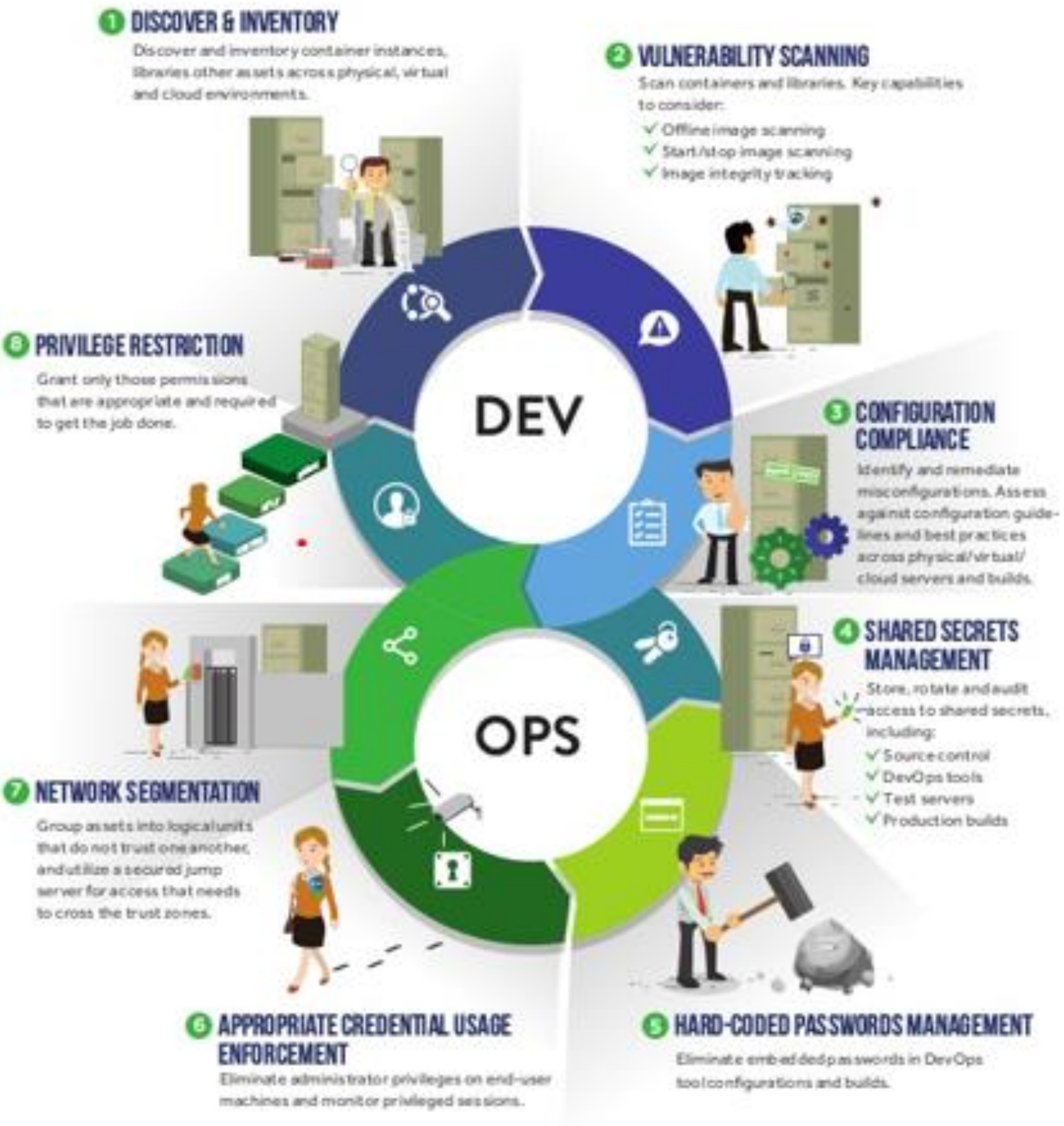
FIT5129

Group Assignment 2



1 DISCOVER & INVENTORY

Discover and inventory container instances, libraries other assets across physical, virtual and cloud environments.

2 VULNERABILITY SCANNING

Scan containers and libraries. Key capabilities to consider:

- ✓ Offline image scanning
- ✓ Start/stop image scanning
- ✓ Image integrity tracking

3 CONFIGURATION COMPLIANCE

Identify and remediate misconfigurations. Assess against configuration guidelines and best practices across physical/virtual/ cloud servers and builds.

