

Position Description

Senior Product Owner – Financial Crime Systems



The Cooperative Bank

Our purpose

Our long-term aspirations are to develop more long-term value-based relationships with our customers, and for our people to grow and develop so that they are better off working at the Cooperative.

Our values

Our values represent who we are, how we think, and how we behave to bring these to life every day. You'll demonstrate behaviours that define our core values and support an inclusive culture with a strong teamwork spirit.



About the team

Financial Crime is a growing area of strategic risk management in the financial services industry. The team has responsibility for all areas of external fraud, including Anti-Money Laundering, Countering the Financing of Terrorism and External Fraud management, as well as some involvement in Sanctions, Anti-Bribery and Corruption and Internal Fraud.

The Financial Crime team sits within the wider Risk team and includes the Anti Money Laundering Compliance Officer (AMLCO), well as a small team of financial crime professionals who cover both first- and second-line risk functions.

The team is also responsible for providing a robust framework and control environment, to mitigate and manage the Bank's exposure to Financial Crimes related risks, with an increased response focus on Scams and industry participation to reduce customer losses.

The team therefore has responsibility to:

- Own the AML/CFT Risk Assessment, Policy, Programme and related sub-documents.
- Own the AML/CFT Assurance Program and complete some first- and second-line testing and reporting.
- Perform operational controls related to AML/CFT account monitoring (ECDD, OCDD, SARs, Transaction Monitoring, PTR, and screening)

- Perform operational controls related to external fraud cases from intelligence, monitoring and from customers.
- Act as SMEs for all the above.

Purpose of this position

The Senior Product Owner, Financial Crime Systems leads the strategy/roadmap and delivery of Financial Crime focused solutions enabled by technology that combat fraud, money laundering (AML/CTF), and other illicit activities.

The challenge is in bridging business needs (compliance, risk reduction) with technology teams (engineers, data scientists) to maintain and deliver systems, detection models, rule sets, and monitoring systems, all while managing product roadmaps, OKR's, and regulatory demands.

Challenges and opportunities of this role

From a relatively simple set of in-house tools and approaches we've got a multi-year program of work designed to implement new transaction monitoring and reporting tools that will fundamentally change how we do our work and lay the foundation for a roadmap for years to come.

While the decisions on which systems those are have been made, we're deep in the planning and delivery planning process and have identified we need someone in the Financial Crime team to help own with the delivery, provide ongoing leadership and running and drive future plans.

As a result, the role has elements of both change and business as usual. As we implement most of the effort will be in delivery, deeply embedded with the project, vendor and technology teams. Focus will then start to shift to how we manage, use and tune the new functions and plan for the future. Challenges and opportunities will therefore be to:

Change and improve the Product/System suite:

- Develop and deliver (via an internal Programme and Project structure) a strategy/roadmap for the future.
- Owning systems from concept to deployment (and beyond!), focusing on data-driven insights, efficient control, and robust user experiences to protect the bank and customers.
- Be a subject matter expert for technical changes and implementation for systems and projects with a Financial Crime impact.

Keep the Product/System suite working effectively:

- Ensure the day-to-day, effective and efficient functioning of the suite of systems:
 - Managing business user/unit level configurations and settings of the suite of Financial Crime systems.
 - Creating, monitoring and maintaining rules, models and reporting associated with the suite of Financial Crime systems.
 - Leading the relationship management with vendors for the suite of external Financial Crime systems used by the Co-operative bank.

Position reports to: Head of Financial Crime (AMLCO) within the Risk Division.
 Direct Reports: None.

