

Rimini Street®

The Software Support and Agentic AI ERP Company™

EBOOK

A GUIDE TO ENTERPRISE SOFTWARE SECURITY AND MODERNISATION FOR AUSTRALIAN GOVERNMENT AGENCIES

How to assess risk, protect what works and prioritise what needs to change

Contents

Purpose of this guide 3

Executive summary 4

How to use this guide 5

Key context: PSPF creates the urgency, not the answer. 6

1. Define the outcomes and understand the estate 7

2. Assess risk across four connected domains. 8

3. Validate commercial support and maintenance exposure 9

4. Compare the risk of continued operation with the risk of change 11

5. Select the appropriate response. 13

6. Define layered controls around the application 15

7. Document the decision and keep it current. 16

Conclusion 17

Purpose of this guide

PSPF Direction 002-2026 creates an urgent need for Australian government agencies to assess their existing technology environments and address cybersecurity risks. This guide provides a practical framework for evaluating security, architecture, operations and support so that technology leaders can identify risks, select proportionate treatments and make defensible decisions about what to sustain, remediate, modernise, replace or retire.

This guide provides general information, not legal advice, and does not establish or guarantee compliance. Organisations should seek independent legal advice on their obligations under PSPF Direction 002-2026 and other applicable requirements.



Executive summary

Major upgrades or migrations are not inevitable simply because an ERP system is mature or approaching a vendor milestone. With appropriate security, support and operational practices, organisations can sustain a stable core, improve processes and introduce new capabilities around it, then modernise selectively where change delivers measurable value.

This distinction is important as Australian government entities respond to PSPF Direction 002-2026. The direction requires entities to identify technology classified as “vulnerable” or “legacy,” understand the risks it presents and implement appropriate mitigations. Age and vendor support status may inform that assessment, but neither determines whether a system is secure, resilient or fit for purpose. They are risk indicators to test against evidence, not conclusions in themselves.

A mature application can continue to perform reliably when its exposure is understood, its dependencies are documented and appropriate expertise, controls and support arrangements are in place. Moreover, existing customisations may embody critical processes and institutional knowledge that must be supported and protected rather than treated as evidence that the system should be replaced.

This guide introduces a repeatable framework for assessing applications across four connected risk domains:

- **Security:** Vulnerabilities, access, data sensitivity, exposure, monitoring and response
- **Architecture:** Dependencies, interfaces, customisations, data flows, technical coupling and containment options
- **Operational:** Service criticality, recoverability, skills, documentation, continuity and the risk of change
- **Commercial:** Software rights, support and maintenance coverage, supplier viability, expertise, contractual protections and credible alternatives

The framework helps technology leaders evaluate options for addressing legacy technology risks, rather than treating an upgrade as the starting point. It provides a method to assess whether an existing application can continue operating with independent support, retained expertise, contractual measures and technical controls, or needs modernisation, replacement or retirement. This separates upgrading to retain vendor support from addressing identified risks, while keeping continued operation subject to requirements under PSPF Direction 002-2026.

The intended outcome

A documented, evidence-based decision for each application: *sustain and protect, remediate, modernise, replace* or *retire*. The decision should reflect the risk of continuing to operate the system without proper practices, the value it continues to provide and the cost, disruption and operational risk introduced by changing it.

How to use this guide

Use the framework across the IT estate to identify which applications require deeper assessment, then apply the detailed tests to each prioritised application. The same structure can support a PSPF stocktake, architecture review, investment prioritisation, sourcing decision or application rationalisation exercise.

1. **Define the outcomes and understand the estate.**
2. **Assess risk across four connected domains.**
3. **Validate commercial support and maintenance exposure.**
4. **Compare the risk of continued operation with the risk of change.**
5. **Select the appropriate response: sustain, remediate, modernise, replace or retire.**
6. **Define layered controls around the application.**
7. **Document the decision and keep it current.**

Evaluate each application on its own merits rather than starting with assumptions based on age, version or vendor support status. The objective is to preserve what continues to serve the agency well, address risks and prioritise change where it delivers meaningful value.

A framework, not a formula

The tables and rating scales create consistency, but they don't replace judgement. A low score in one domain does not offset a critical weakness in another. Risks, mandatory requirements and service consequences must be considered in the final decision.



"Technology doesn't become risky simply because it gets older. Risk comes from poor architecture, weak controls and dependencies that have yet to be discovered."

