MONASH University

FIT5057 Project Management
Assignment Two – Team Assignment

Cybersecurity and Data Governance Improvement

Sean Murphy
2230455, Group 0609

Monash University
Project Management FIT5057
Monday 10:00 AM, Farheen Siddiqui

May 2025

Contents

This page intentionally left blank.

Project Overview

This document outlines the Quality Management Plan and the Stakeholder and Communication Management Plan for Monash University's Cybersecurity and Data Governance Improvement project. This strategic initiative is scheduled for completion by June 2026, with a total allocated budget of $1,035,000.

The project directly addresses three critical needs identified within the university's digital infrastructure:

- **Enhanced Cybersecurity Awareness:** Through the implementation of a mandatory Cybersecurity Awareness Framework for Academia (CAFA), the project aims to strengthen the university's human firewall against sophisticated and evolving cyber threats.
- **Improved Data Management:** The deployment of a Master Data Management (MDM) solution will enhance data quality, reduce operational redundancy, and ensure consistent, reliable information across diverse university systems.
- **Strengthened Security Compliance:** Completion of an Australian Cyber Security Centre (ACSC) Essential Eight audit and subsequent remediation activities will validate and improve the university's technical security posture against recognized national standards.

This initiative was prompted by several key factors, including the increasing sophistication of cyber threats targeting educational institutions, the growing complexity of managing data across numerous university systems, evolving regulatory requirements for robust cybersecurity measures, and the clear need for standardized cybersecurity awareness among all staff and students.

The Cybersecurity and Data Governance Improvement project aligns with Monash University's overarching commitment to digital excellence, operational resilience, and comprehensive data security, while ensuring compliance with national cybersecurity standards. The successful planning and execution of quality management and stakeholder engagement, as detailed herein, are critical to achieving the project's goal of significantly enhancing the university's cyber resilience and data governance capabilities.

1 Project Quality Management

1.1 Quality Requirement #1 - CAFA Effectiveness and Usability

Quality Objective To ensure the Cybersecurity Awareness Framework for Academia (CAFA) program, including the CATM training modules integrated with the Monash LMS, effectively improves cybersecurity knowledge among staff and students, and is highly usable and accessible.

Quality Standards Two primary quality standards guide this objective:

- **ISO/IEC 27001:2022, Annex A Control 6.3 (Information security awareness, education and training)** (International Organization for Standardization, 2022). This framework ensures personnel understand information security threats and responsibilities, guiding the relevance and comprehensiveness of CATM content.
- **Web Content Accessibility Guidelines (WCAG) 2.2 Level AA** (W3C Web Accessibility Initiative (WAI), 2023). This standard will be applied to CATMs and their LMS interface.

Justification ISO 27001 alignment ensures CAFA content addresses pertinent university cybersecurity threats and compliance needs, tackling specific risks like phishing (Alharbi & Tassaddiq, 2021; Khader et al., 2021) and addressing the problem of inadequate awareness. WCAG 2.2 AA compliance is vital for Monash as an inclusive institution, ensuring training materials are perceivable, operable, understandable, and robust for users with disabilities. This promotes equitable access, maximizing reach and effectiveness. Poorly designed or inaccessible modules would significantly hinder user engagement and the 90% completion target. These standards ensure CAFA is both meaningful and universally deliverable.

Assumptions

- The Cybersecurity Awareness Center (CAC) possesses expertise to validate CATM content relevance against ISO 27001.
- The Monash LMS platform supports WCAG 2.2 AA compliant module delivery and accurate user tracking for metrics.
- A representative user sample will be available for pilot testing to validate usability and knowledge improvement metrics.

