

MIS761: T2 2024 – Assessment Task 2 – Group Assignment

	Unsatisfactory	Needs Improvement	Pass	Credit	Distinction	High Distinction
Executive Summary and Business Background <i>Weighting: 12.5%</i> <i>Max: 4.38 Marks</i> <i>ULO: 4</i>	Provides little to no meaningful information content relating to minimal report expectations. Does not meet expectations regarding any findings, implications and little or only shallow purposeful security recommendations only. Substantive parts of the report either not covered or missing. The business background contains no meaningful detail and is highly superficial or misrepresents the actual current business security management goals.	Inadequate executive summary that omits main findings, implications and key recommendations for improvement. Thus, it does not engage, inform or motivate the report audience. Alternatively, executive summary may be missing. Very little background to the business has been provided. The background is inconsistent and confusing or incomplete and frames little of the current security management goals and related aspects expected. Little or no current business security management goals identified or expressed.	Executive summary presents only limited findings, implications and recommendations for improvement and may therefore not fully engage, inform or motivate the report audience. Alternatively, executive summary may be missing. Acceptable background provided that just meets the scope of the report and some of the key points expected. However, it is still very general and discusses only some of the business background and goals. Little discussion of existing security related strategy, services or applied and frames some of the business and security management goals identified or expressed.	Fair executive summary that provides quite interesting information about findings and recommendations and should interest or inform the report audience. Alternatively, executive summary may be missing. Good background provided that meets the scope of the report and adequately determines many of the key points expected. It is reasonable and discusses much of the business background, goals and frames most of some of the current security management goals and related aspects expected.	Very good executive summary with main findings and recommendations clearly presented. Very good background provided that effectively meets the scope of the report and clearly explains most of the key points expected. It is strategically relevant and discusses most the business background and goals pertaining to most of the current security management aspects expected.	Excellent executive summary that identifies the main findings, implications and key recommendations for improvement clearly, logically and effectively. The background section consistently and effectively outlines all the key points expected. The type of business strategy, goals, products and services are clearly identified. It is highly relevant and directly discusses the business background security and effectively frames the key current security management aspects as aligned with the business goals and aspirations.
Current Profile <i>Weighting: 24%</i> <i>Max: 8.4 Marks</i> <i>ULO: 3 & 4</i>	Fails to accurately summarize the cybersecurity postures across any of the NIST functions. The ratings provided are baseless or missing. Provides no real analysis of how the business achieves or falls short in cybersecurity measures. Lacks any mention of specific practices or technologies. Does not identify any strengths or weaknesses, offering no insights into the business’s cybersecurity landscape.	Incompletely summarizes the cybersecurity postures, missing several NIST functions. Ratings are provided but with little to no justification. Descriptions of how the business manages its cybersecurity are vague and lack detail on practices or technologies. Minimal use of direct quotes or summaries from the questionnaire. Some strengths and weaknesses are noted but are not well-supported by specific examples or analysis of underlying factors.	Provides a basic summary of the business’s cybersecurity across all functions with simplistic justifications for the ratings. Describes general practices and technologies but with limited depth. Mentions how the business achieves or fails in areas without extensive detail. Identifies broad strengths and weaknesses but lacks a thorough examination of the reasons behind the business's cybersecurity performance.	Adequately summarizes the cybersecurity postures with justified ratings. Each NIST function is covered, showing a basic understanding of the firm’s practices. Provides a clear description of cybersecurity practices, including some specifics on technologies and policies. Utilizes quotes or summaries from the questionnaire effectively. Highlights strengths and weaknesses with some discussion of underlying factors such as resource allocation and employee training.	Provides a detailed and accurate summary of the business’s cybersecurity across all NIST functions. Ratings are well-justified with in-depth explanations. Descriptions include detailed specifics of practices, technologies, and policies. Makes good use of the questionnaire to support points. Thoroughly discusses both strengths and weaknesses, with insightful analysis of underlying reasons such as technology adoption and training effectiveness.	Provides an exceptional, comprehensive summary of cybersecurity postures across all NIST functions, with nuanced justifications for each rating. Offers an in-depth analysis of current practices, technologies, and policies, adequately citing the questionnaire to substantiate detailed descriptions. Excellently highlights and critically evaluates strengths and weaknesses, including a deep dive into underlying factors such as strategic resource allocation and organizational cybersecurity culture.
Target Profile <i>Weighting: 24%</i> <i>Max: 8.4 Marks</i> <i>ULO: 3 & 4</i>	Fails to appropriately focus on the required three NIST functions, including Govern. The profile lacks any substantial context relating to the business's threat environment, regulatory requirements, or strategic business objectives. Does not consider the organization's risk tolerance or propose any future-oriented cybersecurity enhancements. The vision for cybersecurity improvements is absent or incoherent, showing no alignment with business needs or proactive planning.	Partially addresses the three NIST functions but omits significant details regarding the Govern function or the business's specific context. Minimal discussion of threat environment and regulatory requirements. Briefly mentions the organization's risk tolerance but does not effectively integrate this into cybersecurity planning. Goals are stated but are basic and not tailored to any dynamic factors. Offers a vague and weak vision for enhancing cybersecurity practices, lacking clarity and strategic alignment with business needs.	Covers the three required NIST functions, including Govern, with a basic understanding of the business's unique context. Acknowledges the threat environment and some regulatory requirements. Discusses the organization's risk tolerance and provides generic cybersecurity goals. There is minimal anticipation of changes in business requirements or technology impacts. Provides a straightforward vision for enhancing cybersecurity. The approach addresses immediate needs but lacks a proactive strategy for future challenges.	Good analysis of the three selected NIST functions, including Govern, reflecting an adequate understanding of the business's unique context. Adequately discusses the threat environment and regulatory requirements. Considers the organization's risk tolerance and begins to acknowledge potential changes in business requirements and technology, but the integration of these aspects into cybersecurity planning is still limited. Offers a clear vision for enhanced cybersecurity that aligns with immediate needs. The approach is proactive but needs greater	Detailed analysis of the three NIST functions, including Govern. The profile is well-contextualized within the business's environment and objectives. Effectively considers the organization's risk tolerance. Begins to integrate anticipation of new business demands, regulatory changes, and technology adoption into the cybersecurity goals, though this is not yet fully developed. Articulates a strong vision for cybersecurity that begins to consider future challenges. The strategy is proactive and anticipates some future business shifts.	Exceptional and comprehensive analysis of the required three NIST functions, including Govern. Perfectly contextualizes the cybersecurity strategy within the business's unique environment and strategic objectives. Fully anticipates changes in the business landscape and cybersecurity threat intelligence. Shows a deep understanding of the organization's risk tolerance and dynamically integrates future business and technology shifts. Goals are clearly defined, responsive, and highly adaptable. Offers an outstanding and visionary approach to cybersecurity