— Tal Nathan,
Regional CTO, ANZ
Rimini Street

Key context: PSPF creates the urgency, not the answer

PSPF Direction 002-2026 requires Australian government entities to reduce cybersecurity risks arising from technology classified as "vulnerable" or "legacy," and strengthen their cyber posture across government systems. It makes understanding and addressing material technology risk a current governance and management priority.

Agencies still need to determine whether existing architecture, controls, expertise, support and operational practices provide an acceptable level of security and resilience. Where they do, a stable ERP core can remain in service while new capabilities are introduced around it.

Therefore, the objective is to identify cybersecurity risk and address it appropriately, rather than treating age or lifecycle status alone as a reason to modernise by default.

A compliant and responsible response begins with evidence: what software applications the entity operates, what each system supports, what data it handles, how it is exposed and where material risks sit. The entity can then determine which treatment will reduce those risks most effectively without introducing disproportionate cost, disruption or delivery risk.

Meeting the requirement of PSPF Direction 002-2026 therefore involves two linked disciplines:

- **Immediate risk reduction:** Identify urgent exposures and implement controls or mitigations that protect critical services.
- **Portfolio direction:** Decide which systems should be sustained and protected, modernised, replaced or retired, and sequence investment accordingly.

This is especially important in complex, established technology environments. Critical services can't simply be suspended while every system is rebuilt. Budgets, specialist resources and organisational capacity are limited, and major change can introduce its own security, continuity and delivery risks.

ERP age is just a number

A useful assessment doesn't begin by asking how old the software is. Instead, it begins by asking whether the system remains fit for purpose, supportable and secure: what could fail, what the consequences would be and whether those consequences can be prevented, contained or managed and resolved.

Age and end-of-support status remain relevant indicators because they may affect access to fixes, expertise and assurance. But neither is a security verdict. With third-party support providers and interoperability, security and Agentic AI solutions that do not require a rip-and-replace disruption, there are proven, flexible paths to keeping systems running for years to come while maintaining full compliance and protection of mission-critical investments.

1 Define the outcomes and understand the estate

Before selecting a technology response, define the outcomes the organisation is trying to protect or improve. Typical outcomes include:

- Continuity of essential services
- Protection of sensitive information
- Regulatory compliance
- Operational resilience
- Improved capability
- Reduced cost
- Greater agility
- A simplified application estate

This outcome-first approach prevents a vendor milestone, product roadmap or upgrade programme from becoming the default course of action. The organisation should own its strategy, define the capabilities and assurance it requires, then evaluate how the market can meet those requirements.

An outcome-first approach also helps agencies allocate investment more effectively. Where an existing system remains reliable, secure and fit for purpose, the organisation can strengthen interoperability and controls around it while directing funding and specialist capacity to the services and capabilities that need the most improvement.

Build a reliable evidence base

The first practical step is discovery. Existing asset registers can provide a baseline, but they should be tested against architecture records, contracts, configuration data, support arrangements, operational knowledge and automated discovery.

For each application, document:

- Business service and criticality
- Business owner, technology owner, risk owner and support owner
- Software product, version, deployment model and lifecycle status
- Data held, processed or accessed, including sensitivity and residency
- Users, privileged access and external exposure
- Interfaces, integrations, dependencies and upstream or downstream effects
- Customisations, extensions and locally developed components
- Vendor and service-provider support coverage
- Internal skills, documentation, recoverability and continuity arrangements
- Known vulnerabilities, incidents, audit findings and accepted risks
- Current cost, planned investment and realistic change dependencies



"Organisations must consider risk holistically from an enterprise architecture perspective and then work backward from the outcomes the organisation needs."

— Tal Nathan
Regional CTO, ANZ
Rimini Street

"You can't fully assess your risk exposure unless you first have discovery and observability across your environment. This gives you a clearer view of what's actually happening inside your organisation."

— George Goosen
Chief Innovation Officer,
Rimini Street

2 Assess risk across four connected domains

Applications should be assessed as part of an operating environment, not as isolated software products. A system that remains valuable and reliable may be a strong candidate for continued operation when its exposure is understood, appropriate controls are in place and credible support remains available.

The framework below brings security, architecture, operational and commercial considerations into one assessment. Together, these four domains help determine where material risk exists, where existing controls are effective and whether the appropriate response is to sustain, strengthen or change the application.