4 SHARED SECRETS MANAGEMENT

Store, rotate and audit access to shared secrets, including:

- ✓ Source control
- ✓ DevOps tools
- ✓ Test servers
- ✓ Production builds

5 HARD-CODED PASSWORDS MANAGEMENT

Eliminate embedded passwords in DevOps tool configurations and builds.

6 APPROPRIATE CREDENTIAL USAGE ENFORCEMENT

Eliminate administrator privileges on end-user machines and monitor privileged sessions.

7 NETWORK SEGMENTATION

Group assets into logical units that do not trust one another, and utilize a secured jump server for access that needs to cross the trust zones.

8 PRIVILEGE RESTRICTION

Grant only those permissions that are appropriate and required to get the job done.

(Sourced from Instagram of Beyond Trust, 2021)

Case Problem Solving:

Managing Cyber Risks in DevOps Projects

Disclaimer

The information contained in this case story is to be used only as a case study example for teaching and learning purposes. The case information is both factual and fictional. The assignment expresses opinions that are intended to stimulate and assess students in their abilities to apply cybersecurity knowledge and critical thinking in a mock-up and complex problem-solving scenario.

Learning Outcomes

The following table cross references the unit and assignment learning outcomes.

Unit Learning Outcomes	This Assignment Learning Outcomes
• Explain critical factors of enterprise security planning, operations and management;	Students are confident to explain: • the enterprise goals of cybersecurity; • how cybersecurity incidents of intrusion, sabotage, espionage or data theft, and vandalism prevails in many forms, all attempting to undermine these goals.
• Perform risk analysis and assessment;	Students are able to research and innovate a cybersecurity framework, which guides project managers to be cybersecurity diligent in their DevOps project management (PM) work.
• Provide practical security policies, strategies and implementation plan for enterprise systems.	Students understand how cybersecurity, a governance and compliance obligation, is applied in designing cybersecurity frameworks and functional guides for use in project management work.

The assignment also helps students to experience, firsthand, the complex nature of thinking when working as a group to examine multiple resources. At the same time, students also perform a number of interrelated and dynamically varying activities to solve a cybersecurity problem, by using cybersecurity concepts and academic research, critical thinking and literacy techniques.

The Case Story

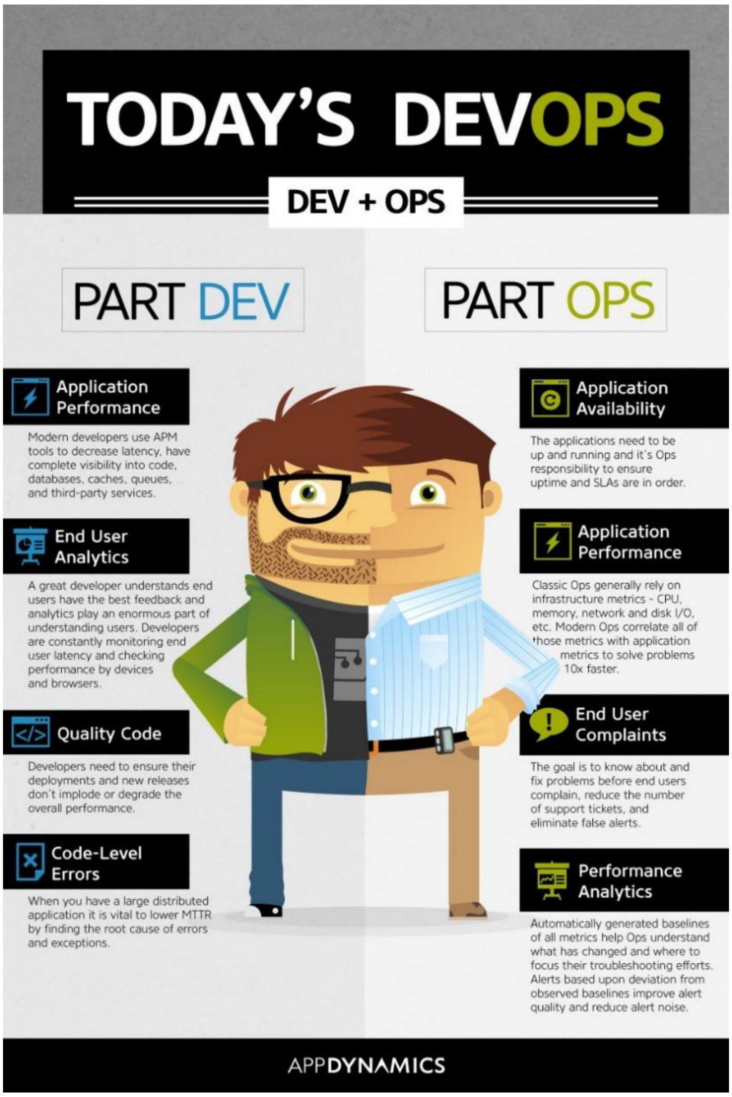
Problem Insights: During the last five years, the need to integrate cybersecurity effectively in DevOp and project management work has significantly increased. There are many underlying reasons one can find in the literature. Covid-19 has exasperated the immediate rush to fulfil this enterprise need. No one institution can fight cyberattacks alone. Enterprises are collaborating with each other and aligning their capacity building to their governments' cybersecurity priorities. Not surprising, many researchers and practitioners worldwide are adopting the US's NIST cybersecurity recommendations to build their cybersecurity capacities in software DevOp projects. Despite this fast-growing community of practice (CoP) work is growing, the prevalence of software security (especially open source) vulnerabilities continues to exist without effective detection. This short falling cybersecurity trend is expected to continue for several years to come (Osbourne, 2020).