Metrics and Measurement Methods

- **Metric 1: Training Completion Rate:**
  - *Measure:* Percentage of assigned staff/students completing mandatory CATMs.
  - *Source:* LMS tracking.
  - *Target:* ≥90% by December 31, 2026.
- **Metric 2: User Satisfaction Score:**
  - *Measure:* Average score from post-module surveys (5-point Likert scale) assessing relevance, clarity, ease of use, accessibility.
  - *Source:* Embedded LMS surveys.
  - *Target:* ≥4.0/5.0 average across modules by end of initial rollout (Q1 2026).
- **Metric 3: Knowledge Assessment Score Improvement:**
  - *Measure:* Average percentage improvement between pre-module quiz and post-module assessment scores.
  - *Source:* Pilot phase testing.
  - *Target:* ≥30% improvement on key concepts (Q3 2025).
- **Metric 4: WCAG 2.2 AA Conformance:**
  - *Measure:* Percentage of WCAG 2.2 Level AA success criteria met.
  - *Source:* Automated tools (e.g., WAVE, Axe) and manual audits by Test Analyst.
  - *Target:* 100% conformance for all CATMs prior to deployment.

Monitoring and Review Process

- **Oversight:** Project Manager and contracted Test Analyst oversee CAFA quality. The CAC board will be consulted on content alignment with ISO 27001 during scheduled reviews.
- **Compliance & Usability Testing:** Test Analyst conducts WCAG checks and usability testing during module development (Q2-Q3 2025).
- **Ongoing Monitoring:**
  - User satisfaction and completion rates: Monitored monthly via LMS reports from program rollout (Q1 2026).
  - Knowledge assessment scores: Analyzed post-pilot phase (end Q3 2025).
- **Review Meetings:** Monthly quality reviews (PM, Test Analyst, Content Writer, CAC representative) to discuss metrics, feedback, and deviations.

- **Corrective Action:** Issues (e.g., low satisfaction, accessibility barriers, content misalignment) trigger review and revision of CATMs/interface using a PDCA cycle.

1.2 Quality Requirement #2 - MDM Data Quality, Reliability, and Efficiency

Quality Objective To ensure the MDM solution establishes high data quality (accuracy, completeness, consistency, timeliness) for critical domains, ensures high system availability, and achieves a 10% reduction in data management costs by end of 2026.

Quality Standards This objective will be guided by two key frameworks:

- **DAMA-DMBOK (Data Management Body of Knowledge) framework**, specifically its Data Quality and Data Architecture knowledge areas (DAMA International, 2017). This informs data quality rules, stewardship, and architectural design, promoting a view of data as an asset.
- **ISO 8000-110:2019 (Data quality – Part 110: Master data)** principles for master data exchange, characteristic data syntax, semantic encoding, and conformance (International Organization for Standardization, 2019). This guides structuring and validation of master data entities for clarity and interoperability.

Justification DAMA-DMBOK principles provide a structured approach to data governance, addressing fragmented data practices (Schmuck et al., 2024) and building a foundation for reliable data crucial for university operations and reporting. ISO 8000 principles ensure MDM-managed core data entities are well-defined and conformant. This is essential for automated validation, error reduction, and reliable data exchange, directly supporting operational efficiency and cost reduction. High system reliability is also paramount; MDM hub downtime would disrupt dependent university systems.

Assumptions

- Business units will commit to standardized master data definitions and quality rules necessary for achieving target metrics.
- The Informatica MDM platform's data quality tools are adequate for measuring and monitoring the defined data quality metrics.
- Baseline data for 2024 data management operational expenditures is accurate for measuring cost reduction.

Metrics and Measurement Methods

- **Metric 1: Data Quality Score (Composite Index):** Calculated quarterly from automated MDM hub profiling. The 20% improvement target applies to this overall index derived from sub-metrics.