				emphasis on future challenges and adaptability.		practices, proactively planning for both current needs and future challenges. The strategy is exemplary in its foresight and adaptability, aligning perfectly with business strategies.
Gap Analysis and Action Plan <i>Weighting: 27%</i> <i>Max: 9.45 Marks</i> <i>ULO: 3</i>	<p>No identification of meaningful gaps. Lacks insight into potential risks or impacts of these gaps.</p> <p>No actionable plan presented. Does not reference Implementation Examples or other frameworks/guidelines.</p> <p>No timelines, budgets, or metrics proposed. Completely lacks detail on how to evaluate improvements.</p>	<p>Identifies basic gaps but lacks depth in analysis of implications and risks. Minimal holistic perspective.</p> <p>Suggests a basic action plan without substantial details or clear strategies. Limited use of Implementation Examples or other frameworks/guidelines.</p> <p>Provides timelines and budgets, but these are not well-founded. Metrics for evaluating effectiveness are suggested but are simplistic and lack clarity.</p>	<p>Identifies significant gaps with some discussion of potential risks, though lacking in detail and comprehensive analysis.</p> <p>Action plan includes some specific initiatives but lacks thoroughness. References to Implementation Examples or other frameworks/guidelines are minimal and not well integrated.</p> <p>Timelines and budgets are somewhat realistic but lack detailed justification. Basic metrics are included but they do not provide detailed measures of effectiveness.</p>	<p>Good identification of significant gaps with reasonable analysis of implications and risks.</p> <p>Acknowledges the impact of gaps. Detailed action plan including specific initiatives and reasonable use of Implementation Examples or other frameworks/guidelines. Plan shows practical relevance.</p> <p>Realistic timelines and budgets, with basic metrics provided that are somewhat useful for measuring the effectiveness of the improvements.</p>	<p>Very good identification of significant gaps, offering a holistic perspective on potential risks .</p> <p>Analyzes dependencies between gaps, showing how they are interconnected and the cumulative impact of non-action.</p> <p>Comprehensive action plan that integrates detailed initiatives addressing multiple gaps simultaneously. Utilizes Implementation Examples or other frameworks/guidelines effectively to create synergistic strategies that address underlying systemic issues.</p> <p>Well-justified timelines and budgets. Metrics are detailed and actionable, providing clear measures of the effectiveness of the improvements.</p>	<p>Exceptional analysis of significant gaps, thoroughly understanding risks and non-action implications.</p> <p>Explores in-depth dependencies among gaps, showing how addressing one impacts others, fostering comprehensive improvements across the cybersecurity landscape.</p> <p>Exceptional, detailed action plan with innovative and strategic initiatives, robustly grounded in NIST CSF 2.0 or other relevant frameworks. Demonstrates deep integration with the business’s resources and strategic objectives.</p> <p>Proposes highly realistic and precise timelines and budgets, based on comprehensive business analysis.</p> <p>Advanced, clearly defined metrics provide meaningful insights into the effectiveness of the improvements and are fully actionable within 18 months.</p>
Reflection <i>Weighting: 7.5%</i> <i>Max: 2.62 Marks</i> <i>ULO: 4</i>	<p>No proper reflection undertaken with little to no insight into the team's effectiveness or no examples drawn from the project team experience.</p> <p>Clearly limited or no consideration given to lessons learnt from the experience, either at the team or individual level.</p> <p>No cohesion of discussion, unfocused, no use of examples and discussions are highly superfluous to expectations.</p>	<p>Reflection is inadequate and does not meet the report expectations of a reflective consideration of individual and group experiences of the tasks undertaken.</p> <p>Lacked cohesion and limited insight into the team’s effectiveness and only limited examples drawn from the project team experience.