GOOD SECURITY

Security Questionnaire Response Pack

Evidence-backed answers, domain structure, and explicit follow-up items where judgement is required.

CLIENT	QUESTIONNAIRE	PROFILE
Kiwi Manufacturing Ltd	Enterprise Security Review 2026	High scrutiny

RESPONSES	AVERAGE CONFIDENCE	MANUAL REVIEW
45	89%	2

RESPONSE PACK STANDARD

This example shows the fuller response pack used for enterprise procurement, regulated buyers, and detailed security due diligence. It includes domain-by-domain answer coverage, implementation notes, evidence references, and unresolved items for customer follow-up.

Executive summary

Kiwi Manufacturing Ltd is responding to Enterprise Security Review 2026 with 45 answered questions across 9 control domains. Average confidence is 89%, with 2 items flagged for human confirmation before final submission.

The pack is designed to let a buyer review the control story quickly while still giving the delivery team a traceable answer set, linked evidence, and explicit follow-up points.

Questionnaire scope and assumptions

Answers assume current production controls and documented practices as at the sample generation date. Where a question requires contractual confirmation, supplier evidence, or consultant judgement, the response is still surfaced with a clear manual-review note rather than being silently omitted.

Domain summaries

Domain	Questions	Approved	Manual review	Average confidence
Governance / Risk / Compliance	5	5	0	90%
Identity & Access Management	5	5	0	90%
Asset & Infrastructure Security	5	5	0	90%
Application & Interface Security	5	5	0	90%
Data Security & Information Lifecycle Management	5	5	0	90%
Threat & Vulnerability Management	5	4	1	84%
Incident Management / Resilience	5	5	0	90%
Third-Party / Supply Chain Security	5	5	0	90%
Human Resources / Awareness / Operational Controls	5	4	1	85%

Governance / Risk / Compliance

5 representative questions in this domain. 0 need human follow-up.

Question	Answer	Confidence	Review
Do you maintain a formal security governance cadence with leadership oversight?	Yes. Security posture, material risks, decisions, and action ownership are reviewed through monthly leadership reporting and a quarterly governance pack.	90%	Approved
How are security risks identified, rated, and tracked?	Risks are captured in a maintained register, scored using likelihood and impact, and linked to named owners and remediation actions.	90%	Approved
Do you align your control programme to recognised frameworks?	Yes. The current programme references ISO 27001:2022, NZISM, and the Privacy Act 2020, with cross-framework mapping used where buyers request equivalence.	90%	Approved
How do you track compliance obligations and customer-specific requirements?	Compliance milestones and customer obligations are tracked in dedicated registers so evidence, remediation, and review cadence can be managed explicitly.	90%	Approved
Is there an audit-ready evidence pack for key controls?	Yes. Key policy, register, reporting, and implementation evidence can be assembled into a reusable evidence pack rather than recreated per request.	90%	Approved

Identity & Access Management

5 representative questions in this domain. 0 need human follow-up.

Question	Answer	Confidence	Review
Do you enforce MFA for workforce and privileged access?	Yes. Workforce MFA is enforced through Entra ID Conditional Access, with stronger controls applied to privileged roles and external access scenarios.	90%	Approved
How is privileged access approved and reviewed?	Privileged access is approved through change control, limited to named roles, reviewed quarterly, and tracked separately for emergency access.	90%	Approved
How do you manage service accounts and non-human identities?	Service accounts are registered, linked to owners, and reviewed as part of privileged-access and application-control reviews.	90%	Approved
How are joiners, movers, and leavers handled operationally?	Workforce access changes are processed against a documented HR-linked workflow with same-day removal or role change verification.	90%	Approved
Do you support SSO for core enterprise applications?	Yes. Core business services are integrated with Entra ID SSO, with exceptions tracked and reviewed as part of the application inventory.	90%	Approved

Asset & Infrastructure Security

5 representative questions in this domain. 0 need human follow-up.

