controls. AWS supports 143 security standards and compliance certifications, including PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171, helping its customers satisfy compliance requirements around the globe.

Monitoring, Notifications and Review

Regulated entities must ensure that the FINEOS Platform performs to the contractually agreed service levels. FINEOS maintains ongoing communications to clients via the FINEOS Service Manager(s).

As part of the FINEOS solution, automated infrastructure and application monitoring is used to ensure that the service is operating effectively. Any exceptions are automatically raised to the appropriate FINEOS team for resolution.

In the event of an issue, a remediation plan is immediately developed by FINEOS and communicated to the client via the Service Manager in an agreed timeframe.

As part of its standard client governance, FINEOS conducts Cloud Support Services meetings including monthly walkthroughs of all reported incidents and SLAs, quarterly Support Service reviews in the form of an operational account level meeting, and an annual account review to discuss the Support Service scope, suitability, and performance.

Regulated FSIs must notify APRA as soon as possible, and not later than twenty-four hours after if it has suffered a disruption to a critical operation outside the tolerance (RTO/RPO). During disruptions to the FINEOS Platform service – FINEOS maintains ongoing communications with clients via the FINEOS Service Manager(s) providing ongoing status updates. After any major incident, FINEOS work with clients to provide information on the investigation, root cause analysis and solution to any disruptions of the FINEOS Platform.

Conclusion

FINEOS has and will continue to successfully support our clients' move to the FINEOS Platform. FINEOS is committed to support Australian based clients' technology and service provider choices allowing them to comply with and exceed APRA's requirements.

Written and published by FINEOS Corporation Ltd.