NIST AI RMF Implementation Engagement

Enabling your team to implement secure AI.

Cyber Dynamo

Contents

Introduction

Our NIST AI Risk Management Framework (RMF) consulting services are designed to set your organisation up for success implementing and utilising the NIST AI RMF. Our consultants will train your staff in the NIST AI RMF, tailor an implementation to your specific business, and deploy the NIST AI RMF into your organisation.

Your staff will work alongside our consultants to gain hands-on experience designing and implementing an AI risk management (AIRM) framework. We will guide the first few projects through the process until your staff are ready to take over and manage all AI projects going forward.

Each stage of the engagement results in a deliverable that is used to guide following stages in this process. Each process will have a stage gate at which time you can decide to continue with us or take the rest of the journey on your own. We want to teach you how to fish which requires knowledge transfer and confidence in your team's abilities.

Scoping

For us to deliver the best possible outcomes for your organisation, we will conduct a scoping exercise to determine a baseline for your current processes and experience in AI Risk management. This scoping exercise is a one day free exercise to determine the estimated depth and cost of the engagement phases outlined below.

Engagement Phases

Phase 1: Current state gap analysis

This phase kicks off with our two day training course for the NIST AI RMF. The outline for the workshop is in Appendix A of this document. With a foundational knowledge of the NIST AI RMF, we will guide your team in performing a gap analysis of your current AIRM capabilities. This process will help them understand how the NIST AI RMF applies to your organization.

Deliverables:

- NIST AI RMF training materials and workshop knowledge
- AI RMF gap analysis
- Gap remediation plan

Phase 2: AI RMF Implementation

Once the gap analysis remediation plan is complete, we will guide your staff through writing and establishing AIRM policies for your organization. This includes stakeholder engagement, establishing ownership of the policy and AIRM processes. This phase is critical to establishing executive level sponsorship for your AIRM program.

With executive sponsorship and policies in place, we will move on to guiding your team in designing an AIRMF. This process follows through the AI Risks and Trustworthiness characteristics as they apply to your environment, and the 4 Core functions, Govern, Map, Measure and Manage. It also includes artefacts and templates for integration into your development processes, monitoring and reporting on deployment level risks, testing for AI risk eventuation, and feedback processes for improving the AIRM process.

Once your team has been through the process with us, we will perform a handover exercise that validates their understanding of the process, how to use the programs developed during the engagement, and take over the management of your AIRMF. This process includes a post-mortem feedback process to allow us to reflect on any lessons learnt and areas for improvement.

Deliverables:

- AIRM Stakeholder map
- Executive sponsorship
- AI Ethics statement(s)
- AIRM Risks and Trustworthiness Map
- NIST AI RMF Core mapping and function processes
- Contextualized templates for AIRM
- A Set of applicable AI RMF use-case, temporal, and cross-sectional profiles
- Documented artefacts for the Govern, Map, Measure and Manage functions
- Project completion report
- Project evaluation
- Project closure documentation

Process

Our NIST AI RMF engagement begins with an information and scoping meeting. We want to understand your business and environment so that we can ensure that you are getting value for your time and money. Once the scoping is complete, we will present you with a statement of work, estimated cost breakdown, estimated timelines, and suggested start dates.

Upon commencement of the engagement, regular health check meetings will occur to ensure we stay on course and to identify any issues as soon as possible. Once phase one is delivered and the deliverables are handed over, we will conduct feedback sessions and second phase planning.

The second phase operates the same as the first. The deliverables for phase two are more substantial and a review and acceptance period will be expected. Once all deliverables are accepted, a project closure meeting will be conducted, and the project signed off.

Cost and Booking

The cost of this engagement is broken down into two sections as it relates to the phases of the engagement.

Phase 1: Current State Gap Analysis

The estimated time for Phase 1 is 5 working days including two days for the NIST AI RMF workshop for up to 10 attendees. The cost of this phase is a fixed $20,000AUD plus any applicable travel expenses.

Phase 2: AI RMF Implementation

This phase is based on a scoping exercise which relies on the output from Phase 1 to determine the size and complexity of the process to deliver phase 2. Estimates will be made based on Cyber Dynamo Principal Consultant daily rates of $2000AUD per day plus any applicable travel expenses.

An estimated costing of a Phase 2 delivery based on the output of Phase 1 will be provided prior to any work being performed on Phase 2.

Travel and expenses are not included in the above pricing and will be determined after initial scoping call. The client is responsible for all travel expenses incurred.

