

SECURITY

Solutions Partner for Security Designation

GOVERNMENT

Determine Industry Requirements

What Are We Assessing?

The first step is to identify which industries are ideal for our Security solution, which we have done using data available to us, as outlined in Lesson 2. We will now determine the specific requirements of these solutions by industry. We look at this from three perspectives – partner, customer and the results delivered.



What Is the Information Provided?

- **Partner oriented:** Provides information on the technical outcomes anticipated within this industry and outlines the required functionalities to achieve them.
- **Customer oriented:** Communicates with the customer about achievable outcomes in plain language, providing appropriate context messaging.
- **Outcome oriented:** Communicates to the customer the results or outcomes they will gain after transitioning to your new solution.

Why Is This Information Important to Understand and Use?

To create a successful solution, it is essential to understand the primary priorities of the industry, as they are crucial for meeting customer needs. This step clarifies our solution's goals, allowing us to identify the necessary technical components in our next lesson.

Partner Oriented



What are top 10 security priorities faced by Government agencies in Australia. List the reason and requirement. Visualise in a table. Do not list numbers.



Top 10 Security Priorities for Government Agencies in Australia

Priority	Reason	Requirement
Data Protection	To safeguard sensitive information from unauthorised access and breaches.	Implement robust encryption and access control mechanisms.
Cyber Threat Intelligence	To stay ahead of emerging threats and vulnerabilities.	Utilise advanced threat detection and monitoring tools.
Network Security	To ensure the security and integrity of governmental communication networks.	Deploy firewalls, intrusion detection systems, and secure communication protocols.
Identity and Access Management	To control and monitor who can access critical systems and data.	Use multi-factor authentication and role-based access control.
Incident Response	To respond to security breaches and incidents quickly and effectively.	Establish a comprehensive incident response plan and team.
Compliance and Regulatory Requirements	To adhere to national and international security standards and regulations.	Regularly update policies and conduct compliance audits.
Supply Chain Security	To protect against vulnerabilities in the supply chain that can compromise security.	Implement stringent security measures for third-party vendors and suppliers.
Endpoint Security	To protect devices such as computers, smartphones, and tablets from threats.	Deploy antivirus software, endpoint detection, and response solutions.
Employee Training and Awareness	To ensure staff are aware of security best practices and potential threats.	Conduct regular cybersecurity training and awareness programs.
Cloud Security	To safeguard data and applications hosted in cloud environments.	Utilise secure cloud services and implement cloud security policies.

Customer Oriented



What are top 10 security priorities faced by Government agencies in Australia. List the reason and requirement. Deliver clearly and not using technical terms. Visualise in a table. Do not list numbers.



Top 10 Security Priorities for Government Agencies in Australia

Security Priority	Reason	Requirement
Protecting Devices	To safeguard devices such as computers, smartphones, and tablets from threats.	Deploy antivirus software, endpoint detection, and response solutions.
Employee Training and Awareness	To ensure staff are aware of security best practices and potential threats.	Conduct regular cybersecurity training and awareness programs.
Cloud Security	To safeguard data and applications hosted in cloud environments.	Utilise secure cloud services and implement cloud security policies.
Data Protection	To prevent unauthorised access to sensitive information.	Implement data encryption and access control measures.
Network Security	To protect internal networks from external threats.	Use firewalls and intrusion detection systems.
Identity Management	To ensure only authorised personnel can access certain systems.	Implement multi-factor authentication and role-based access controls.
Incident Response	To quickly address and mitigate security breaches.	Develop and regularly update incident response plans.
Supply Chain Security	To protect against vulnerabilities within the supply chain.	Conduct regular assessments and enforce supplier security standards.
Application Security	To prevent vulnerabilities within software applications.	Regularly assess and update applications to fix security gaps.
Physical Security	To protect facilities and physical assets from unauthorised access.	Implement access controls and surveillance systems in physical locations.

Outcome Oriented



What are top 10 security priorities faced by Government agencies in Australia. List the reason and security outcomes delivered. Deliver clearly and not using technical terms. Visualise in a table. Do not list numbers.



Top 10 Security Priorities for Government Agencies in Australia

Security Priority	Reason	Security Outcomes Delivered
Supply Chain Security	To safeguard against threats within the supply chain	Regular assessments and enforcement of supplier standards
Application Security	To prevent weaknesses in software applications	Regular testing and updates to fix vulnerabilities
Physical Security	To protect facilities from unauthorised access	Implementation of access controls and surveillance systems
Data Protection	To ensure the privacy and integrity of sensitive information	Encryption and strict data access policies
Network Security	To secure government networks from cyber threats	Firewalls and regular network monitoring
User Access Management	To control who can access government systems	Strong authentication methods and user role management
Incident Response	To be prepared for and respond to security breaches	Clear response plans and regular training exercises
Disaster Recovery	To ensure continuity of operations after a disaster	Backup systems and disaster recovery plans
Employee Training	To educate staff on security best practices	Regular training sessions and awareness programs
Policy and Compliance	To adhere to legal and regulatory requirements	Development and enforcement of security policies

Continue on your path to achieving a Microsoft Partner for Security designation.

Visit dickerdata.com.au/Microsoft or contact the Dicker Data Microsoft Team

(02) 8556 8061 Microsoft.Sales@DickerData.com.au