



LEGAL
PRACTITIONERS'
LIABILITY
COMMITTEE

CYBERSECURITY STANDARDS AND IMPLEMENTATION GUIDE

lplc.com.au



Cybersecurity is a core component of running a legal practice. With law firms handling large sums of money and highly sensitive client information, the legal profession is an attractive target for cybercriminals. Even a single incident can have devastating financial, reputational, and regulatory consequences.

To fight against cybercriminals, it is essential that all law practices, regardless of size, implement a cybersecurity strategy that is practical, scalable, and aligned with both professional obligations and industry standards.

This guide has been developed by the LPLC to support law firms in building cybersecurity practices that are appropriate to their firm. It recognises that while cybersecurity may appear technical or costly, effective cyber risk mitigation is achievable through a structured, staged approach.

Overview of cybersecurity standards

There is no single cybersecurity standard that fits all law firms and a firm's cybersecurity requirements can change over time. While there are multiple cybersecurity frameworks that law practices can choose to adhere to, the VLSB+C Minimum Cybersecurity Expectations, the LPLC Recommendations, and the Dynamic Standards International (DSI) SMB1001, are most appropriate for small to medium-sized law practices. From meeting basic professional obligations to achieving industry-aligned cyber maturity, these frameworks offer strong alignment with the needs cybersecurity requirements of law firms.

(Note: Large law practices generally have robust cybersecurity strategies that adhere to higher-level international cybersecurity standards such as ISO, ASD, and NIST Cybersecurity Framework. These standards are not considered in this guide as they require a comprehensive strategy for implementation and maintenance.)

This section provides a comparative overview of three key standards relevant to legal practices:

- VLSB+C Minimum Cybersecurity Expectations
- LPLC Recommendations
- DSI SMB 1001 (Platinum)

Each framework provides an appropriate approach to legal practice cybersecurity in terms of sophistication, control coverage, and resilience against modern cyber threats.

1. VLSB+C minimum cybersecurity expectations

The **Victorian Legal Services Board (VLSB+C)** has set out the minimum cybersecurity requirements that every Victorian law firm must implement. These expectations are not optional — failure to comply can result in disciplinary action against the principals of a law practice. The expectations focus on basic but essential cybersecurity controls that serve as a starting point for a firm’s cybersecurity journey.

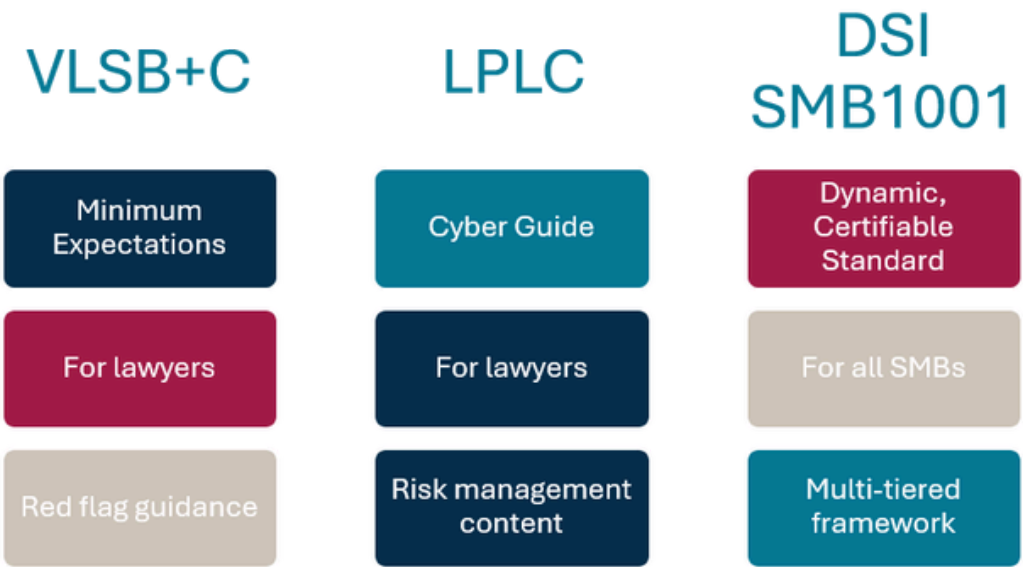
2. LPLC recommendations

Building on the foundations of the VLSB+C' minimum expectations, the Legal Practitioners’ Liability Committee (LPLC) has developed enhanced cybersecurity recommendations tailored to the needs of legal practices. These recommendations focus on improving cybersecurity controls and are informed by claims data and industry trends.