  - *Sub-Metric 1a: Completeness:* Target ≥98% for defined critical data elements (e.g., student records: student ID, legal name; staff records: employee ID, primary department).
  - *Sub-Metric 1b: Consistency:* Target ≥95% match rate for key identifiers across integrated systems.
  - *Sub-Metric 1c: Timeliness:* Target <24 hours latency for critical data updates to the MDM hub.
  - *Overall Target:* 20% improvement in the composite index score from baseline (Q2 2025) by project end (Q2 2026).
- **Metric 2: System Availability:**
  - *Measure:* Percentage uptime of the core MDM platform (excluding planned maintenance).
  - *Source:* Monitored by Monash IT Operations post-handover.
  - *Target:* ≥99.5% availability (starting Q2 2026).
- **Metric 3: Data Management Cost Reduction:**
  - *Measure:* Comparison of 2026 actual data management operational expenditures (incl. MDM maintenance) against the 2024 baseline (~$5.84M), adjusted for inflation if needed.
  - *Source:* Annual financial reports.
  - *Target:* ≥10% reduction by December 31, 2026.

Monitoring and Review Process

- **Oversight:** Project Manager, supported by contracted Data Architect, GRC Consultant, and Senior Test Analyst.
- **Automated Monitoring:** Data quality profiling tools (Informatica) provide continuous monitoring, with reports reviewed quarterly.
- **Validation:** Senior Test Analyst validates system functionality and integration reliability during implementation (Q4 2025 - Q1 2026).
- **Operational Monitoring:** System availability monitored by Monash IT Operations post-handover. Cost reduction tracked annually by PM with Monash Finance.
- **Review Meetings:** Quarterly MDM quality reviews to assess metrics against targets.
- **Corrective Action:** Significant deviations (e.g., data quality score drops, low availability) trigger root cause analysis by technical team and data stewards, leading to corrective actions (e.g., refining data rules, adjusting integrations, system optimization).

2

Project Stakeholder and Communication Management

2.1 Stakeholder Register

Table 2.1: *Stakeholder Register*

No.	Name	Title	Role in Project	Contact
1	Sharon Pickering (She/Her)	Vice Chancellor, Monash University	Project Sponsor	sharon.pickering @monash.edu, +61399012345
2	Dan Maslin (He/Him)	Group Chief Information Security Officer (CISO), Monash University	Key Internal Stakeholder (Operational Security Lead, Policy Endorsement)	dan.maslin @monash.edu, +61412345678
3	Josh Teichman (He/Him)	Chief Transformation Officer and Acting Executive Director, eSolutions, Monash University	Key Internal Stakeholder (Oversees eSolutions, strategic alignment of tech initiatives)	josh.teichman @monash.edu, +61423456789
4	Sean Murphy (He/Him)	IT Project Manager, Monash University	Project Manager	smur0055 @student.monash.edu, +61434567890
5	Siddhant Tandon (He/Him)	Director, Information & Records Management, Monash University (eSolutions)	Key Internal Stakeholder (Data Governance, Information Policy Owner)	siddhant.tandon @monash.edu, +61401234567

Continued on next page

Table 2.1: *Stakeholder Register (Continued)*

No.	Name	Title	Role in Project	Contact
6	Amr Hassan (He/Him)	Director, Technology Services, Monash University (eSolutions)	Key Internal Stakeholder (Infrastructure & Systems Operations Owner)	amr.hassan @monash.edu, +61411223344
7	John Donaldson (He/Him)	General Counsel & University Solicitor, Monash University	Key Internal Stakeholder (Compliance & Legal Advisor)	ogc@monash.edu, +61399023456
8	Olivia Rodriguez (She/Her)	GRC Consultant, GRC Consulting Group	Contractor (MDM Governance Framework Development)	olivia.rodriguez @grcconsultinggroup.com, +61422334455
9	Alexander Taylor (He/Him)	Cybersecurity Analyst, Cybersecurity Analysts	Contractor (ACSC Audit & Remediation Support)	alexander.taylor @cybersecurityanalysts.com, +61433445566
10	William Chen (He/Him)	Cyber Architect, Tech Innovators	Contractor (Design MDM security architecture)	william.chen @techinnovators.com, +61404556677
11	Sophia Hernandez (She/Her)	Data Architect, Tech Innovators	Contractor (Structure MDM data models, pipeline integration oversight)	sophia.hernandez @techinnovators.com, +61415667788
12	Daniel Thomas (He/Him)	Cybersecurity Engineer, Cyber Engineer Tech	Contractor (Implement ACSC Essential Eight controls)	daniel.thomas @cyberengineertech.com, +61426778899
13	Sasha Braybrooke (She/Her)	President, Monash Student Association (MSA)	Key External Stakeholder (Representative of Student Body - CAFA End Users)	msa-president @monash.edu, +61437889900
14	Monash Staff (They/Them)	Staff, Monash University	End Users (CAFA), Data Users (affected by MDM changes and new data policies)	Via Internal Comms Channels (e.g., Staff News)
15	Emily Carter (She/Her)	Content Writer, Creative Content Works	Contractor (Develop CAFA Training Modules - CATMs)	emily.carter @creativecontentworks.com, +61408990011

