ICT Professional Services — Use Cases

Effective Sep 2025

Executive summary

Virtus Group Professional Services help agencies set direction, reduce risk, and land change. We design and embed information security governance, strategy, and risk management that's pragmatic, NZ-centric, and audit-ready. Our work aligns to PSR/NZISM and recognised international frameworks (ISO 27001/27005, NIST CSF), with NZ as the primary residency (AU permitted for elected DR). We prioritise clarity, evidence, and reuse—policies, patterns, and runbooks you can keep operating after we're gone.

Evidence	Policies (client-safe), Assurance Index, MS & CPS Evidence Packs, Capability Statement, Pricing Annex, PCBU H&S, Privacy Summary.
Residency	NZ primary; AU permitted for DR if elected.
Contacts	hello@virtusgroup.biz • privacy@virtusgroup.biz • 0800 847 887

What we deliver

- Governance & strategy: policy/standards suites, Statements of Applicability, roadmaps, KPIs, and assurance calendars
- Risk management: business-focused risk & privacy impact assessments, threat modelling, treatment plans, and executive reporting
- Reference architecture & patterns: identity/MFA/admin tiering, endpoint/M365 hygiene, secure email (SPF/DKIM/DMARC, MTA-STS/TLS-RPT), network segmentation/Zero Trust
- vCISO services: board/ELT engagement, risk acceptance governance, supplier diligence, and cadence management
- Enablement: workshops, templates, and training that embed capability in your team

How we engage

- Outcome-based scopes: success measures and decision checkpoints agreed up front
- Tool-agnostic delivery: we fit your GRC/ticketing/office stack; evidence packs provided
- Change management: stakeholder mapping, comms/training, and adoption plans to land controls with minimal friction
- Residency: NZ primary; AU permitted for DR when elected
- Boundaries: we do advisory/readiness (e.g., ISO/PCI preparation). Formal certifications (QSA/ISO audits) and court-defensible forensics are delivered via accredited partners under our leadership if requested.

Assurance & governance

- Policies and artefacts mapped to PSR/NZISM and exportable to ISO/NIST views
- Two-person reviews, RACI, and change control on key deliverables
- Monthly progress/KPI packs; risk dashboards; acceptance records
- Classified handling
- Work is UNCLASSIFIED/OFFICIAL by default. Where CONFIDENTIAL access is essential, we engage cleared partner personnel for those touchpoints; our core team remains on unclassified artefacts with segregation of duties and full logging.

Outcomes

- A maintainable governance stack, a living risk register with owners and due dates, measurable posture uplift, and audit-ready evidence that stands up to scrutiny.

Start with a governance/risk health check or a 10-day Risk & PIA sprint to unblock your next decision.

Use Case 1 — Incident Response uplift (Microsoft 365 + BCDR)

Requirements

- Named Incident Manager and contact tree; existing IR artefacts (if any).
- Change window in M365; access to security portals (Defender/EOP/Entra) with appropriate roles.
- Agreement on SLA targets and escalation paths; vendor/carrier contacts where relevant.

Aligned to our Incident Response Summary (client-safe).

Deliverables

- IR Plan with severity matrix and RACI; evidence-handling guide; comms templates; PIR template.
- M365 runbooks: Defender/EOP purge, ZAP, OAuth revoke; Conditional Access recovery; break-glass process.
- BCDR summary with restore test cadence and go/no-go checklist; illustration of IR lifecycle.

Outcome

- Complete IR Plan with playbooks (ransomware/exfil, BEC/payment fraud, OAuth/token abuse, oversharing).
- M365 micro-runbooks (purge/ZAP, revoke OAuth, break-glass), decision aids for DR go/no-go.

Use Case 2 — Secure M365 tenant baseline & data protection

Requirements

- Global Admin time-box or change window; Entra/Exchange/SharePoint admin roles as needed.
- Tenant inventory (domains, licences, third-party senders, integrations).
- Licensing availability (e.g., Entra P1/P2, Defender, Purview features) or acceptance of alternatives.

Deliverables

- Baseline configuration with exception register and rollback plan.
- KQL queries and Defender reports for verification; external sharing recall process.
- Acceptance checklist and training handouts for administrators.

Outcome

- Tenant governance with Conditional Access, strong MFA, break-glass, DLP/ labels.
- External sharing controls for SharePoint/OneDrive; cleanup of malicious inbox rules and risky OAuth consents.

Use Case 3 — Infrastructure resilience & backup/DR modernisation

Requirements

- Inventory of systems, tiers and recovery objectives; access to backup platforms and repositories.
- Test windows for restore exercises (non-prod where possible); provider contacts for cloud/SaaS backups.
- Agreement on change freeze/rollback criteria during tests.

Deliverables

- Backup/restore runbook; test reports with evidence; golden-config checklist for network/security devices.
- Monitoring & alerting handover; retention/telemetry plan; weekly status cadence with RAID & decision logs.