3. DSI SMB 1001

The Dynamic Standards International (DSI) SMB 1001 is a multi-level cybersecurity standard created for small and medium-sized businesses. It provides a broader, industry-based control set that is certifiable through authorised Technical Support Specialists. Being multi-tiered, the standard provides a pathway for law firms to progressively implement cybersecurity controls.

The diagram below provides a side-by-side comparison of these standards, highlighting areas of alignment and progression.



Develop and implement your cybersecurity strategy

Transitioning from understanding cybersecurity standards to implementing an effective strategy requires a structured, methodical approach tailored to your legal practice's specific needs and resources.

Developing your cybersecurity strategy is not simply about selecting controls from a checklist. It requires an appropriate assessment of your firm's unique risk profile, regulatory obligations, and operational constraints. This section provides a nine-step roadmap designed to guide law practices through the strategic planning and implementation process. The approach emphasises the importance of professional guidance while empowering legal practices to make informed decisions about their cybersecurity investments and priorities.

Implementing cybersecurity controls

- 1. Understand your legal obligations and current position:** You must know what you are protecting.
- 2. Find a cybersecurity consultant:** Cybersecurity should be done by a professional.
- 3. Assess your risk:** Each firm and IT setup may have its own unique issues. Operators must understand the risk that they are facing.
- 4. Review your budget:** A cybersecurity strategy should not be seen as a sunk cost but rather an investment in your firm's and client's security. Don't try and do it on the cheap. There are strategies and experts to suit your firm. The key concept is 'proportionality'.
- 5. Choose your standard:** A standard should be chosen that fits your risk profile and budget.
- 6. Implement your controls:** The implementation of cybersecurity controls can be complicated and may require a cybersecurity consultant to execute.
- 7. Monitor your technology:** As your technology set-up changes, so do your risks.
- 8. Stay current with evolving scams and attacks:** Cybercriminals are constantly coming up with new ways to breach your cybersecurity defences.
- 9. Review your controls regularly:** In a world that changes rapidly, law practices must regularly review their cybersecurity strategy to ensure that it still offers the most appropriate protection.

Once you have chosen your standard and controls – you need your own cyber plan. This outlines your controls, who's responsible for what aspect of the plan, and what is to be done to maintain and improve each control.

Step 1: Understand your legal obligations and current position

Law practices need to understand their technology and data assets in order to build an effective cybersecurity strategy. Before engaging external consultants or implementing technical solutions, it is helpful to develop a clear understanding of your current technology, data assets, and baseline security requirements.

Before engaging a consultant, practitioners should understand their baseline:

- **Know your regulatory landscape** - VLSB+C Minimum Cybersecurity Expectations are important controls for Victorian law practices, with violations potentially constituting professional misconduct.
- **Conduct initial self-assessment** - Use VLSB+C's checklist to identify obvious gaps in critical controls (MFA, password policies, automatic updates)
- **Document your current technology inventory** - List all systems, software, devices, and data storage locations your firm uses.
- **Identify your data** - Understand what client information and firm data you have and where it is located. Classify your data as to its sensitivity and legal obligations.
- **Review existing policies** - Assess current written procedures and identify policy gaps that require development or updating.

Why this matters

Legal practitioners are not expected to become cybersecurity experts or have all the technical answers before seeking professional assistance. This initial step is to establish sufficient baseline knowledge to facilitate meaningful conversations with cybersecurity consultants and ensure that professional advice is tailored to your firm's specific circumstances. Your cybersecurity consultant will assist with any outstanding technical assessments, gap analysis, and complex security evaluations that require specialised expertise.

Step 2: Find and select a cybersecurity consultant with professional services experience

Selecting the right cybersecurity consultant is critical to developing an effective security strategy. Unlike general IT consultants, cybersecurity professionals bridge the gap between complex cybersecurity controls and practical business applications. They can translate cybersecurity requirements into strategies while recognising the resource constraints and operational realities of legal practices.

Essential consultant qualifications:

- **Professional services expertise** – Must understand the issues that affect professional services such as law practices. This includes issues such as client privilege, privacy, and data retention and deletion requirements.
- **Relevant certifications** - Look for CISSP, CISM, or industry-specific credentials.
- **SMB focus** - Experience with the resource constraints of smaller practices, not just large corporate clients.