DOMAIN	CORE QUESTION	KEY CONSIDERATIONS	EVIDENCE
Security	Can the system and its data be protected at an acceptable level?	Exposure, data sensitivity, identity and access, known vulnerabilities, configuration, logging, monitoring, segmentation, recovery, incident response	Security assessments, vulnerability data, architecture diagrams, access reviews, incidents, control testing
Architecture	Is the application understood, well-controlled and supportable within the broader environment?	Dependencies, interfaces, customisations, data flows, coupling, component lifecycle, containment, observability, integration failure modes	Application and data architecture, dependency maps, interface catalogue, code/configuration records
Operational	Can the service be operated and recovered reliably?	Criticality, availability, capacity, skills, documentation, key-person dependency, backup, recovery, impact of change, continuity, testability	SLAs, incidents, DR tests, operating procedures, skills matrix, service reports, change history
Commercial	Are there credible arrangements to maintain the software and service?	Support rights, maintenance coverage, response commitments, supplier viability, expertise, licensing, escrow, exit rights, alternative providers, cost predictability	Contracts, licences, statements of work, support policies, renewal terms, supplier due diligence

Important

Vendor end of support is a commercial milestone, not a security verdict. Assess what capability is changing, whether that change is material to the application and whether existing expertise, independent support or compensating controls can provide an acceptable response.

Use a consistent rating scale

RATING	MEANING	DECISION IMPLICATION
1 – Low	Controls are effective; evidence is current; failure consequences are limited or readily contained.	Continue operation with routine management and monitoring.
2 – Moderate	Some weaknesses or dependencies exist, but they are understood and manageable.	Sustain and protect with planned improvements and review triggers.
3 – Significant	Material weakness, incomplete evidence or increasing exposure requires funded treatment.	Remediate or modernise within an agreed horizon.
4 – High	Control failure, dependency without an adequate support or mitigation path or operational fragility could materially affect the service.	Prioritise intervention and constrain exposure while treatment proceeds.
5 – Critical	Unacceptable exposure, a mandatory breach or a severe consequence with no credible control or recovery path.	Take immediate action to mitigate exposure and determine whether to remediate, isolate, replace or retire.

3 Validate commercial support and maintenance exposure

A change in vendor support or maintenance status is often presented as a binary event: upgrade or accept unacceptable risk. In practice, however, an end-of-support date typically only changes the available commercial support arrangements. It does not, by itself, make an application insecure, unsupportable or unsuitable for continued operation.

The critical question is whether the application remains fit for purpose and whether the agency retains the rights, expertise, response capability and assurance needed to operate it safely and reliably. These capabilities may be provided internally, via a third-party provider or through a mixed support model.

The commercial-exposure test

- **Identify the capability that is changing.** Separate software rights and access to updates, security fixes, technical assistance, escalation, regulatory statements, certifications, knowledge bases and tooling.
- **Determine materiality.** Establish which capabilities the application actually requires based on its exposure, criticality, architecture, customisations and operating model.
- **Confirm the agency's rights.** Review current entitlements, licence conditions, maintenance terms, usage rights, notice periods, audit provisions and exit obligations.
- **Assess the support model.** Determine the expertise, response capability, escalation paths and service commitments available internally and through independent or mixed support arrangements.
- **Evaluate provider concentration.** Identify reliance on a single vendor, service provider, specialist or individual and the consequences if that capability becomes unavailable.
- **Test credible alternatives.** Validate whether third-party support, retained expertise, managed services, source or configuration access, escrow, extended support or architectural containment can provide the required continuity and assurance.
- **Assess the residual exposure.** Document what remains after alternative support arrangements and controls are applied, who owns that exposure and whether it is acceptable.
- **Compare with the risk of change.** Weigh the residual support exposure, if any, against the migration, integration, data, service disruption, cost and delivery risks introduced by modernisation or replacement.



