Cybersecurity & PDPA Training Readiness Checklist

This high-level, non-exhaustive checklist helps organisations do an initial sense-check of their readiness to design, deliver, and sustain an effective Cybersecurity and PDPA (Personal Data Protection Act) training and awareness program.

Use this as a starting point to identify potential gaps. It is intended as a practical guide and does not replace legal or professional advice.

1. Governance & Objectives

☐ Training objectives for cybersecurity and PDPA are documented and aligned to organisational risk and compliance needs.

☐ Responsibility for the training programme is clearly assigned (e.g. DPO, HR, L&D, Information Security).

☐ A written policy or guideline exists that sets expectations for mandatory training and refresher frequency.

☐ Management supports and endorses the programme (e.g. through opening remarks, internal communications, participation).

☐ Training scope covers all relevant business units, locations, and staff categories (including contractors where applicable).

2. Audience, Roles & Risk Profile

☐ Different staff groups and roles are identified (e.g. management, HR, IT, frontline, back-office, vendors).

☐ Role-based training needs are defined (e.g. DPO and data handlers receive deeper PDPA content).

☐ High-risk roles (e.g. system admins, customer-facing staff, data analysts) are prioritised for enhanced training.

☐ Training content reflects the organisation’s actual systems, processes, and types of personal data handled.

☐ New joiners, temporary staff, and interns are included in the training plan.

3. Training Content – Cybersecurity

☐ Core cybersecurity concepts are covered (e.g. passwords, phishing, malware, social engineering, safe browsing).

☐ Realistic examples or case studies are used (e.g. phishing emails, business email compromise, ransomware).

☐ Guidance is provided on secure use of company devices, remote work, and mobile/portable storage.

☐ Staff are trained on reporting suspicious emails, messages, or activities through a clear reporting channel.

☐ Content includes organisation-specific security policies and procedures (e.g. acceptable use, incident reporting).

☐ Specific modules exist for IT and technical staff (e.g. patching, access control, logging, backup, monitoring).

4. Training Content – PDPA & Data Protection

☐ PDPA principles and obligations are introduced in clear, non-legal language.

☐ Staff understand what constitutes personal data and sensitive personal data in the organisation’s context.

☐ The data lifecycle is explained (collection, use, disclosure, storage, retention, disposal).

☐ Training covers consent, notification, purpose limitation, and access/correction rights.

☐ Data breach and incident response obligations are explained (including when and how to escalate).

☐ Role-specific PDPA training is provided for HR, marketing, customer service, and others who handle personal data frequently.

☐ Staff are shown practical examples of correct and incorrect data-handling behaviours (e.g. email, printing, file sharing).

5. Delivery Methods & Learning Design

☐ A blended approach is used where possible (e.g. live sessions, e-learning modules, videos, micro-learning).

☐ Training materials are engaging and accessible (e.g. scenarios, quizzes, polls, discussion, role play).

☐ Content is adapted to different levels of digital literacy among staff.

☐ Key messages are summarised in simple takeaways or job aids (e.g. one-page guides, posters, intranet pages).

☐ Refresher training frequency is defined (e.g. annually, plus ad-hoc refreshers after major incidents or changes).

6. Records, Tracking & Measurement

☐ A system exists to track attendance and completion (e.g. LMS, HR system, training register).

☐ Completion reports can be generated by department, role, or location for management review.

☐ Knowledge checks or quizzes are used to test understanding of key concepts.

☐ Training effectiveness is evaluated (e.g. feedback forms, surveys, follow-up interviews).

☐ Key metrics are monitored (e.g. completion rate, quiz scores, phishing simulation results, incident trends).

7. Integration with Policies, Processes & Culture

☐ Training content is consistent with current policies, procedures, and guidelines (e.g. data protection policy, IT security policy).

☐ Staff know where to find relevant policies, FAQs, and contact points for questions (e.g. DPO contact).

☐ Cybersecurity and PDPA messages are reinforced through ongoing communications (e.g. newsletters, posters, townhalls).

☐ Lessons from incidents, audits, or near-misses are incorporated into future training content.

☐ Management and supervisors model expected behaviours (e.g. locking screens, careful data sharing, reporting incidents).

8. Onboarding, Refresher & Trigger-Based Training

☐ Cybersecurity and PDPA training is included in the new-joiner onboarding process.

☐ Periodic refresher training is conducted (e.g. annually) and scheduled in advance.

☐ Additional training is triggered by key events (e.g. new system rollout, policy changes, significant data breach).

☐ Specialised training is provided for project teams handling new initiatives involving personal data.

☐ Records show that staff who change roles receive updated, role-specific training where needed.

9. External Trainers, Vendors & Materials (if applicable)

☐ Selection criteria exist for external training providers (e.g. subject matter expertise, sector relevance).

☐ Training content from external providers is reviewed and tailored to the organisation’s context before delivery.

☐ Vendor contracts or agreements address confidentiality and proper handling of any staff or customer data used in training.

☐ Feedback on external training is collected and reviewed before renewal or repeat engagement.

☐ Ownership and rights to training materials are clear (e.g. reuse, adaptation, branding).

10. Continuous Improvement

☐ Training content is periodically reviewed for accuracy, relevance, and alignment with current threats and regulations.

☐ Updates in laws, regulations, or industry guidelines (e.g. PDPC guidance, sectoral rules) are reflected in training materials.

☐ Feedback from staff and management is used to refine delivery methods and topics.

☐ The organisation periodically benchmarks or compares its training practices against peers or best practices.

☐ Cybersecurity and PDPA training is recognised as part of the organisation's broader culture and risk management approach, not a one-off exercise.

For assistance, contact:

Hari Krishnan, Managing Director
Apex Organisational Solutions | www.apexorganisationalsolutions.com | hari.krishnan@apexorganisationalsolutions.com