For booking information see the Cyber Dynamo NIST AI RMF Engagement Booking Form at the end of this document.

NOTE: *All costings are estimates and could change based on changes in scope, environment, delays, deviations from the statement of work, or unforeseen circumstances. While we do our best to estimate as accurately as possible, we cannot foresee everything.*

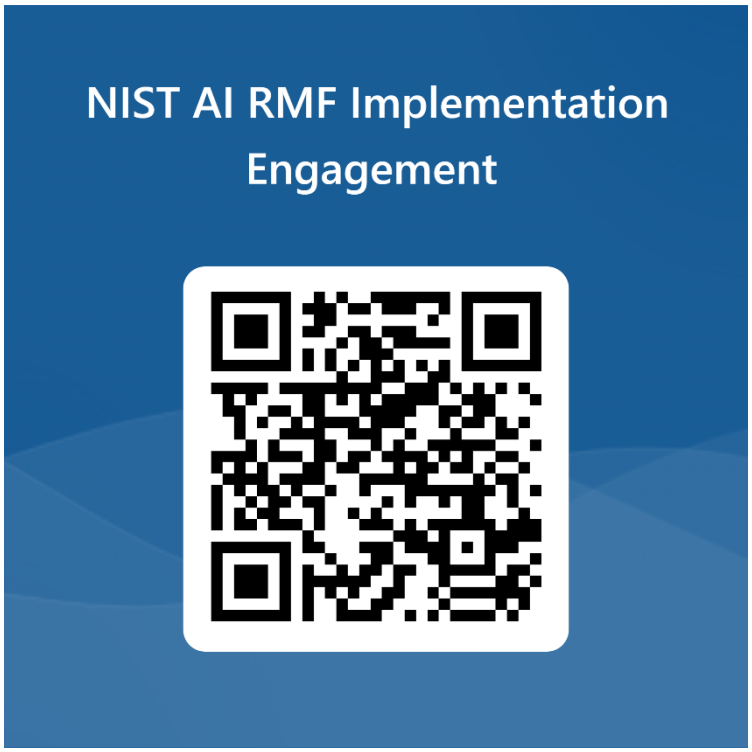
Appendix A

Day 1	Day 2
Audience: Exec Sponsors, CISO, Risk Managers	**Audience**: Risk Managers
AI RMF Introduction 1. Overview a. Introduction to AI RMF b. Audience c. Associated standards and references d. AI Lifecycle and Dimensions 2. AI Risk and how it extends cybersecurity risk a. Measuring AI Risk b. Setting Risk Tolerance c. Prioritising contextual risks d. Integrating AI Risk into corporate risk strategy 3. AI Risks and Trustworthiness a. Validity and Reliability b. Safety c. Security and Resilience d. Accountability and Transparency e. Explainability and Interpretability f. Privacy Protection g. Fairness 4. Monitoring and Evaluation for Effectiveness a. Lessons learned b. Improvement cycles c. Feedback internally d. Feedback to NIST **AI RMF Core** 1. Overview 2. Govern a. Overview b. Policies, processes, procedures and practices c. Accountability structures d. Workforce diversity e. Organisational commitment on AI risk communication f. Communication channels for AI actors g. Third party risks and benefits	**AI RMF Core Part 2** 1. AI RMF Profiles a. Overview b. AI RMF Use Case Profiles c. AI RMF Temporal Profiles d. AI RMF cross-sectoral profiles 2. Map a. Overview b. Establishing and communicating context c. Categorizing AI systems d. Cost and ROI and goals e. Risk and benefit mapping f. Impact assessment 3. Measure a. Overview b. Establishing appropriate metrics c. Evaluating trustworthiness d. AI Risk tracking e. Feedback loops 4. Manage a. Overview b. Prioritise and manage identified risks c. Implement strategies to maximise benefits, and minimize risks d. Manage third party benefits and risks e. Document and monitor risk response and communication plans

Cyber Dynamo NIST AI RMF Engagement Booking Form

When we receive your booking request, we will contact you to arrange scheduling. A non-refundable 20% deposit is due upon scheduling confirmation to cover the cost of materials.

Fill out the booking request form online at: https://forms.office.com/r/kuixb7mLsR
or scan this QR Code



NIST AI RMF

Anyone building or using AI needs to be concerned with AI Security. If you need help designing your AI Risk Management program, AI Security, or AI system design get in touch with us, we can help.
ConsultRequest@cyberdynamo.com

Cyber Dynamo