COMMERCIAL CONSIDERATION	QUESTIONS TO TEST	WARNING SIGNS	POTENTIAL TREATMENT
Support entitlement	What assistance, fixes, tooling and escalation paths are available under the current and alternative support models?	Ambiguous coverage; critical services outside the support scope; response capability dependent on discretionary effort	Clarify or renegotiate terms; procure extended, independent or mixed support; address remaining exposure.
Maintenance and issue resolution	Can defects and vulnerabilities be diagnosed, mitigated and resolved in a timely manner?	No credible diagnosis or resolution path; no access to expertise; mitigations unable to be implemented or tested	Apply alternative engineering/support; seek configuration or code-level resolution; implement protective tools; contain exposure; modernise selectively where required.
Provider capability	Can the provider deliver the required expertise, responsiveness and service over the decision horizon?	Capability loss; unclear accountability; inadequate service commitments; limited expertise	Perform provider due diligence; explore a multi-provider model; transfer knowledge; establish an exit plan.
Skills and knowledge	Is sufficient application, integration and customisation expertise available internally or externally?	Single-person dependency; undocumented customisations, interfaces or operating practices; scarce product skills	Document; cross-train personnel; retain specialists; contract additional capacity; establish knowledge transfer requirements.
Licensing and rights	Does the organisation hold the rights needed to run, modify, test and recover?	Unclear rights; restrictive use; dependency on vendor-controlled keys, tools or services	Review licences and entitlements; clarify contractual rights; establish escrow where appropriate; preserve entitled software; develop an alternative deployment or recovery plan.
Assurance and accountability	Can the organisation demonstrate that the support model is governed, effective and appropriate for the application?	No service evidence; unclear ownership; unmanaged exceptions; controls untested	Define SLAs/KPIs; assign accountable owners; test controls; document risk exceptions; establish review requirements.
Exit and transition	Can support or service delivery move to another arrangement if the current model no longer meets requirements?	No data export, documentation, tooling, skills or transition rights	Establish exit clauses; test handover processes; preserve portable data and knowledge; maintain a transition plan and funding.



"Risk mitigation doesn't mean everything needs to be replaced. Understand the extent of your estate and your licensing rights, determine the support it requires and evaluate the options available."

— George Goosen
Chief Innovation Officer, Rimini Street

4 Compare the risk of continued operation with the risk of change

A sound decision compares two positions: the residual risk of continuing to operate the application with appropriate support, controls and operational practices in place, and the risks introduced by changing it. Ignoring either side distorts the result.

Continued operation shouldn't be treated as the higher-risk option by default. Where an application remains valuable, secure, well-controlled and supported, sustaining it can preserve stability while allowing the organisation to direct resources towards higher-priority security, service and modernisation needs.

RISK CONSIDERATIONS FOR CONTINUED OPERATION	RISK CONSIDERATIONS FOR CHANGE
Unresolved vulnerabilities and appropriate remediation or mitigation options	Service continuity during implementation or cutover
Availability and concentration of skills, expertise and support	Data retention and integrity during migration
Operational resilience, recovery capability and continuity	Interoperability across integrations and dependent services
Long-term cost and maintainability of support arrangements	Preservation of embedded business rules or custom capabilities
Ability to accommodate new capability or policy requirements	Delivery, adoption and capability outcomes
Contractual coverage, assurance and governance	Vendor concentration, lock-in and ongoing operating costs

This comparison is especially important for applications with extensive customisations, integrations and embedded processes. These investments may support capabilities that remain valuable to the organisation. Replacing the underlying platform does not automatically eliminate the business rules, data requirements, interfaces and operating requirements surrounding it. Those capabilities must still be redesigned, migrated, tested and supported.

> ***"Your IT investments should be doing the following 3 things: Improve profitability, lower operating costs and/or create competitive advantage. If none of the above, it's not worth doing them now."***
>
> ***— Greg Mennie***
> *Senior Account Executive, Rimini Street*

Prioritise with consequence and controllability

Prioritisation should reflect more than the number of identified issues. Give greater weight to material consequences, actual exposure, the effectiveness of existing controls and the ability to recover. Then, consider how readily the remaining exposure can be reduced. Some issues can be addressed through targeted controls or alternative support arrangements; others may require structural change.

POSITION	CHARACTERISTICS	LIKELY DIRECTION
High operating risk / manageable change	Material exposure; weak controls or poor recovery; a credible modernisation, replacement or retirement option is available.	Prioritise modernisation, replacement or retirement.
High operating risk / high change risk	Critical weakness requires action, but a major change could disrupt essential services or fail due to complexity.	Strengthen controls, contain exposure and remediate immediate weaknesses while developing a staged modernisation plan.
Manageable operating risk / high change risk	Risk can be controlled; replacement is complex, costly or disruptive.	Sustain and protect with layered controls, a defined support model and review triggers.
Manageable operating risk / manageable change	The current position is acceptable, and change is feasible.	Base the decision on value, strategy and timing rather than age or lifecycle status.



5 Select the appropriate response

Once the evidence is assembled, select the response that best addresses the application's requirements, material risks and value to the organisation. The objective is not to force every application towards modernisation or replacement, but to determine which response delivers the strongest outcome while preserving what continues to work well.

The five response paths below distinguish between applications that remain valuable and controllable, those that need targeted remediation or modernisation and those whose risks or limitations justify replacement or retirement.

