[**Principal Project Manager - Cyber Security**](https://www.seek.com.au/job/77342166?ref=search-standalone&type=standard&origin=jobTitle#sol=230cbdd286bc96e7366a6de2bd3aa089479ab3e0)

**Role Overview:**

Manage complex Information Management (IM) and Information and Communication Technology (ICT) projects to enhance healthcare delivery while maintaining information security.  
    
**Key Responsibilities:**

* Lead large-scale, complex projects following organisational project management methodologies
* Implement and oversee project management techniques, including risk management and benefits realisation
* Monitor and report on project performance, resources, and costs
* Manage stakeholder relationships and facilitate effective communication
* Lead and mentor multi-disciplinary project teams

**Current Projects Include:**

* Upgrading endpoint protection systems
* Improving vulnerability management services
* Implementing application control on servers
* Deploying enterprise password management solution
* Migrating endpoint privilege management to cloud
* Modernising remote access authentication
* Upgrading enterprise firewall at a major hospital
* Enhancing web gateway platform

**Requirements:**

* Adherence to organisational values and quality standards
* Strong project management skills
* Experience in cybersecurity or related IT fields
* Excellent communication and leadership abilities

The role focuses on delivering critical cybersecurity improvements in a healthcare setting, balancing modern service delivery with robust information security practices.

# Interview Script

**Interview Question 1: Leading Large-Scale, Complex Projects**

**Interviewer:** "Can you describe a large-scale, complex project you have managed, particularly in the context of information security?"

**Less Effective Response**

**Interviewee:** "I've managed large projects before, focusing on various aspects like budget and timelines. It's important to keep everything on track."

**More Effective Response**

**Interviewee:** "In my previous role, I led a large-scale project to implement a comprehensive endpoint protection system across a healthcare network. This project involved coordinating with multiple stakeholders, including IT, compliance, and clinical teams, to ensure that the new system met both security and usability requirements. We adhered to a strict project management methodology, which included detailed risk assessments, resource allocation, and continuous monitoring of progress. I implemented a robust communication plan to keep all stakeholders informed and engaged, addressing concerns and ensuring alignment with the project goals. The project was completed on time and within budget, significantly enhancing our cybersecurity posture and protecting sensitive patient data."

**Interview Question 2: Implementing Project Management Techniques**

**Interviewer:** "How do you implement and oversee project management techniques like risk management and benefits realization?"

**Less Effective Response**

**Interviewee:** "I use standard project management techniques like risk assessments and tracking benefits. It's part of the process."

**More Effective Response**

**Interviewee:** "Implementing project management techniques like risk management and benefits realization is crucial for project success. I start by identifying potential risks during the project planning phase, categorizing them by likelihood and impact. We develop mitigation strategies for high-risk areas and regularly review these risks throughout the project lifecycle. For benefits realization, I define clear metrics and key performance indicators (KPIs) at the outset to measure the project's success. For example, during a vulnerability management services improvement project, we set KPIs for reducing identified vulnerabilities by 40% within the first six months post-implementation. These techniques help ensure that we not only deliver projects on time and within budget but also achieve the intended security enhancements and value for the organization."

**Interview Question 3: Monitoring and Reporting on Project Performance**

**Interviewer:** "Can you provide an example of how you have monitored and reported on project performance, resources, and costs?"

**Less Effective Response**

**Interviewee:** "I keep track of project performance using standard tools and make sure to report regularly to stakeholders."

**More Effective Response**

**Interviewee:** "In my previous position, I used a combination of project management software and dashboard tools to monitor project performance, resources, and costs. For a project involving the upgrade of our enterprise firewall, I established a detailed project plan with specific milestones and deliverables. Weekly status meetings were held to review progress, and I used dashboards to provide real-time visibility into resource allocation, budget adherence, and any emerging issues. I also prepared comprehensive monthly reports for senior management, highlighting key achievements, budget status, and any risks or issues requiring escalation. This transparent and data-driven approach ensured that we stayed on track and allowed for timely adjustments as needed."

**Interview Question 4: Managing Stakeholder Relationships**

**Interviewer:** "How do you manage stakeholder relationships and ensure effective communication throughout a project?"

**Less Effective Response**

**Interviewee:** "I keep stakeholders informed through emails and meetings. I make sure everyone knows what's going on."

**More Effective Response**

**Interviewee:** "Managing stakeholder relationships is critical, especially in complex cybersecurity projects. I start by identifying all key stakeholders and understanding their concerns and expectations. I then establish a communication plan that includes regular updates through various channels, such as email, video conferences, and in-person meetings. For example, during the deployment of an enterprise password management solution, I held weekly briefings with the IT team, monthly steering committee meetings with senior executives, and user training sessions. I also created a project newsletter to keep all stakeholders informed about progress and any changes. By maintaining open and transparent communication, I ensured that stakeholders were engaged, informed, and supportive throughout the project lifecycle."

**Interview Question 5: Leading and Mentoring Multi-Disciplinary Project Teams**

**Interviewer:** "Can you share your experience leading and mentoring multi-disciplinary project teams in a cybersecurity context?"

**Less Effective Response**

**Interviewee:** "I've led teams with different skills and backgrounds. I make sure everyone knows their tasks and support them as needed."