Consultant selection process:

- **Request case studies** from similar-sized legal practices
- **Verify their understanding** of standards hierarchy (VLSB+C → SMB1001)
- **Assess communication skills** - Can they explain technical concepts in business terms?
- **Check references** from other legal clients, focusing on practical implementation success.

Warning signs to avoid:

- Consultants who don't understand legal professional obligations.
- One-size-fits-all approaches without customisation for legal practices.
- Over-reliance on the use of consumer or 'off-the-shelf' products that are inadequate for legal firms.
- Promises of "quick fixes" for complex security challenges.

Why this matters

The complexity of IT and cybersecurity infrastructures means that a cybersecurity strategy should be undertaken with the assistance of a specially trained cybersecurity professionals who are adequately qualified to provide the level of security required by a law firm.

Step 3: Conduct cyber risk assessment

Each firm's IT setup and risk profile has a baseline inherent risk. Beyond the baseline risk, there may be more unique cyber risks requiring tailored analysis. Legal practice management and the cybersecurity consultant must work together to prepare a fit-for-purpose cybersecurity strategy.

Risk assessment components:

- **Asset inventory and classification:** Categorise all digital assets by sensitivity and business criticality
- **Threat landscape analysis:** Identify specific threats targeting legal practices (business email compromise, ransomware, client impersonation scams)
- **Vulnerability assessment:** Technical evaluation of current security gaps and weaknesses

Legal-specific risk factors:

- **Client fund transfers:** High-value transaction risks and "call before you pay" verification needs
- **Long-term data retention:** Requirements to securely store client files for extended periods
- **Remote work arrangements:** Security implications of flexible work locations
- **Third-party integrations:** Risks from third-party systems, unverified software, client portals, and practice management software
- **Policy compliance monitoring:** Assess staff adherence to established cybersecurity policies and procedures

Technology risk profiling

- **Legacy system vulnerabilities:** Older software and hardware with security limitations
- **Cloud vs on-premises:** Different risk profiles requiring different controls
- **Mobile device usage:** BYOD policies and mobile security considerations
- **Network architecture:** Home offices, shared networks, and connectivity security

Why this matters

A comprehensive risk assessment forms the foundation of any effective cybersecurity strategy as it provides the intelligence needed to make informed decisions. This assessment process enables strategic resource allocation to address the highest probability threats. In addition, it informs policies such as data retention and deletion by identifying the main cybersecurity risk based on the firm's particular profile.

Note: Accountability for cybersecurity rests with the Principal Solicitors / Directors. Delegated responsibility should be given to suitably skilled technical consultants.

Step 4: Establish a realistic budget framework

Legal practices must view cybersecurity investment as business insurance rather than an expense. It requires balancing security needs with financial constraints. Budget allocation should follow a risk-based approach, prioritising critical controls first while considering long-term implementation phases to manage cash flow. For some firms, the VLSB+C Minimum Cybersecurity Expectations may fulfil their risk assessment requirements, allowing budget planning to focus on meeting these controls while looking towards an uplift program.

Budgeting:

- **Standards:** Law practices should be able to attain the requirements of the VLSB+C Minimum Cybersecurity Expectations. This is the required minimum expenditure for operating a legal practice.
- **Risk-based allocation:** Higher-risk practices (handling sensitive cases, large client funds) may need to invest more to achieve a higher level of security. In some circumstances, clients (such as government or critical infrastructure organisations) may require a certain level of security as part of the engagement.
- **Phased implementation:** Spread costs to manage cash flow impact.

Cost categories to budget for:

- **Technology investments:** Firewalls, backup systems, monitoring tools
- **Professional services:** Initial assessment, implementation, ongoing support
- **Staff training:** Cybersecurity awareness programs (VLSB+C requirement)
- **Compliance activities:** Audits, certifications, policies, documentation
- **Incident response:** Forensic capabilities, recovery and business continuity
- **Cyber insurance:** Coverage for incidents despite preventive measures and costs not covered by professional indemnity insurance

ROI considerations:

- **Cost of breach prevention vs breach response:** Prevention typically costs substantially less than breach recovery costs
- **Client trust and retention:** Demonstrable security as competitive advantage
- **Regulatory compliance:** Avoid professional misconduct and regulatory implications

Why this matters

Proper budget planning prevents both over-investment in unnecessary controls and under-investment that leaves critical gaps. For Victorian practitioners, VLSB+C compliance is considered the minimum and budget allocation for these requirements is extremely important. Where a law practice faces greater cybersecurity risks or requirements, additional expenditure will be required.