Case Requirements: Your client is Monash University's FIT5057 division. A special green-field project has been setup. The project director is Phil Man, who is supported by the following staff members with specialised roles:

1. Chan Cheah and Asha Padisetti – Security Enterprise Architecture & Partners Development.
2. Marino Yang, Karen Vella, Patrick Kennedy – Project Management Research.
3. Nergiz Ilhan and Ross Pearson – Project Management Professional Practice.

Your assignment group belongs to a well-known and upcoming company, Capish Gemingo Global (CEG), specialising in securing DevOp capabilities development in enterprises.

The **FIT5057 DevOps Security** (**FDS**) project team is new to cybersecurity. Phil has completed due diligence on your company, choosing your group to assist in the modernisation of Monash University's project management education and practice capabilities.



Application Performance

Modern developers use APM tools to decrease latency, have complete visibility into code, databases, caches, queues, and third-party services.

End User Analytics

A great developer understands end users have the best feedback and analytics play an enormous part of understanding users. Developers are constantly monitoring end user latency and checking performance by devices and browsers.

Quality Code

Developers need to ensure their deployments and new releases don't implode or degrade the overall performance.

Code-Level Errors

When you have a large distributed application it is vital to lower MTTR by finding the root cause of errors and exceptions.

Application Availability

The applications need to be up and running and it's Ops responsibility to ensure uptime and SLAs are in order.

Application Performance

Classic Ops generally rely on infrastructure metrics - CPU, memory, network and disk I/O, etc. Modern Ops correlate all of those metrics with application metrics to solve problems 10x faster.

End User Complaints

The goal is to know about and fix problems before end users complain, reduce the number of support tickets, and eliminate false alerts.

Performance Analytics

Automatically generated baselines of all metrics help Ops understand what has changed and where to focus their troubleshooting efforts. Alerts based upon deviation from observed baselines improve alert quality and reduce alert noise.

(Instagram, 2021)