**More Effective Response**

**Interviewee:** "Leading multi-disciplinary project teams requires understanding the unique skills and perspectives each member brings to the table. In my role managing a project to modernize remote access authentication, I led a team that included cybersecurity specialists, network engineers, and software developers. I fostered an environment of collaboration by organizing cross-functional workshops and regular team-building activities. I also provided mentorship, offering guidance on technical challenges and career development. By encouraging knowledge sharing and open communication, I helped the team overcome obstacles and deliver innovative solutions. This approach not only ensured the project's success but also contributed to the professional growth and satisfaction of team members."

**Interview Question 6: Upgrading Endpoint Protection Systems**

**Interviewer:** "Can you describe your experience with upgrading endpoint protection systems, particularly in a healthcare environment?"

**Less Effective Response**

**Interviewee:** "I've worked on upgrading antivirus and security systems before. It's important to keep everything up to date."

**More Effective Response**

**Interviewee:** "In a previous role, I led a project to upgrade endpoint protection systems across a network of hospitals. The objective was to replace outdated antivirus software with a more robust endpoint detection and response (EDR) solution. We conducted a comprehensive needs assessment, including evaluating the specific security requirements of different departments, such as emergency services and patient data management. I coordinated with the IT and cybersecurity teams to deploy the new system in phases, ensuring minimal disruption to hospital operations. We also provided extensive training for staff on the new system's features and capabilities. This upgrade significantly improved our ability to detect and respond to threats in real-time, enhancing the overall security of sensitive patient information."

**Interview Question 7: Improving Vulnerability Management Services**

**Interviewer:** "How have you approached improving vulnerability management services in your projects?"

**Less Effective Response**

**Interviewee:** "I've implemented regular vulnerability scans and patch management processes to improve security."

**More Effective Response**

**Interviewee:** "Improving vulnerability management services involves a comprehensive approach that includes proactive identification, assessment, and remediation of vulnerabilities. In one project, I led the initiative to enhance our vulnerability management program by integrating advanced scanning tools and implementing a more rigorous patch management schedule. We conducted a thorough risk assessment to prioritize vulnerabilities based on their potential impact on critical systems, particularly in areas like patient record systems and medical device networks. I also established a cross-functional task force to address high-risk vulnerabilities promptly. This included setting up automated alerts for critical vulnerabilities and creating detailed remediation plans. The improvements resulted in a significant reduction in our risk profile and a more secure healthcare IT environment."

**Interview Question 8: Implementing Application Control on Servers**

**Interviewer:** "Can you discuss a time when you implemented application control on servers and the challenges you faced?"

**Less Effective Response**

**Interviewee:** "I've set up application control policies to restrict access to certain applications on servers. It helps in maintaining security."

**More Effective Response**

**Interviewee:** "In a project to enhance server security, I implemented application control measures to restrict unauthorized software installations and execution. This involved defining and enforcing whitelisting policies, where only approved applications could run on critical servers, such as those handling electronic medical records (EMRs). One challenge we faced was ensuring that these controls did not disrupt legitimate administrative tasks or healthcare services. To address this, we collaborated with various departments to identify essential applications and processes, conducting thorough testing before full deployment. We also established an exception management process to handle legitimate needs for non-whitelisted applications. This implementation not only tightened security controls but also reduced the attack surface significantly."

**Interview Question 9: Migrating Endpoint Privilege Management to the Cloud**

**Interviewer:** "What experience do you have with migrating endpoint privilege management to the cloud, and what considerations did you take into account?"

**Less Effective Response**

**Interviewee:** "I've worked on migrating some security functions to the cloud, including privilege management. It's a good way to improve security."

**More Effective Response**

**Interviewee:** "Migrating endpoint privilege management to the cloud requires careful planning and execution to ensure security and compliance. In my previous role, I led a project to move our on-premises privilege management solution to a cloud-based platform. Key considerations included data security, compliance with healthcare regulations, and integration with existing systems. We selected a solution that offered robust encryption, granular access controls, and audit capabilities. The migration process involved extensive testing in a sandbox environment to ensure compatibility and performance. We also provided comprehensive training for IT staff and end-users to familiarize them with the new system's features. This migration not only enhanced our security posture by providing more flexible and scalable privilege management but also improved visibility and control over user activities."

**Interview Question 10: Modernising Remote Access Authentication**

**Interviewer:** "How have you approached modernizing remote access authentication, especially in the context of a healthcare setting?"

**Less Effective Response**

**Interviewee:** "I've implemented multi-factor authentication (MFA) for remote access. It's a crucial step for securing remote connections."

**More Effective Response**

**Interviewee:** "Modernizing remote access authentication in a healthcare setting involves balancing security with ease of access for medical professionals. In a recent project, I spearheaded the implementation of a modern authentication solution that included multi-factor authentication (MFA) and single sign-on (SSO). We chose a solution that integrated seamlessly with our existing systems, such as EMRs and telemedicine platforms. One key consideration was ensuring that the MFA process was user-friendly, given the high-pressure environment in which healthcare professionals operate. We implemented biometric authentication options and streamlined the user interface to minimize disruptions. Additionally, we conducted extensive user training and established a support team to assist with any issues during the transition. This modernization significantly improved our security while maintaining a seamless user experience for healthcare providers."