How you will contribute:

What you'll do:	Success will mean:
Own Systems and Lead Vendor Relationships	
<p>Lead the delivery of the financial crime systems and provide ongoing leadership of these tools.</p> <p>'Own' a suite of Financial Crime systems and take the lead in keeping them working and developing/changing by influencing other business and technology teams.</p> <p>Manage relationships with vendors to ensure the continuous functioning and improvement of the suite of systems.</p>	<ul style="list-style-type: none"> Successful implementation of financial crime systems that are kept up to date and are fit for purpose. A clear single point of ownership with the technology aspects of our Financial Crime systems. Strong vendor relationships that ensure the bank's interests are well-represented.
Develop and Deliver Financial Crime strategy/roadmaps	
<p>Lead the development of a strategy and the roadmap for Financial Crime systems.</p> <p>Build business cases and change requests for delivery.</p> <p>Work closely with programs, projects and technology change teams to deliver the roadmap.</p>	<ul style="list-style-type: none"> A clear strategy and direction in place for our Financial Crime systems. Customers are better protected with data more readily available to impact business decisions Reduced/managed risk (liability and reputation). Solidly compliant and stable approaches to AML/CFT. Less spreadsheets and user-built tools!
Subject Matter Expert for Financial Crime related change	
<p>Be the subject matter expert for financial crime-related change both within the Risk team and across the bank.</p> <p>Work with other stakeholders and project teams to identify impact, define requirements and make decisions.</p>	<ul style="list-style-type: none"> Change is owned and well-managed by the rest of the business who consider the impact to Financial Crime requirements and obligations, minimising risk to the Bank. Sound, data-driven advice is provided to stakeholders to impact decision-making.
Ensure effective and efficient day to day configuration:	
<p>Make user/business unit level changes to Financial Crime systems.</p>	<ul style="list-style-type: none"> Steady incremental improvements to operational processes. Stable, well managed systems.

What you'll do:	Success will mean:
<p>Make, change and monitor the outputs (rules, models, alerts) of the systems for efficiency and effectiveness.</p> <p>Champion improvements to financial crime systems and communicate these to the immediate team and wider business as required</p>	<ul style="list-style-type: none"> Reduced/managed risk (liability and reputation) and demonstrably compliant systems. Financial crime systems are an integral tool within the team which contribute to overall operational efficiencies.
Healthy and safe work environments	
<p>Follow all health and safety policies, standards, emergency procedures and plans.</p> <p>Participate in health and safety activities, training and meetings as required.</p> <p>Reports hazards, near misses, injuries, incidents, and ideas for continuous improvement.</p> <p>Cease work if an unsafe situation arises and seek assistance.</p>	<ul style="list-style-type: none"> Having healthy and safe ways of working. All workers feel empowered to and aware of opportunities to participate in health and safety activities. Our people can easily report hazards, near misses, injuries, incidents, and ideas for continuous improvement. Workers stop work if they feel unsafe and connect with their people leader or other workers for assistance.

Decision making and responsibilities

a) Decisions and/or financial accountabilities:

- Day to day discretion for rule changes and configurations (within an established process; which you'll develop and own / maintain).
- No financial accountability.

b) Actions and decisions that are recommended to a higher level of management for approval:

- Business Case approvals.

Qualifications and experience

- Role requires at least 7+ years' experience in either systems/product/platform ownership or relevant experience in relation to one or more aspects of Financial Crime.
- A relevant tertiary qualification in finance, business, technology or similar is desired
- Experience in the banking or financial industry environment is desired.
- A strong working knowledge of the financial crime legislation and/or anti-fraud experience

Skills and attributes

Technical Skills

Financial Crime Systems Experience

- Hands-on exposure configuring or operating platforms, any in-house transaction monitoring or fraud engine. The specific vendor (or financial crime systems) is less important than pattern recognition across platforms. Experience with rules engines, scenarios, thresholds and/or workflows.
- Basic to intermediate SQL for querying and validation, or familiarity with programming. Comfort with “if / then” logic, parameters and conditions.
- Data Comfort (Not Data Science).
- Ability to analyse alert volumes and trends.
- Confidence working with datasets to sense-check outcomes.

Personality Attributes

- Detail-focused, proactive, and future-oriented.
- Collaborative, approachable, and able to influence and engage at all levels.
- Committed to continuous improvement and capability uplift.
- Resilient and adaptable in a dynamic regulatory environment.
- Ability to translate between Compliance, Operations, Customer Experience and Technology.
- Strong governance and documentation discipline.
- Comfort making tuning decisions backed by logic and evidence.
- Bias toward continuous improvement, not “set and forget”.

Leadership Skills

You will be expected to demonstrate behaviours from our Leadership skills framework through your actions, the way you work and how you work with others.