

SECURITY

Solutions Partner for Security Designation

FINANCE

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's 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 the finance industry in Australia. List the reason and requirement. Visualise in a table. Don't list numbers.



Top 10 Security Priorities in the Australian Finance Industry

Security Priority	Reason	Requirement
Data Breach Prevention	Confidential information can be exposed or stolen, leading to financial loss and reputational damage.	Implement robust encryption, access controls, and regular security audits.
Fraud Detection	Financial fraud can result in significant financial losses and legal implications.	Utilise advanced AI and machine learning algorithms to detect and prevent fraudulent activities.
Compliance with Regulations	Non-compliance can result in hefty fines and legal consequences.	Ensure adherence to local and international financial regulations through regular compliance checks.
Cybersecurity Training	Human error remains a significant vulnerability in cybersecurity defences.	Conduct regular training sessions to educate employees on the latest security practices.
Secure Online Transactions	Unauthorised access to online transactions can lead to fraud and financial losses.	Implement multi-factor authentication and secure transaction protocols.
Incident Response Planning	Quick response to security incidents can mitigate damage and reduce recovery time.	Develop and regularly update a comprehensive incident response plan.
Identity and Access Management	Uncontrolled access can lead to unauthorised data access and breaches.	Deploy robust identity verification and access management systems.
Endpoint Security	Endpoints are frequent targets for cyber-attacks.	Use advanced endpoint protection solutions to secure all devices.
Network Security	Network vulnerabilities can be exploited to gain unauthorised access to data.	Implement firewalls, intrusion detection systems, and regular network monitoring.
Data Backup and Recovery	Data loss can significantly disrupt operations and incur financial losses.	Establish regular data backup routines and a disaster recovery plan.

Customer Oriented



What are top 10 security priorities faced by the finance industry in Australia. List the reason and requirement. Deliver clearly and not using technical terms. Visualise in a table. Don't list numbers.



Top 10 Security Priorities in the Australian Finance Industry

Security Priority	Reason	Requirement
Data Breach Prevention	Confidential information can be exposed or stolen, leading to financial loss and reputational damage.	Employ advanced monitoring systems, strong encryption, and regular security audits.
Phishing Attack Mitigation	Fraudulent attempts to obtain sensitive information can compromise customer accounts and data.	Implement multi-factor authentication and conduct regular employee training on recognising phishing attempts.
Cloud Security	Data and applications hosted in the cloud are vulnerable to unauthorised access and breaches.	Use strong encryption, access controls, and perform regular security assessments.
Mobile Banking Security	The increased use of mobile devices for banking raises the risk of cyber-attacks.	Secure mobile banking apps and use multi-factor authentication.
Ransomware Protection	Ransomware attacks can lock systems and demand payment, causing financial and operational damage.	Back up data regularly and use advanced threat detection tools.
Insider Threats	Employees or insiders can misuse access to inflict harm on the organisation.	Monitor employee activities and implement access controls.
Third-Party Vendor Security	Vendors may introduce vulnerabilities if their security practices are inadequate.	Conduct thorough vetting and continuous monitoring of third-party vendors.
Regulatory Compliance	Failing to comply with regulations can result in penalties and legal issues.	Stay updated with regulatory changes and ensure all practices comply.
Fraud Detection and Prevention	Fraudulent activities can lead to significant financial losses.	Use advanced analytics and machine learning to detect and prevent fraud.
Network Security	Securing the network is crucial to prevent unauthorised access and cyber-attacks.	Employ firewalls, intrusion detection systems, and regular network monitoring.

Outcome Oriented



What are top 10 security priorities faced by the finance industry in Australia. List the reason and security outcomes delivered. Deliver clearly and not using technical terms. Visualise in a table. Don't list numbers.



Top 10 Security Priorities in the Australian Finance Industry

Security Priority	Reason	Security Outcome
Data Protection	Ensuring customer information is safe from breaches.	Enhanced privacy and customer trust.
Network Security	Preventing unauthorised access to the network.	Secured communication and data transfer.
Fraud Detection	Identifying and preventing fraudulent activities.	Reduced financial losses from fraud.
Access Control	Ensuring only authorised personnel have access to sensitive information.	Minimised risk of insider threats.
Cloud Security	Protecting data and applications hosted in the cloud.	Improved data availability and security in the cloud.
Incident Response	Quickly addressing and mitigating security incidents.	Reduced impact and recovery time from breaches.
Compliance	Adhering to regulations and industry standards.	Avoided penalties and maintained industry reputation.
Employee Training	Educating staff on security best practices.	Increased awareness and reduced human error.
Third-Party Risk Management	Ensuring partners and vendors meet security standards.	Reduced risk from external partnerships.
Endpoint Security	Protecting devices that connect to the network.	Secured endpoints and reduced malware infections.

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