</p> <p>The reflections are missing or too simplistic or provide very little sign of personal and group learning from the assignment experience.</p>	<p>Limited insight into the team’s effectiveness and only limited or weak examples drawn from the project team experience.</p> <p>Otherwise, an acceptable effort.</p> <p>Your reflection articulates and expresses some of the general challenges only and the learning thereby gained.</p> <p>Your reflections are very general and deliver only one or two basic insights stemming from your experiences. There is room for improvement. Reflections could be deeper and much more meaningful.</p>	<p>Reflection still focused on description, personal feelings with some evaluation. Analysis, evaluation and insight into team effectiveness is not strong. Points illustrated were general rather than specific examples drawn from the project team experience.</p> <p>Although a good effort. Your reflection articulates and expresses the main challenges of the assignment and identifies the learning gained. Your reflections are meaningful, argued, justified and deliver mostly informative insights. Further and deeper insights would add value.</p>	<p>Reflection demonstrated analysis, evaluation and critical insights into team effectiveness. Points are illustrated with mostly specific examples drawn from the project (maybe mostly positive). May lack insightful conclusions about the team experience.</p> <p>A very good effort here. Your reflection critically articulates and mostly expresses the challenges experienced and learning gained. Your reflections are very good, well-argued, justified and clearly deliver relevant and informative insights into the tasks undertaken.</p>	<p>Excellent effort. Your reflection critically articulates and insightfully expresses the challenges encountered and the learning experiences gained. Your reflections are exemplary, well-argued, sophisticated and deliver highly relevant and informative insights into the tasks undertaken.</p> <p>Reflection demonstrated deep analysis, evaluation and insights into team effectiveness illustrated with both progressive and negative vignettes drawn from the project team experience. Including insightful conclusions about the team experience.</p>
Report Presentation <i>Weighting: 5%</i> <i>Max: 1.75 Marks</i> <i>ULO: 4</i>	<p>Little to no planning or formatting evident in the structure of the report. Poorly written with spelling and grammar errors prevalent throughout the Report.</p> <p>The report is not of an acceptable professional standard and lacks relevant context, logic or quality</p>	<p>Report presentation demonstrates a lack of attention to presentation detail and inadequately meets report presentation expectations.</p> <p>Very little consideration has been given to engaging the reader though writing style, or to the structure, flow and content of the</p>	<p>Acceptable report presentation.</p> <p>Overall, your report presentation is of a fair standard and of reasonable quality.</p> <p>There is room for improvement in style, expression, business and consideration of the audience.</p>	<p>Good report presentation. Overall, your report presentation is of a good standard, style and expression.</p> <p>It is reasonably engaging and mindful of the intended audience and good to read in structured and logical manner.</p>	<p>Very good report presentation.</p> <p>Overall, your report presentation is of a high standard, with very good style, expression and business.</p> <p>It is for the most part engaging and attentive of the intended audience and easy to read and structured in a logical well written manner.</p>	<p>Excellent report presentation.</p> <p>Overall, your report presentation is exemplary and of an excellent standard.</p> <p>Presentation is of a high quality, well- written, well-organised, and highly engaging. It is very considerate of</p>

advice suitable for a business to find useful.
Highly unprofessional with no attention to detail evident. The poor quality of the report is not suitable for return to the business.

report, resulting in a poorly presented or ambiguous document. The report requires significant revision to reach the expected presentation standard.