* Project title: Cyber Security policy Management System (CSPMS)
* Proposed solution:
* I will develop a system that serves GRC (Governance Risk and Compliance) by managing cyber security policies. This system will help the organizations in creating and flowing approval for these policies which lead to increase the security level of the organization.
* Cyber Security Policy Management System (CPMS) tracks the status of each policy so that can know the status of each policy, whether it has been viewed and approved by the employees. Moreover, it is possible to display the status of the policy based on the department to know the level of approval of the policy, which helps the cybersecurity department to know that this policy has been approved.
* User stories:
* As cyber security department, we may create a category of all accessible polices documents and categorise them according to cyber security policy topics in order to help employees to get access to suitable policies. so that employees may now quickly view the cyber security policy.
* As cyber security department, we may update a department, so they can update descriptions and name of department.
* As cyber security department, we may delete a department, they can delete department without effect user.
* As cyber security department, we may update a category, so they can update descriptions and name of category.
* As cyber security department, we may delete a category, they can delete category without effect policy.
* As cyber security department, we can upload the policies documents as PDFs files and select suitable category, so that each policy document contains detail cyber security policy information. So that enable the employee to read each policy separately.
* As a cyber security department, we may add an image to each policy document, so that make it more accessible for employees.
* As cyber security department, we can create a description for each policy document Contains an overview of this document. so that employees enable to know about this document before they open it.
* As the cyber security department, we may set the date for each policy to take approval on it, so cyber security department can look for employees who have not given approval on this policy.
* As the cyber security department, we may send reminders to employees who have not given approval on this policy by the due date, thus employees can get a notification through email.
* As the cyber security department, we make to escalate to employee’s manager for any employee who have not approved this policy by the due date and have been notified by email. Therefore, the manager can send another notice through the system to remind them to approve these documents.
* As the cyber security department, we have access to the results for both individual employees and the department, which enables us to identify the percentage of employees who have not approved or approved for each policy.
* As a cyber security department, we have the ability to update policy documents as PDF files; as a result, this policy document will be updated. As a consequence, the system will notify employees who have already read this policy to read it again and obtain further approval from them.
* As employees, we have access to our account, which allows us to track our progress.
* As employees, we have access to a thorough page for each policy which enables us to know everything about it.
* As employees, we have access to a catalogue of all available policies, which enables employees to easily access policy documents.
* As employees, we must mark each policy as "viewed" after it has been approved in order to keep track of the policies we have previously completed, and which policies need to read.
* As employees, we may review whatever policies we have completed or have yet to complete in order to determine which policies documents we need to read in order to approve these policies.
* As the manager of each department, I can view the results for each employee and the department averages, allowing me to determine the department's levels of percentage of approval on cyber security policy and also encourage my staff to read and approve.
* As users, we can view the dashboard that displays the approval rate for each policy. This allows us to see approved policies as employees, as department managers, and as cyber security department managers.



* Assumptions
* Each employee has accounted a predefined username and password by active directory (Domain).
* CSPMS can get organisational structure and employee information such as departments and managers from the Human Resources System (HR).
* Policies will be available for uploading and updating on the system.
* All policies are valid and updated.
* The department of cyber security should have an administrator account on our system to take all permissions.
* All key stakeholders (employees, managers, and the cybersecurity department) will get reports on the outcome of polices approvals based on the permissions.
* Departments of cyber security should have all the required expertise and skills to create the policy document.
* When adding or updating a policy to the system, a workflow will be used to create it and then confirm it for employee reading and approval stage it.