Evidence of nonconformities identified and corrective actions arising

# Purpose

The purpose of the document “Evidence of nonconformities identified and corrective actions arising” is to keep a detailed record of nonconformities and the actions taken to address them ensures that the company maintains a transparent operational stance. In the context of Foodie, it is mainly about facilitating the iterative improvement of the ISMS. Using these insights, Foodie can refine its information security strategies, processes, and controls, aligning them more closely with the company's evolving risk and business objectives. As a standard for ISMS, ISO/IEC 27001 requires organizations to identify, manage, and rectify nonconformities. Regularly documenting these instances ensures that Foodie remains compliant with this standard, positioning the company for potential certification or recertification. This document will also record the process map of the deming cycle linking to the improvement of Foodie’s maturity level.

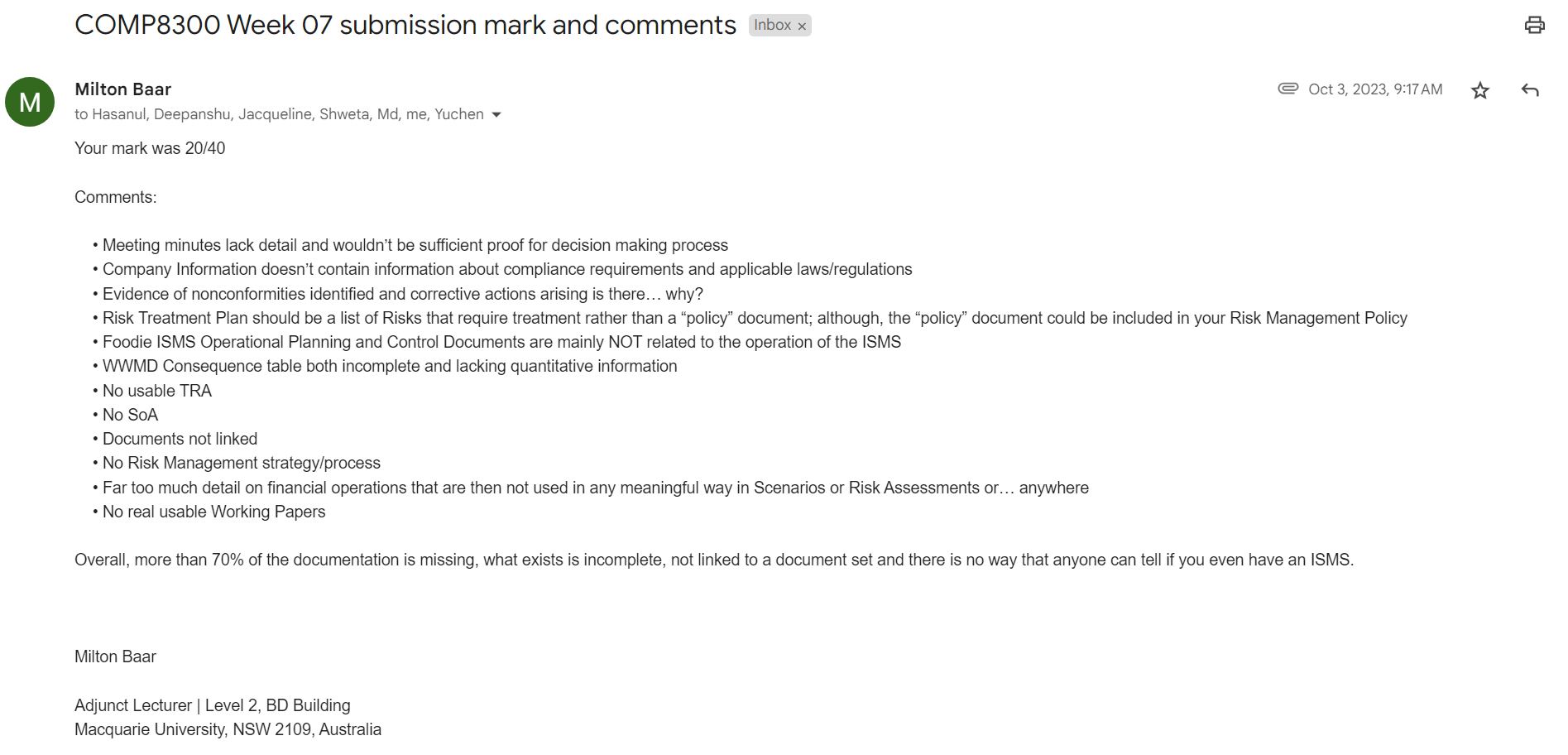
# Nonconformities Identified

Nonconformities are discrepancies, violations, or deviations from established procedures, policies, or requirements. They represent situations where certain aspects of the ISMS do not align with the set criteria, standards, or expectations. Identifying these nonconformities is vital for an organization to address security vulnerabilities and ensure the continued effectiveness of its ISMS.