Question	Answer	Confidence	Review
Do you maintain an up-to-date inventory of systems and technology assets?	Yes. Managed assets, cloud services, and key OT-adjacent devices are tracked in the information asset register with owner and risk context.	90%	Approved
How do you apply secure baseline configuration to infrastructure and endpoints?	Baseline configurations are applied through Intune, cloud configuration standards, and managed firewall or platform settings, with exceptions tracked formally.	90%	Approved
How do you manage unsupported or legacy systems?	Legacy systems are risk-assessed separately, with compensating controls, visibility notes, and remediation timing documented in the reporting cadence.	90%	Approved
Do you monitor infrastructure health and security alerts centrally?	Yes. Core endpoint, identity, and network alerts are surfaced through managed monitoring and fed into the incident-management workflow.	90%	Approved
How do you manage patching and exposure windows for infrastructure components?	Critical patching follows defined remediation targets, with open exposure tracked and escalated when vendor or operational constraints delay remediation.	90%	Approved

Application & Interface Security

5 representative questions in this domain. 0 need human follow-up.

Question	Answer	Confidence	Review
Do you maintain an application inventory with owners and interface dependencies?	Yes. Core applications, owners, and major interface dependencies are maintained so security obligations can be tied back to the right business owner.	90%	Approved
How do you assess new application changes for security impact?	New material changes are reviewed through architecture and delivery governance, with security or privacy assessment triggered when the change affects data, integrations, or exposure.	90%	Approved
Are public-facing interfaces and APIs reviewed for access and data exposure risk?	Yes. Public-facing interfaces are reviewed for access control, authentication, and data exposure as part of change assurance and periodic testing.	90%	Approved
How do you control third-party integrations with customer or workforce data?	Third-party integrations are documented with owner, purpose, and data-flow context so access and disclosure implications can be reviewed before approval.	90%	Approved
Do you have a secure release or change process for material application changes?	Yes. Material releases follow change control, production approval, rollback planning, and post-change validation, with exceptions recorded for review.	90%	Approved

Data Security & Information Lifecycle Management

5 representative questions in this domain. 0 need human follow-up.

Question	Answer	Confidence	Review
How do you classify and protect sensitive information?	Sensitive information is covered by a documented classification model and applied controls for access, retention, and sharing restrictions.	90%	Approved
Do you maintain a personal data inventory and retention schedule?	Yes. Core data holdings, retention periods, storage locations, and cross-border considerations are maintained in a dedicated inventory.	90%	Approved
How do you manage cross-border disclosure and privacy risk for cloud services?	Cross-border processing is recorded in the data inventory and reviewed through privacy assessment before new disclosures or vendor arrangements are approved.	90%	Approved
Do you use technical controls to reduce accidental or unauthorised disclosure?	Yes. Core collaboration platforms use DLP, access controls, and sharing restrictions for personal and financially sensitive information.	90%	Approved
How do you evidence data lifecycle management to customers or auditors?	Retention, disclosure, and evidence controls are supported through the data inventory, privacy assessments, and linked policy set rather than ad hoc statements.	90%	Approved

Threat & Vulnerability Management

5 representative questions in this domain. 1 need human follow-up.

Question	Answer	Confidence	Review
How do you identify vulnerabilities across infrastructure and applications?	Exposure is identified through vendor intelligence, platform telemetry, and scheduled review points, then prioritised through the risk and reporting cadence.	90%	Approved
How are critical vulnerabilities remediated or risk-accepted?	Critical issues are assigned named owners, remediation windows, and escalation routes. Where remediation is delayed, compensating controls and risk acceptance are documented.	90%	Approved
Do you commission independent security testing?	Independent testing is part of the annual assurance plan, but the precise 2026 statement still requires consultant confirmation before it would be submitted externally.	58%	Manual review
How do you communicate vulnerability posture to leadership?	Exposure and remediation movement are surfaced through monthly posture reporting and quarterly leadership scorecards, with priority issues highlighted for decision-makers.	90%	Approved
How do you treat supplier-driven vulnerability risk?	Supplier dependencies and delayed third-party fixes are tracked as part of vendor and customer requirements governance rather than treated as isolated IT issues.	90%	Approved

Incident Management / Resilience

5 representative questions in this domain. 0 need human follow-up.