RESPONSE	WHEN IT FITS	MINIMUM EXPECTATION
Sustain and protect	Business value remains strong; residual risk can be controlled, and a credible support model is available; modernisation or replacement wouldn't deliver sufficient value to justify the cost or risk of change.	Documented support model, layered controls, recovery capability, accountable ownership and review triggers
Remediate	The application remains valuable and defined weaknesses can be reduced without replacing the underlying system.	Funded actions, accountable owners, target dates and evidence that controls work
Modernise in place	The application is still reliable, but targeted improvements to architecture, security, experience or integration would deliver measurable value.	Clear target architecture, controlled interfaces, measurable improvement and sequenced delivery stages to minimise disruption
Replace	A material risk, constraint or capability gap cannot be acceptably addressed in place, and replacement provides a demonstrably stronger outcome.	Business-led case, dependency and migration plan, security-by-design, transition support and value measures
Retire	The service is duplicated or no longer required, or the application's remaining value no longer justifies its cost and management requirements.	Data disposition, dependency removal, user transition, licence closure and decommissioning verification

Decision principle

Modernise where change materially improves security, resilience, service or capability. Sustain and protect where the application continues to deliver value, risk can be controlled and the existing environment remains fit for purpose.



A repeatable eight-step decision process

1. **Discover the estate.** Build and validate the inventory of applications, infrastructure, data, integrations and dependencies.

2. **Establish criticality.** Identify the service or business function that depends on each system and the consequences of outage or compromise.

3. **Map data, access and dependencies.** Document what the system holds, processes and connects to, including sensitive data and privileged access.

4. **Locate material risk.** Determine whether risk sits in the software, architecture, integrations, access, exposure, support model, operations or dependencies.

5. **Validate commercial exposure.** Identify what support or maintenance capability may change and test credible alternatives.

6. **Test available responses.** Evaluate whether controls, remediation, alternative support, modernisation, replacement or retirement can appropriately address the identified need.

7. **Evaluate value and risk of change.** Compare residual operating risk with cost, disruption, migration risk, capability and strategic fit.

8. **Decide, document and monitor.** Record the selected path, rationale, controls, ownership, milestones, assumptions and review triggers.

6 Define layered controls around the application

Sustainment doesn't mean leaving an application untouched. It means deliberately managing it within a layered architecture and control environment that addresses its actual exposure, dependencies and operational requirements. Technology controls are only part of that model. Skilled people, clear accountability, documented practices and continuous monitoring are equally important to maintaining a secure and reliable environment over time.

It's important to keep this distinction in mind, as newer software is not inherently secure — just as mature software is not inherently insecure. The appropriate security posture depends on how effectively the organisation understands its exposure and applies controls and mitigations suited to the environment.

Apply controls to the actual exposure

- Select controls based on the application's architecture, exposure and potential failure modes. Depending on the environment, actions may include:
- Reduce the attack surface by removing unnecessary network paths, services, accounts and integrations.
- Segment or isolate the application to contain the potential effect of a threat.
- Strengthen identity and access with modern controls such as multifactor authentication, privileged-access management or access brokering around the application.
- Apply compensating controls where direct remediation is constrained, using measures such as application allowlisting, protective monitoring, virtual patching or gateway controls.
- Increase observability across application behaviour, interfaces, data access and service health so that changing conditions can be identified and assessed.
- Improve resilience and recovery through backup, restoration testing and manual continuity procedures.
- Document the environment by keeping customisations, interfaces, operational procedures and known failure modes current.
- Establish clear support responsibilities for diagnosis, escalation, remediation and communications.

Control test

A compensating control is useful only if it addresses the identified risk, operates reliably, produces evidence and has an accountable owner. The objective isn't to accumulate a list of controls but to create a layered environment that can protect the application, detect changing conditions and support an appropriate response.

Maintained together, these technical, human and operational practices can help organisations keep stable systems secure and running smoothly while freeing up capacity for higher-value technology initiatives.

"Even if you're running the latest, newest, most sophisticated software, it doesn't mean it is secure. Security is continual, and it depends on how the system is configured, protected, monitored and operated."

— Vinyl Shetty
Senior Security Architect, APAC
Rimini Street

"The shift has to be toward continuous monitoring and protection: address the underlying weakness, put mitigations in place without disrupting the ecosystem and continuously monitor as risks emerge."