Outcome

- Backups hardened with immutability; restore tests recorded with achieved RTO/RPO.
- Patch/endpoint baselines; monitoring with retention and alerting.

Use Case 4 — Programme/Project Management (PMO-lite)

Requirements

- Executive sponsor and product owner(s); access to roadmap/backlog and tooling (e.g., DevOps/Jira).
- Decision authority matrix (RACI) agreed; cadence for status and steering.
- Defined artefact repository and document standard for the programme.

Deliverables

- Stage-gated plan with acceptance criteria; weekly Status + RAID + Decision Log set.
- Change Requests with impact analysis and approvals; close-out with acceptance certificates and lessons learned.

Outcome

- Transparent stage-gates, RAID/decision logs, controlled change, benefits tracking.
- Assurance of auditable outcomes and predictable delivery.

Use Case 5 — Secure Email Authentication & DMARC Enforcement

Requirements

- Registrar/DNS access; list of all domains and third-party senders (marketing, finance, ticketing, etc.).
- Mail flow diagram and change window; mailbox for RUA/RUF reports.
- Agreement on staged policy (none→quarantine→reject) and exception handling.

Public artefacts: Insurance Summary, System Security Policy; deeper configs on request.

Deliverables

- Domain/sender inventory; DNS records; enforcement plan with milestones and rollback.
- DMARC analytics (RUA/RUF) summary; exception workflow; executive metrics pack.
- Connector hardening; VIP/mailbox protections; staff comms templates.

Outcome

- Spoofing risk reduced via SPF/DKIM validation and staged DMARC enforcement (none → quarantine → reject).
- Transport security uplift with MTA-STS and TLS-RPT; partner onboarding without mail disruption.

Use Case 6 — Zero Trust Remote Access / ZTNA

Requirements

- Application inventory and identity provider details; device management posture (Intune/MDM) for compliance signals.
- Pilot user cohort and test apps; change window for access policy rollout.
- Network path assumptions (public/private) confirmed, with fallbacks for legacy apps.

Deliverables

- Access patterns & segmentation plan; Conditional Access policies; device compliance requirements.
- Pilot rollout with rollback; admin runbook; executive summary of risk reduction.
- Metrics: adoption, failed auths, policy hits; exceptions register.

Outcome

- Legacy VPN risk reduced; least-privilege, identity-aware access to apps with CA/MFA.

- Improved user experience with per-app access; auditability of access decisions.

Use Case 7 — Vulnerability Management & Patch Cadence Uplift

Requirements

- Access to scanner data or tooling (or agreement to deploy); patch tooling access.
- Maintenance windows by system tier; risk thresholds and SLAs agreed.
- Stakeholders: owners for servers, endpoints, network devices; CAB cadence confirmed.

Deliverables

- VM process definition; severity thresholds; change governance and rollback.
- Ring strategy; monthly compliance reports; exceptions with time-bound approvals.
- Dashboard: exposure over time; SLA performance; PIRs for failed patches.

Outcome

- Predictable patch windows and emergency paths for critical CVEs.
- Measurable reduction of high/critical backlog; improved compliance across OS and key apps.

Use Case 8 — Service Transition & Handover (Managed → Agency)

Requirements

- Current SOPs and inventories (CMDB/export); credential/access matrix for accounts and tools.
- Contract/licence lists and vendor contacts; acceptance criteria for handover.
- Agreed ‘warranty’ period and support boundaries post-handover.

Deliverables

- Handover kit: runbooks, access matrix, inventory, licences, vendor contacts.
- Knowledge transfer sessions; acceptance tests; warranty support window.
- Exit plan with data/keys handback; account deprovision checklist.

Outcome

- Clean transition with documented SOPs, RACI, and evidence trails.

- Agency autonomy increased without service disruption.

Use Case 9 — Network Segmentation & Identity-Aware Microsegmentation

Requirements

- Current network diagrams and firewall inventories; access to policy management tools.
- Directory groups and identity posture available; test/lab segment for pilot.
- Change windows coordinated with owners; rollback and monitoring agreed.

Deliverables

- Target state diagram; firewall/policy templates; identity group design.
- Pilot in a low-risk segment; rollback plan; packet-capture validation scripts.
- Runbook for change and monitoring; metrics for blocked/allowed flows.

Outcome

- Reduced lateral movement via zone/segment design tied to identity and device posture.
- Clarity on east–west policy and privileged access boundaries.

Use Case 10 — SaaS Intake Governance & Onboarding

Requirements

- Authority to standardise the intake; procurement/legal contact; vendor security documents (CAIQ/SoC2 or equivalent).
- SSO/MFA capability with IdP details; data residency requirements confirmed.
- Pilot service identified; logging/monitoring endpoints accessible.

Deliverables

- Intake form & checklist (data categories, residency, sub-processors, auth).
- 10-day risk & PIA sprint outputs; baseline controls (SSO/MFA, DLP/labels, logging).
- Go-live conditions; review cadence; deprovision/exit criteria.