Question	Answer	Confidence	Review
Do you maintain a documented incident response process?	Yes. The organisation maintains incident response, breach-notification, and communications playbooks with role-based actions for containment, escalation, and recovery.	90%	Approved
How are security events escalated and triaged?	Alerts are triaged through managed monitoring and service desk escalation paths, with documented severity thresholds and decision points for external escalation.	90%	Approved
Do you exercise response and continuity scenarios?	Exercises are planned through the annual assurance schedule, and the resulting actions are tracked into the improvement backlog and leadership reporting cycle.	90%	Approved
How do you manage privacy breach notification obligations?	Privacy breach readiness is aligned to the incident workflow, with notification and decision steps tied to named leadership and privacy roles.	90%	Approved
Are recovery dependencies and resilience assumptions visible to leadership?	Yes. Recovery assumptions, critical dependencies, and open resilience gaps are surfaced in the quarterly reporting cadence and supporting evidence pack.	90%	Approved

Third-Party / Supply Chain Security

5 representative questions in this domain. 0 need human follow-up.

Question	Answer	Confidence	Review
Do you maintain a vendor risk process for critical suppliers?	Yes. Critical suppliers are assessed using a documented vendor risk process with tiering, evidence tracking, and remediation follow-up.	90%	Approved
How do you track customer-imposed security requirements?	Customer requirements are consolidated into one register so obligations, coverage, and evidence gaps can be managed commercially rather than reactively.	90%	Approved
Are supplier access and security obligations reviewed during contract changes or renewals?	Yes. Renewal reviews include access, data handling, and assurance obligations so supplier risk posture stays aligned to current business use.	90%	Approved
How do you manage third-party processing of personal information?	Third-party processing arrangements are documented in the privacy inventory and reviewed for disclosure, retention, and contractual safeguards.	90%	Approved
Do you monitor supplier non-compliance or drift over time?	Yes. Supplier or requirement drift is surfaced through vendor and customer requirement registers so actions can be tracked before they turn into audit findings or renewal blockers.	90%	Approved

Human Resources / Awareness / Operational Controls

5 representative questions in this domain. 1 need human follow-up.

Question	Answer	Confidence	Review
Do staff complete security awareness training on an ongoing basis?	Yes. Security awareness training follows a planned cadence with phishing testing, leadership reporting, and tracking of completion and click rates.	90%	Approved
How are role-based security responsibilities communicated?	Role-based responsibilities are set through policy, operational procedures, and leadership reporting so IT, privacy, and business owners understand their specific obligations.	90%	Approved
Do you screen or verify staff in line with role sensitivity?	Staff screening follows normal HR controls, but the exact role-based screening statement should still be confirmed against the latest HR policy before external submission.	63%	Manual review
How do you ensure operational processes remain current?	Core procedures and evidence artefacts are reviewed through scheduled ownership and lifecycle controls rather than being left to ad hoc updates.	90%	Approved
How are security findings turned into owned actions?	Security findings are converted into named actions with owners, timing, and success measures, then tracked through the monthly and quarterly operating cadence.	90%	Approved

Implementation notes / shared-responsibility clarifications

Question	Implementation note / shared responsibility
Do you commission independent security testing?	Customer-facing answer must be aligned to the final 2026 testing scope.
Do you screen or verify staff in line with role sensitivity?	HR screening language must be confirmed before submission.

Evidence references appendix

Question	Evidence references
Do you maintain a formal security governance cadence with leadership oversight?	Board Advisory Reporting Pack - Q1 2026, Security Governance Calendar 2026
How are security risks identified, rated, and tracked?	Risk Register - March 2026, Risk Management Standard v1.6
Do you align your control programme to recognised frameworks?	Cross-Framework Control Mapping, Security Baseline Assessment
How do you track compliance obligations and customer-specific requirements?	Customer Requirements Register, Compliance Timeline - Q1 2026
Is there an audit-ready evidence pack for key controls?	Audit Readiness Score Snapshot, Evidence Pack Index
Do you enforce MFA for workforce and privileged access?	Access Management Policy v2.3, Conditional Access Standard v1.8
How is privileged access approved and reviewed?	Privileged Access Procedure v1.6, Quarterly Access Review Record - Q1 2026
How do you manage service accounts and non-human identities?	Identity Register - Service Accounts, Application Ownership Matrix
How are joiners, movers, and leavers handled operationally?	Workforce Access Governance Standard v1.4, HR Offboarding Checklist v3.1
Do you support SSO for core enterprise applications?	Identity Architecture Overview 2026, Entra Application Register
Do you maintain an up-to-date inventory of systems and technology assets?	Information Asset Register - March 2026, Technology Ownership Matrix
How do you apply secure baseline configuration to infrastructure and endpoints?	Endpoint Baseline Standard v1.9, Cloud Configuration Standard v1.4
How do you manage unsupported or legacy systems?	Legacy Device Exception Log, Quarterly Security Scorecard - Q1 2026
Do you monitor infrastructure health and security alerts centrally?	Monitoring and Escalation Matrix, Managed Detection Service Overview