— Vinyl Shetty
Senior Security Architect, APAC
Rimini Street

7 Document the decision and keep it current

A defensible decision records not only the outcome but also the evidence and rationale behind it. This is particularly important when the decision is to sustain an existing application: continued operation should be documented as an active, governed choice backed up by controls, support arrangements with a credible provider and review triggers.

For each application, retain a concise decision record containing:

- Application, service, owner and criticality
- Assessment date, scope, evidence and material assumptions
- Ratings across security, architecture, operational and commercial risk
- Material risks, existing controls and residual exposure
- Commercial-support findings, including any capability that may change and validated alternatives such as third-party support providers
- Risk of continued operation compared with risk of change
- Selected response and alternatives considered
- Required controls, investment, milestones and accountable owners
- Review date and event-based triggers
- Approvals, exceptions and formal risk acceptance where required

The decision should remain up to date as the application and its surrounding environment evolve. Review it at an established interval and when a material event changes the evidence or assumptions on which the decision was based. Relevant triggers may include a new vulnerability, supplier or support change, major incident, architecture change, failed recovery test, significant cost increase, loss of key skills or a new policy requirement.

Governance principle

Documenting a decision to sustain an application doesn't make that decision permanent. It merely establishes the conditions under which continued operations remain appropriate and the triggers that should prompt reassessment.



Conclusion

The central principle

Age alone does not determine risk. Evidence, consequence, controllability and value should determine the response.

PSPF Direction 002-2026 establishes a clear imperative for Australian government agencies to understand their environments and address cybersecurity risks. The appropriate response is not a blanket modernisation programme based on age or vendor lifecycle status, but an evidence-led assessment of whether each system remains secure, supported, operable and fit for purpose.

The stronger response is to determine where risk exists, validate the organisation's support options and direct investment where change can make the greatest impact.

Some systems will require urgent remediation, modernisation, replacement or retirement. Others can be sustained safely and responsibly with the right architecture, layered controls, operational practices, expertise and support model in place.

The discipline is to make each decision deliberately and keep it current: sustain what continues to serve the agency well, address risks with proportionate controls and invest in change where the evidence shows it will deliver a stronger outcome.

For organisations that choose to sustain existing enterprise software, the right combination of support, security, operational expertise, optimisation and interoperability can help keep the core stable while creating capacity for innovation. Rimini Street helps government organisations support and optimise mission-critical systems, strengthen operational resilience and redirect resources towards priority services and public outcomes.

Rimini Street®

Make your next technology decision with confidence

Schedule a consultation with Rimini Street to assess your application estate, evaluate support and sustainment options and identify a practical, risk-based path forward.



Rimini Street, Inc. (Nasdaq: RMNI), a Russell 2000® Company, is a proven, trusted global provider of end-to-end, mission-critical enterprise software support, optimisation and innovative Agentic AI ERP solutions, and is the leading third-party support provider for Oracle, SAP and VMware software. The Company has signed thousands of IT service contracts with Fortune Global 100, Fortune 500, midmarket, public sector and government organisations that have leveraged the Rimini Smart Path™ methodology to achieve better operational outcomes, billions of U.S. dollars in savings and self-funded AI and other innovation.

Rimini Street®

riministreet.com
info@riministreet.com
x.com/riministreet
linkedin.com/company/rimini-street

© 2026 Rimini Street, Inc. All rights reserved. “Rimini Street” is a registered trademark of Rimini Street, Inc. in the United States and other countries, and Rimini Street, the Rimini Street logo, and combinations thereof, and other marks marked by TM are trademarks of Rimini Street, Inc. All other trademarks remain the property of their respective owners, and unless otherwise specified, Rimini Street claims no affiliation, endorsement, or association with any such trademark holder or other companies referenced herein.

This guide is for general informational purposes only and does not constitute legal advice. Organisations should obtain independent legal advice on their obligations under PSPF Direction 002-2026 and other applicable requirements. Use of this guide does not establish or guarantee compliance.

This document was created by Rimini Street, Inc. (“Rimini Street”) and is not sponsored by, endorsed by, or affiliated with any other party. Except as otherwise expressly provided in writing, Rimini Street assumes no liability whatsoever and disclaims any express, implied or statutory warranty relating to the information presented, including, without limitation, any implied warranty of merchantability or fitness for a particular purpose. Rimini Street shall not be liable for any direct, indirect, consequential, punitive, special, or incidental damages arising out of the use or inability to use the information. Rimini Street makes no representations or warranties with respect to the accuracy or completeness of the information provided by third parties, and reserves the right to make changes to the information, services or products, at any time. M_09911 | 11042026 | LR0061055