Outcome

- Faster, safer SaaS adoption with consistent intake, risk & privacy checks, and controls.
- Reduced shadow IT and predictable data handling/residency posture.

Use Case 11 — Managed Cloud — Azure Landing Zone Ops & Compliance

Requirements

- Access to Azure tenant with delegated permissions; list of subscriptions/ management groups; policy/compliance targets (PSR/NZISM/ISO).
- Change windows; contact list for platform owners; baseline billing/export for tagging policy.

Deliverables

- Runbook for provisioning (subscriptions, RBAC, PIM/JIT, key vaults, logging).
- Azure Policy & Defender baselines; cost-management tags; management group structure; blueprint-as-code.
- Monthly posture report (compliance drift, identity risk, public exposure, cost anomalies).

Outcomes

- Hardened, repeatable landing zone operations with RBAC/PIM and guardrails.
- Measured improvement in compliance scores and reduction in public exposure findings.
- Tagging coverage and spend visibility improved; predictable provisioning SLAs.

Use Case 12 — Managed Cloud — FinOps & Budget Guardrails

Requirements

- Read-only access to billing exports/Cost Management; tagging policy; business unit/service owner map.
- Approval to set budgets/alerts and apply right-sizing recommendations in non-prod first.

Deliverables

- Budgets and alerts per BU/environment; anomaly detection playbook; rightsizing recommendations and change tickets.
- Monthly cost & utilisation report (unit economics, RI/Savings Plan coverage, idle/orphaned resources).
- Tag compliance dashboard and remediation plan.

Outcomes

- 5–15% cloud cost reduction within 90 days without impacting SLAs.

- Improved tag hygiene enabling showback/chargeback and better forecasting.
- Fewer surprise bills via budget guardrails and anomaly response.

Use Case 13 — Managed Network — SD-WAN Service (Design, Cutover & Ops)

Requirements

- Inventory of sites/links/providers; target QoS and critical apps; access to SD-WAN orchestrator or approval to deploy.
- Change windows for pilot and staged cutover; escalation contacts with carriers.

Deliverables

- Low-risk pilot with success criteria; SD-WAN policies (business intent, QoS, DIA/MPLS usage, failover).
- Cutover runbook and rollback plans; monitoring & alerting integrations; monthly performance report (jitter/latency/loss, uptime).
- SOPs for incident handling and carrier escalation; config backup/versioning.

Outcomes

- Higher availability and performance for critical apps; reduced failover times.
- Carrier dependency risk lowered; visibility into per-site health and usage.
- Documented, repeatable ops model with measurable SLAs.

Use Case 14 — Managed Network — Wireless LAN Lifecycle & Assurance

Requirements

- Floor plans and site survey inputs; controller/orchestrator access; device identity (802.1X/guest) requirements.
- Change windows for AP/channel changes; agreed RF policy (channels, power, coverage).

Deliverables

- Predictive & on-site surveys; SSID design (corp/guest/IoT) with NAC; RF policy and channel plans.
- Security baselines (WPA3/802.1X), guest onboarding; monthly WLAN health report (coverage, retries, airtime, client experience).
- Incident SOPs for interference/rogue APs; firmware lifecycle and staged

upgrades.

Outcomes

- Better user experience and fewer dropouts; measurable improvements in coverage and client success rate.
- Stronger WLAN security posture; predictable maintenance windows.
- Clear metrics for capacity planning and troubleshooting.

Use Case 15 — Managed Infrastructure — Server Patching & Compliance as a Service

Requirements

- Asset inventory with tiers/maintenance windows; endpoint mgmt tooling access (WSUS/SCCM/Intune/Linux repo).
- Risk thresholds/SLA; rollback criteria; contact list for app owners.

Deliverables

- Monthly patch plan per tier; emergency path for critical CVEs; ring strategy and pilot groups.
- Compliance dashboard; exceptions with expiry; PIRs for failed updates; audit-ready evidence exports.
- Quarterly patch efficacy review and optimisation recommendations.

Outcomes

- Reduced high/critical exposure and predictable compliance levels.
- Lower unplanned downtime through ringed deployments and defined rollback.
- Auditable trail suitable for assurance reviews.

Use Case 16 — Managed Infrastructure — Monitoring, Alerting & SRE-lite

Requirements

- Access to monitoring platform/APIs or approval to deploy agents; list of services/SLIs/KPIs; on-call escalation paths.
- Thresholds and maintenance windows agreed; log retention requirements.

Deliverables

- Unified dashboards (availability, latency, saturation, errors); alert policy tuning to reduce noise.

- Runbooks for top incident classes; weekly ops review; post-incident review templates and action tracking.
- Quarterly capacity & reliability report with recommendations (SLOs/SLA alignment).

Outcomes

- Improved MTTD/MTTR and fewer false alarms; clearer ownership and runbooks.
- Trend-based capacity planning; fewer repeat incidents via PIR actions.
- Visibility that supports governance and vendor management.

Document control

Version / date	v1.3 / 29 Sep 2025
Owner	Principal (ICT Professional Services)
Domain	Public