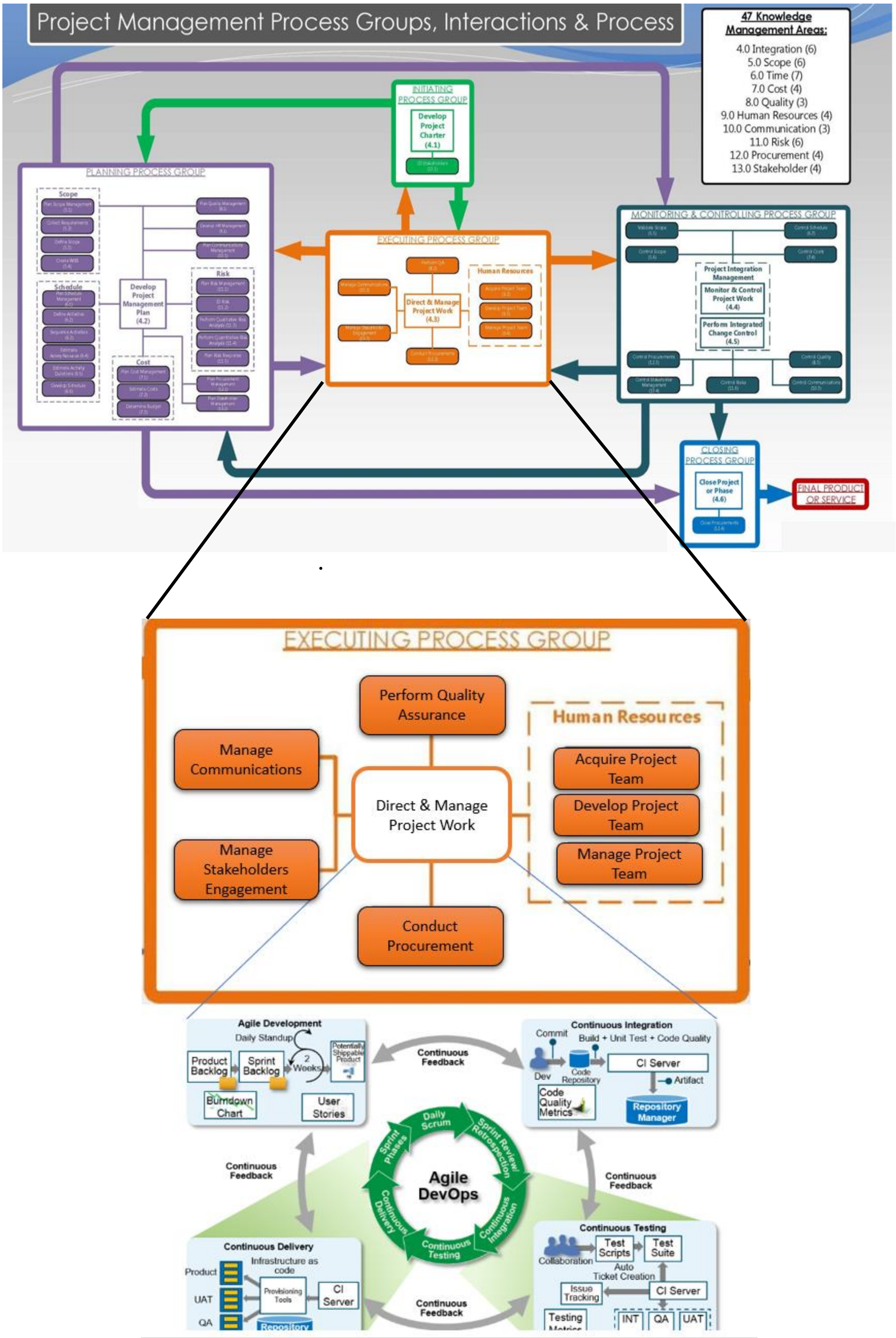
You have been advised by the Monash Cybersecurity Unit that the university adopts NIST cybersecurity recommendations to formulate the university's cybersecurity policy and compliance procedures, for all projects and online activities.

University research data is considered as Australia's critical infrastructure for a number of reasons. Hence, it is important that project managers take ownership to identify and manage the vulnerabilities in their DevOps software development work and support operations. NIST has done significant work to address this global problem and provides reliable resources for the project team to use as official user requirements.

This a first-time green field cybersecurity practice development project. You have been asked to **recommend an NIST aligned cybersecurity framework and procedural instructions for securing research software that are in development and currently accessed by other university's stakeholders.** The research outcomes will also potentially be integrated in teaching curriculums.

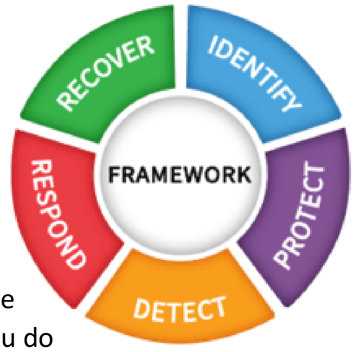
The Project Director has asked your company to assist his team to develop an NIST driven project management framework and guidelines for research project managers. All research software projects adopt Agile Scrum methodology and takes a DevOps perspective in its SDLC work.

The university uses PMBoK as its corporate project management standard. How PMBoK process groups' workflows integrate DevOps activities is summarised as follows (Instagram, 2021):



The diagram above gives you insights of the chosen knowledge areas that you need to focus on, to identify and manage the cyber risks of DevOp work during project management. These knowledge areas are *scope management, stakeholders management, communications management, procurement management and project team resource management*.