The following are the nonconformities identified during the internal audits of Foodie:

* Documentation and Record Keeping Issues:
  + Meeting Documentation: Meeting minutes lack sufficient detail, making them inadequate records of decision-making processes.
  + Inadequate Company Information: Information doesn't cover compliance requirements and lacks mention of applicable laws and regulations.
  + Evidence Gaps: The reason for documenting "Evidence of nonconformities identified and corrective actions arising" is unclear.
  + Document Linking: Existing documents aren't interlinked, making it challenging to trace relevant information.
  + Missing Documentation: Over 70% of the required documentation is missing, rendering the present information incomplete and incoherent.
  + Unusable TRA: Threat Risk Analysis (TRA) is either missing, incomplete, or not properly documented.
  + No Statement of Applicability (SoA): A critical document in ISMS, outlining the controls in use, is missing.
* Strategy and Policy Nonconformities:
  + Risk Treatment Plan Format: The plan is presented as a "policy" rather than a list of actionable risks that require treatment.
  + Operational Planning: Documents related to the operation of the ISMS are irrelevant.
  + Missing Risk Management Strategy: There's no clear strategy or process for risk management, a core component of ISMS.
  + WWMD Consequence Table: The "What Would Management Do" table is both incomplete and lacks quantitative data.
  + Financial Operations Detail: Excessive and unnecessary detail on financial operations, which isn't subsequently used in scenarios or risk assessments.
  + No Usable Working Papers: Absence of structured documents that record all facts, figures, and activities related to the ISMS.
* Implementation and Operational Nonconformities:
  + Inefficacy of the ISMS: The existing system doesn't show any coherent structure or operational capabilities of an ISMS.

# Evidence of Nonconformities





# Deming cycle and Corrective Actions Arising

Once Foodie received its internal audits and identified the relevant non conformities, we started to Improve the identified nonconformities through corrective actions and utilizing the Deming Cycle (Plan-Do-Check-Act).

* Plan:
  + Documentation & Record Keeping:
    - Develop more sophisticated templates for meeting minutes to ensure they capture all necessary details.
    - Update the Company Information document to include compliance requirements and applicable laws and regulations.
    - Clearly define the purpose and format for documenting evidence of nonconformities and corrective actions.
    - Create an organized document (see “Readme document”) where all documents are linked and easily accessible.
    - Start building missing documentation, including TRA, SoA, and Risk Management strategy.
  + Strategy & Policy:
    - Revise the Risk Treatment Plan to be an actionable list of risks.
    - Review all existing ISMS operational documents and align them with ISMS objectives.
    - Develop a comprehensive risk management strategy that defines the risk assessment and risk treatment processes.
  + Implementation & Operational:
    - Assess the current state of the ISMS and identify gaps.
    - Develop an ISMS implementation roadmap that is aligned with the identified corrective actions.
* Do:
  + Implement the defined strategies and policies in the planning phase.
  + Set up periodic reviews of the implemented changes to ensure they are working as intended.
* Check:
  + Monitor and review the changes.
  + Conduct internal audits to verify the effectiveness of the corrective actions.
  + Analyze feedback from the internal auditor to ensure that the implemented changes are practical and effective.
* Act:
  + Based on the reviews, make any necessary adjustments to improve.
  + Document lessons learned and continue to refine the processes as necessary.

**Maturity Level:**

Given the previously identified nonconformities, it appears Foodie's ISMS is at an early stage of maturity ( Policy Level 1). To properly identify the maturity level of Foodie before and after the deming cycle of improvements, we would use five levels of progressive maturity in NIST CSEAT IT Security Maturity Model.

**Five levels of progressive maturity in NIST CSEAT IT Security Maturity Model.**

* Policy (Level 1): This is the foundational level where the organization establishes its cybersecurity policies. These policies define the organization's stance on security, its goals, and its commitments.It sets the tone for what is acceptable and what is not within the organization.Policies might cover areas such as access control, incident response, data protection, and more.
* Procedure (Level 2): With policies in place, the organization then defines the procedures or the "how-to" for implementing these policies. Procedures provide detailed steps and guidelines on how various tasks should be carried out to ensure alignment with the stated policies. This could involve processes like how to regularly update software, how to verify user identities, or how to respond when a security incident occurs.
* Implementation (Level 3): At this stage, the organization takes the defined procedures and puts them into action. This involves deploying tools, technologies, and practices to ensure that procedures are followed. Implementation ensures that the organization's cybersecurity stance is not just theoretical but is actively practiced. Regular training might be conducted to ensure all staff members are aware of their roles in this phase.
* Testing (Level 4): Once procedures are implemented, they need to be tested for effectiveness. This involves regular security assessments, penetration tests, and vulnerability assessments. Testing helps identify gaps or weaknesses in the current implementation and assesses whether the organization's security measures stand up to real-world threats. It's an iterative process, where findings from the tests lead to refinements in the procedures and implementation.
* Integration (Level 5): At the highest level of maturity, cybersecurity practices are fully integrated into the organization's day-to-day operations. Security becomes a part of the organization's culture, with every department and team member understanding their role in maintaining it. This level also sees the organization proactively evolving its cybersecurity stance, adapting to new threats, and integrating security considerations into all business decisions.

Addressing the listed nonconformities would involve:

* Establishing clear documentation.
* Aligning ISMS operations with actual requirements.
* Implementing a comprehensive risk management strategy.
* Making sure documents are interlinked and forming a coherent ISMS framework.
* Creating and testing the necessary procedures and controls.

After addressing these nonconformities using the Deming Cycle:

* Foodie would likely move beyond the initial "Policy" level, where only the foundational ISMS policies are in place.
* The company would then progress to the "Procedure" level, having established and documented structured procedures for its ISMS operations.
* If Foodie successfully implements the defined procedures and controls, the maturity progresses to the "Implementation" level.

However, to advance further to "Testing" and "Integration" levels, Foodie would need to demonstrate consistent effectiveness of the ISMS, not just its establishment. This would involve iterative cycles of the Deming process, ensuring that the ISMS is not only implemented but is also effective, integrated, and continually improving.

**In conclusion, Foodie's ISMS would likely be between the "Procedure" and "Implementation" levels of maturity. Continual application of the Deming Cycle would be crucial for further progression.**