Step 5: Choose appropriate standards framework

In consultation with your cybersecurity consultant, select a standard that matches your risk profile, budget, and regulatory requirements. The selected standard must be able to meet all your current requirements. The standard may also be chosen with a view of an uplift path being undertaken in the future.

VLSB+C Minimum Cybersecurity Expectations (Minimum baseline)

- **Critical controls:** MFA, strong passwords, automatic updates
- **System controls:** Technical safeguards, network security, data protection
- **Behavioural controls:** Staff training, incident response procedures
- **Suitable for:** All Victorian legal practices as minimum compliance requirement

DSI SMB1001 - A multi-tiered standard

- **Five progressive levels:** Bronze through to Diamond certification tiers
- **Practical approach:** Designed specifically for SMB resource constraints
- **Annual updates:** Framework evolves with threat landscape
- **Suitable for:** Practices wanting competitive advantage through certification and a structured improvement path

Selection criteria:

- **Regulatory requirements:** VLSB+C minimum is non-negotiable for Victorian practitioners and must be met or exceeded by implementing a higher standard
- **Client expectations:** Some clients may require specific controls or certifications
- **Risk tolerance:** Higher-risk practices need more comprehensive frameworks
- **Available resources** - Both financial and staff time constraints
- **Growth trajectory:** Consider frameworks that scale with practice expansion

Why this matters:

Selecting the appropriate cybersecurity framework determines both your compliance status and security effectiveness. It also directly impacts budget allocation, staff training requirements, and technology investments for years to come. Different frameworks serve different business needs and different clients may require specific security certifications before engagement. The tiered approach allows strategic planning for future security improvements. This prevents costly framework changes later when client requirements or regulatory standards increase.

Note: In some situations, controls from one standard may be used in conjunction with controls from another standard. For example: a firm may use the DSI SMB1001 Level 4 (Platinum) standard for their technical controls and certification purposes however, this might be enhanced with behavioural controls taken from the VLSB+C Minimum Cybersecurity Expectations.

Step 6: Implement controls with professional guidance

Implementation of cybersecurity controls must follow the plan developed with your consultant, using a phased approach to minimise disruption and ensure each control is correctly deployed.

Suggested implementation phases:

- **Phase 1: Critical controls first:** Address VLSB+C critical controls (MFA, passwords, updates). (Suggested timeframe: within 30 days)
- **Phase 2: Core security measures:** Deploy endpoint protection, backups, access controls. (Suggested timeframe: within 90 days)
- **Phase 3: Advanced protections:** Implement monitoring, incident response procedures, comprehensive policy documentation, compliance documentation. (Suggested timeframe: within 180 days)

Technical control categories:

- **Identity and access management:** MFA, role-based access, privileged account management
- **Network security:** Firewalls, VPNs, network segmentation, intrusion detection
- **Endpoint protection:** Anti-malware, device encryption, mobile device management
- **Data protection:** Encryption at rest and in transit, data loss prevention, secure communications
- **Backup and recovery:** Automated backups, offline storage, recovery testing

Implementation best practices:

- **Pilot testing:** Deploy controls in phases to minimise business disruption
- **Staff communication:** Explain changes and benefits to gain user acceptance
- **Documentation:** Maintain implementation records for compliance auditing
- **Change management:** Formal processes for system changes and updates
- **Policy Integration and Staff Engagement:** Develop clear written policies that explain the "why" behind security requirements. Conduct policy review sessions with staff to address questions and gain buy-in for security procedures.

Why this matters:

Proper implementation avoids misconfigurations that create security gaps or disrupt workflows. Phased deployment ensures that critical protections are in place quickly while allowing time for user acceptance and fine-tuning. Proper change management and training reduce resistance and errors, improving long-term control effectiveness. Engaging a consultant guarantees that technical controls align with legal practice needs and that documentation supports future audits and continuous improvement.

Step 7: Establish continuous monitoring and maintenance

A cybersecurity strategy is not a set-and-forget affair. Technology environments are dynamic, requiring ongoing vigilance. For many cybersecurity strategies, some threat monitoring may occur automatically as part of your cybersecurity solution. In terms of maintenance, some cybersecurity strategies require specialised reviews and intervention best suited to a cybersecurity consultant.