Your work focus should be directed at protecting Monash University's research data from cyber-attacks. Australian universities research databases are considered part of Australia's critical infrastructure. You need to research why research data, during project development and after project closure needs protection.



You are expected to design a visual conceptual framework that uses the NIST Cybersecurity framework. This means you need to figure out how to cross reference the high-level process-groups of the NIST framework against the work breakdown structures of the specified PM knowledge areas. Using this cross-reference map, you can organise and write the instructions for integrating the NIST process groups in PM work. The instructions are clear enough to to manage the cyber threats you have identified and new future ones that you may not even be aware today. You do not have to drill down to the level specifying tasks and referencing to underpinning best practice standards' specifications.

Some resources to help you get started in your literature review. However they are not academe peer reviewed literature, the later which you have to consider including in your citations:

1. The NIST master cybersecurity framework - https://www.nist.gov/cyberframework
2. NIST's recent whitepaper titled Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework
3. Current NISTIR 8286 publications that discuss the implications of cybersecurity and enterprise risk management integration
4. The State of DevOps Report - the 2019 report (more relevant for this assignment) and the 2020 report.
5. NIST System Engineering Approach V1 and V2:
    a. Volume 1 - *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems;*

    b. Volume 2 *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*

A report template is provided. Review it with a critical eye, as it also help you understand how to communicate critical thinking ideas in writing. You will realise that one can use the generic process flows of problem-solving to structure the writing to be analytical, logically flowing and easy to read.

Recommended Report Writing Guidelines

Executive Summary – summarises the client's problem; solution proposal and next step recommendation within 1 page or lessor.

Some writing tips:

- Be outcomes focused on your writing. Avoid writing what you did. Business readers are interested in your problem-solving findings first. If they are interested to know what you did, they would then read the full report later on.
- Executive summaries are for readers who are time poor. An executive overview enables them to extract the key and relevant information of the full report The writing goals are for readers to (a) get a clear understanding of your proposal; and (b) be informed and confident to make quick decisions that support your proposal and recommendations.
- Do not write additional information that is irrelevant to achieving these writing goals.

Main Report components

1. **Introduction** – clearly states the purpose of writing. It should also link to the report's last section, avoiding unnecessary information.

2. **Problem Description** (recommended 2 pages or under)
   2.1. **Problem Analysis** – Identifies and analyses why it is important that Monash protects its research data from cyber-attacks; indicates at least 6 diverse types (human and machine) of likely cyber-attacks exposing Monash.
   2.2. **Problem Statement** – Provides an objective and clear statement of the current problem Monash is facing and the immediate resolution action that initiated this assignment (recommended 1 paragraph).

3. **Assumptions**: To do this assignment, you are to apply certain knowledge concepts from different disciplines, other than cybersecurity. You are to state and define all these knowledge concepts, including any practice methodologies (e.g. NIST Cybersecurity Framework, PMBoK) you would have used.

   We will also assess you on how you organise the sought information in a manner that makes easy reading and we can easily see that you understand and can apply these stated concepts proficiently. We will focus on how you structure this section's heading hierarchy, use research citations and construct and link your paragraphs to demonstrate your competency in analytical writing to express your critical ideas.

4. **Prevailing Cybersecurity Threats in Monash's Software Development Research Projects**: Referring to the cyber attacks you identified earlier, research and apply your findings to predict these cyber risks' occurrence likelihoods and impact severities, both qualitatively and quantitatively.

5. **Solution Proposal - <give a meaningful name>**: Present and introduce a visual overview of your solution, followed by instructional procedures that explain how Monash project managers can apply it to integrate cybersecurity diligence in their PM work.

   We will focus on how you structure this section's heading hierarchy; use research citations; construct and link your paragraphs; and use visual communication and instructional writing techniques to demonstrate your ability in writing easy to read and follow procedural instructions.

6. **Conclusion & Recommendation:** Present an opening paragraph that *concludes* clearly from your problem statement and refers to the solution you discussed in section 5, stressing why the solution is important. Following 1-3 paragraphs *recommend* what to do next, usually providing high level implementation planning insights.

   Make sure there is a connection between your Introduction and this section.

7. **Reference List** – at least 20, of which 50% must be academe sourced.

   Max ~~minimum~~ of pages – **30 pages**, inclusive of executive summary & reference list.