2.2 Communication Matrix

Table 2.2: *Communication Matrix*

Communication Type	Objective of Communication	Medium	Frequency & Timing	Audience	Owner	Deliverable	Format
Project Kick-off Meeting	Align key stakeholders on project scope, objectives, timeline, roles, success criteria, and comms plan.	Hybrid (In-person + Video Conf)	Once - At project initiation phase.	Project Sponsor, PM, CISO, IT Ops Head, Data Gov Lead, Legal Counsel, Key Contractor Leads, MSA President (optional)	Project Manager	Kick-off Presentation, Meeting Minutes	PPTX, PDF
Monthly Project Status Report	Provide high-level summary of progress against milestones, budget status, key risks/issues, upcoming tasks.	Email + Link to Dashboard/Doc	Monthly - First week of each month throughout project lifecycle.	Project Sponsor, CISO, IT Ops Head, Data Gov Lead, Legal Counsel	Project Manager	Status Report, Online Dashboard	PDF, Web
Bi-Weekly Core Team Sync	Detailed operational sync-up on tasks, dependencies, technical challenges, immediate risks.	Video Conference (MS Teams)	Bi-Weekly - Every other Wednesday 9AM, throughout project execution phases.	Project Manager, Contractor Team Leads (CAFA, MDM, ACSC), relevant Monash IT SMEs as needed.	Project Manager	Action Items Log, Verbal Updates, Shared Screen Demos	Word/Wiki, PPTX

Continued on next page

Table 2.2: *Communication Matrix (Continued)*

Communication Type	Objective of Communication	Medium	Frequency & Timing	Audience	Owner	Deliverable	Format
Steering Committee Update	Strategic review, major decision making, budget/scope change approval, escalation resolution.	Formal Presentation (Hybrid)	Quarterly - Mid-point of each project quarter (or ad-hoc for urgent major decisions).	Project Sponsor, CISO, IT Ops Head, Data Gov Lead, Legal Counsel, Josh Teichman (CTO), Project Manager	Project Sponsor / PM (Co-lead)	Steering Committee Deck, Decision Log	PPTX, Word/PDF
CAFA Content Review & Alignment (CAC & Writer)	Ensure CAFA training module content is accurate, relevant, aligned with ISO 27001, and meets university needs.	Video Conference / Shared Docs	Weekly during CATM development phase; then bi-weekly during pilot and initial refinement.	Content Writer (Contractor), CAC Representatives (once established), Test Analyst (for usability/accessibility input).	CAC Lead / Content Writer (Co-lead)	Draft CATM Content, Feedback Log, Approved Content Versions	Word, Collaborative Docs
CAFA Rollout Communications	Inform staff/students about mandatory training, deadlines, access, support.	University-wide Email, LMS Banners, Intranet News, Digital Signage	Campaign-based: Initial announcement (1 month prior to rollout), reminders (weekly during first month of rollout), ongoing FAQs.	All Monash Staff, All Monash Students	Project Manager	Email Templates, Web Content, FAQs	HTML, PDF