Question	Evidence references
How do you manage patching and exposure windows for infrastructure components?	Vulnerability Management Procedure v1.5, Monthly Security Posture Report - February 2026
Do you maintain an application inventory with owners and interface dependencies?	Application Ownership Matrix, Integration Register
How do you assess new application changes for security impact?	Change Governance Standard v1.2, Privacy Impact Assessment - ERP Migration
Are public-facing interfaces and APIs reviewed for access and data exposure risk?	Interface Security Standard v1.1, Annual Assurance Plan 2026
How do you control third-party integrations with customer or workforce data?	Data Flow Register, Third-Party Integration Review Checklist
Do you have a secure release or change process for material application changes?	Change Governance Standard v1.2, Release Assurance Checklist
How do you classify and protect sensitive information?	Information Classification Standard v1.3, Microsoft 365 Protection Configuration
Do you maintain a personal data inventory and retention schedule?	Personal Data Inventory - March 2026, Retention Schedule v1.2
How do you manage cross-border disclosure and privacy risk for cloud services?	Privacy Impact Assessment - ERP Migration, Cross-Border Transfer Register
Do you use technical controls to reduce accidental or unauthorised disclosure?	Data Protection Standard v1.4, M365 DLP Policy Set
How do you evidence data lifecycle management to customers or auditors?	Personal Data Inventory - March 2026, Policy Suite Lifecycle Management
How do you identify vulnerabilities across infrastructure and applications?	Vulnerability Management Procedure v1.5, Monthly Security Posture Report - February 2026
How are critical vulnerabilities remediated or risk-accepted?	Risk Register - March 2026, Remediation Tracking Board
Do you commission independent security testing?	Annual Assurance Plan 2026
How do you communicate vulnerability posture to leadership?	Monthly Security Posture Report - February 2026, Quarterly Security Scorecard - Q1 2026
How do you treat supplier-driven vulnerability risk?	Vendor Risk Register, Customer Requirements Register
Do you maintain a documented incident response process?	Incident Response Playbook Suite v2.1, Privacy Breach Readiness Review
How are security events escalated and triaged?	Monitoring and Escalation Matrix, Incident Severity Matrix

Question	Evidence references
Do you exercise response and continuity scenarios?	Annual Assurance Plan 2026, Exercise Improvement Register
How do you manage privacy breach notification obligations?	Privacy Breach Readiness Review, Privacy Incident Notification Workflow
Are recovery dependencies and resilience assumptions visible to leadership?	Board Advisory Reporting Pack - Q1 2026, Recovery Dependency Register
Do you maintain a vendor risk process for critical suppliers?	Vendor Risk Register, Vendor Risk Management Standard v1.3
How do you track customer-imposed security requirements?	Customer Requirements Register, Commercial Assurance Review - March 2026
Are supplier access and security obligations reviewed during contract changes or renewals?	Vendor Renewal Review Checklist, Vendor Risk Register
How do you manage third-party processing of personal information?	Personal Data Inventory - March 2026, Cross-Border Transfer Register
Do you monitor supplier non-compliance or drift over time?	Vendor Risk Register, Customer Requirements Register
Do staff complete security awareness training on an ongoing basis?	Security Awareness Programme Plan, Awareness Metrics Dashboard
How are role-based security responsibilities communicated?	Security Roles and Responsibilities Matrix, Policy Suite Lifecycle Management
Do you screen or verify staff in line with role sensitivity?	People Risk Management Standard
How do you ensure operational processes remain current?	Policy Suite Lifecycle Management, Operational Control Review Calendar
How are security findings turned into owned actions?	Quarterly Security Scorecard - Q1 2026, Remediation Tracking Board

Manual-review / unresolved items

Question	Why it needs confirmation	Follow-up
Do you commission independent security testing?	Confirm the final 2026 penetration-testing scope and provider statement.	Customer-facing answer must be aligned to the final 2026 testing scope.
Do you screen or verify staff in line with role sensitivity?	Confirm the current role-based screening statement against the live HR policy.	HR screening language must be confirmed before submission.