Monitoring components:

- **Real-time threat detection:** Log analysis, anomaly detection, security analytics platforms
- **Vulnerability management:** Regular scanning, patch management, configuration monitoring
- **Compliance monitoring:** Ongoing verification of standards adherence
- **Policy effectiveness review:** Regular evaluation of policy adherence and effectiveness through staff feedback and incident analysis

Technology change management:

- **Asset inventory updates:** Track new systems, software, and devices
- **Control adjustment:** Modify security measures for changes in your technology and personnel
- **Documentation maintenance:** Keep policies and procedures current

Review process:

- **Threat landscape updates:** New attack methods and vulnerabilities
- **Control effectiveness:** Performance metrics and incident analysis
- **Compliance status:** Standards adherence and regulatory changes
- **Budget and resource planning:** Upcoming security investments

Why this matters:

Continuous monitoring keeps your security controls effective as technology and threats evolve. Ongoing maintenance prevents small issues from becoming major incidents and ensures controls remain aligned with your firm's risk profile.

Step 8: Stay current with evolving threats and attack methods

Cybercriminals constantly develop new techniques in an effort to defeat cybersecurity protections. A cybersecurity strategy must employ processes and solutions that allow you to regularly review and update your cybersecurity posture.

Threat intelligence sources:

- **Industry-specific alerts:** Legal sector threat advisories and case studies
- **Government advisories:** ACSC, OAIC, and international cybersecurity bulletins
- **Professional networks:** Attend cybersecurity working groups and forums and receives updates from the VLSB+C, LPLC and the LIV
- **Vendor communications:** Security updates from technology providers

Current threat trends affecting legal practices:

- **Business email compromise:** Increasingly sophisticated client fund theft schemes
- **AI-enhanced social engineering:** More convincing phishing and impersonation attacks
- **Supply chain compromises:** Attacks through technology vendors or third-parties (for example: real estate agents and mortgage brokers)
- **Ransomware evolution:** More targeted attacks with higher ransom demands

Response strategies:

- **Monthly threat briefings:** Regular updates for all staff on current scams
- **Simulation exercises:** Phishing tests and incident response drills
- **Vendor security reviews:** Regular assessment of third-party providers
- **Client communication:** Educating clients about current fraud trends

Why this matters:

Staying current with evolving threats helps your firm in the fight against adversaries who continuously refine their attack methods. Updated attack types, such as AI-driven phishing, supply-chain compromises, and sophisticated ransomware, are being specifically designed to target the legal sector. Without proactive threat intelligence and adaptation, new vulnerabilities can go unnoticed, increasing the likelihood of a cybersecurity breach.

Step 9: Conduct regular strategic reviews

Strategic reviews ensure cybersecurity strategies remain effective as business needs, technology, and threats evolve. Partner with your cybersecurity consultant to evaluate risk changes, regulatory updates, framework evolution, and technology refresh requirements. Use review outcomes to adjust strategies, plan budgets, develop staff capabilities, and evaluate vendor relationships.

Regular comprehensive review:

- **Risk environment changes:** New practice areas, client types, technology adoption
- **Regulatory updates:** Changes to VLSB+C expectations, new compliance requirements
- **Standards evolution:** Updates to the standards
- **Technology refresh:** Planned system upgrades or replacements

Review methodology:

- **Consultant partnership:** Annual strategy sessions with cybersecurity advisors
- **Peer benchmarking:** Comparison with similar practices and industry standards
- **Control testing:** Verification that implemented measures remain effective
- **Cost-benefit analysis:** ROI assessment of security investments
- **Policy effectiveness review:** Regular evaluation of policy adherence and effectiveness through staff feedback and incident analysis

Outcome planning:

- **Strategy adjustments:** Modifications to address identified gaps or changes
- **Budget planning:** Next year's cybersecurity investment priorities
- **Staff development:** Training needs and capability building requirements
- **Vendor relationships:** Evaluation of consultant and technology provider performance

Why this matters:

Regular strategic reviews prevent cybersecurity programs from becoming outdated or ineffective against emerging threats. Reviews ensure your chosen framework remains aligned with regulatory changes and client expectations, particularly as government and corporate clients increasingly demand specific security certifications.