Continued on next page

Table 2.2: *Communication Matrix (Continued)*

Communication Type	Objective of Communication	Medium	Frequency & Timing	Audience	Owner	Deliverable	Format
MDM Technical Design & Scoping Workshops	Define detailed technical requirements, scope data domains, map integrations, and refine MDM architecture.	Workshops (Video Conf / In-person)	Weekly - During MDM detailed design and scoping phase (pre-implementation).	Data Architect, Cyber Architect, Data Engineer, Software Developer, GRC Consultant, Senior Test Analyst, relevant Monash Business/IT SMEs, PM.	Data Architect	Detailed Design Specs, Data Models, Integration Maps	Visio/ Lucidchart, PDF, Wiki
MDM Implementation Progress & Issue Tracking	Monitor MDM development progress, track technical tasks, identify/resolve roadblocks, review configurations.	Video Conference (MS Teams) + Jira/DevOps	Daily stand-ups (30 min) during active sprints; Weekly (1 hour) deep-dive/review throughout MDM implementation phase.	MDM Technical Team (Data Architect, Cyber Architect, Data Eng, Software Dev, Sr Test Analyst), PM.	Data Architect	Sprint Backlog, Burn-down Charts, Issue Tracker Updates	Jira/Azure DevOps
MDM Technical Design Review	Formal review and approval of MDM architecture, data models, integration points, security design.	Workshop (Video Conference)	Once - Prior to MDM core implementation phase commencement (conclusion of scoping workshops).	PM, GRC Consultant, Cyber Architect, Data Architect, Data Engineer, Software Dev, Senior Test Analyst, CISO delegate, IT Ops Head delegate, Data Gov Lead delegate.	Data Arch. / Cyber Arch. (Co-lead)	MDM Design Document, Security Architecture Document	PDF

Continued on next page

Table 2.2: *Communication Matrix (Continued)*

Communication Type	Objective of Communication	Medium	Frequency & Timing	Audience	Owner	Deliverable	Format
ACSC Audit Findings Briefing	Present Essential Eight assessment results, identified gaps, and proposed remediation plan.	Formal Presentation (In-person/VC)	Once - Following completion of the ACSC baseline assessment phase.	Project Sponsor, CISO, IT Ops Head, Legal Counsel, Josh Teichman (CTO), Project Manager, Lead Cybersecurity Analyst	Lead Cybersecurity Analyst	Audit Findings Report, Remediation Plan Proposal	PDF, XLSX
Stakeholder Feedback Session (CAFA Pilot)	Gather usability and content feedback on CAFA modules from representative users.	Focus Groups / Surveys (Online)	Twice - Mid-point and end of the CAFA pilot testing phase.	Representative sample of Staff and Students (coordinated via Internal Comms / MSA).	Test Analyst / Content Writer (Co-lead)	Feedback Summary Report, Survey Results Analysis	PDF, Word
Change Request Notification & Review	Communicate proposed changes to scope/schedule/budget, assess impact, and facilitate decision.	Formal Email + CR Form + Meeting	As needed - CR submitted, then review meeting scheduled within 5 business days.	Project Sponsor, CISO, relevant budget holders, PM, relevant technical leads.	Project Manager	Change Request Form, Impact Assessment, Decision Record	Word/PDF

Continued on next page

Table 2.2: *Communication Matrix (Continued)*

Communication Type	Objective of Communication	Medium	Frequency & Timing	Audience	Owner	Deliverable	Format
Project Closure Meeting & Report	Summarize final outcomes, performance against objectives, budget, lessons learned, and formal handover.	Meeting (Hybrid) + Report	Once - At project completion and formal closure phase.	Project Sponsor, CISO, IT Ops Head, Data Gov Lead, Legal Counsel, Josh Teichman (CTO), PMO, Key Contractor Leads, Project Manager.	Project Manager	Final Project Report, Lessons Learned Register, Handover Docs	PDF, XLSX

2.3 Engagement Strategy

2.3.1 Dan Maslin (He/Him) – Group Chief Information Security Officer (CISO), Monash University

- **Power Level:** High
- **Interest Level:** High
- **Current Engagement:** Supportive (but discerning)
- **Engagement Strategy:** Dan is an experienced and pragmatic CISO with deep technical understanding, values data-driven arguments and concise information. Engagement will focus on providing him with executive-level monthly status reports on risk posture and ACSC progress. Direct access to technical leads will be offered for optional deep dives, respecting his busy schedule. We will actively seek his strategic input on ACSC remediation priorities, leveraging his expertise. For the MDM security architecture, his delegates will be involved in technical reviews, with summary endorsements provided to him. This approach aims to maintain his confidence by showing competence, proactive risk management, and alignment with his goal of practical, efficient risk reduction without operational friction. Regular, transparent updates on challenges will ensure he remains well-informed and engaged.
- **Conflict Management Approach:**
  - Address disagreements on priorities or technical approaches with evidence-based arguments, referencing ACSC guidelines and risk assessments, acknowledging his need for strong justification.
  - Facilitate direct discussions between Dan's team and project technical leads if specific technical solutions are questioned.
  - Document significant strategic disagreements on risk acceptance, including differing viewpoints, and escalate to the Project Sponsor via the Steering Committee with a clear recommendation, ensuring his expert opinion is represented.
  - Maintain transparency about project challenges and risks to build trust and avoid surprises.

2.3.2 Sasha Braybrooke (She/Her) – President, Monash Student Association (MSA)

- **Power Level:** Medium
- **Interest Level:** High
- **Current Engagement:** Neutral (Needs proactive engagement)
- **Engagement Strategy:** Sasha is a passionate advocate for student welfare, valuing transparency and genuine consultation. Engagement will begin with a briefing to explain the CAFA initiative's student impact, emphasizing a partnership. Communications will be jargon-free, focusing on *why* CAFA is important for *their* data security and online safety. We will utilize MSA channels for outreach, co-developing content. Her or an MSA delegate's participation in CAFA pilot feedback sessions will be cru-

cial for gathering insights on usability, relevance (especially concerning mandatory training and privacy), and accessibility. This feedback will visibly inform module improvements. The goal is to make Sasha an ally who can effectively communicate the program's benefits to students, addressing their concerns proactively.

- **Conflict Management Approach:**
  - Proactively address anticipated student concerns (e.g., mandatory training time, privacy) in initial communications and FAQs.
  - Listen actively if specific issues are raised via MSA (e.g., module length, relevance) and schedule meetings to explore feasible adjustments while explaining constraints.
  - Engage collaboratively to find solutions for broader student pushback, emphasizing the necessity of cyber awareness while remaining flexible on implementation details where possible.
  - Ensure that feedback mechanisms are clear and that students feel their concerns are acknowledged, even if not all requests can be accommodated.

References

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of majmaah university. *Big Data and Cognitive Computing*, *5*(2), 23. https://doi.org/10.3390/bdcc5020023

DAMA International. (2017). *Dama-dmbok: Data management body of knowledge* (2nd). Technics Publications.

International Organization for Standardization. (2019). *Data quality — part 110: Master data: Exchange of characteristic data: Syntax, semantic encoding, and conformance to data specifications*. International Organization for Standardization. https://www.iso.org/standard/66732.html

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — information security management systems — requirements*. International Organization for Standardization. https://www.iso.org/standard/27001

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information*, *12*(10), 417. https://doi.org/10.3390/info12100417

Schmuck, M., Georgescu, M. R., & Ioan, A. (2024). Master data management in higher education: Enhancing effectiveness study on universities from romania and germany. *Informatica Economica*, *28*(4), 5–21. https://doi.org/10.24818/issn14531305/28.4.2024.01

W3C Web Accessibility Initiative (WAI). (2023, October). Web content accessibility guidelines (wcag) 2.2. https://www.w3.org/TR/WCAG22/