netcraft

2026-2027

Scams Prevention Framework Checklist

A step-by-step assessment for banks, telecommunications providers, and digital platforms

How to use this checklist

This checklist is designed to help you assess your readiness against the six principles of Australia's Scams Prevention Framework.

Work through each section, mark every item as **"Met," "Partially met,"** or **"Not met,"** then use the scorecard at the end to identify areas that need attention.

Two things to keep in mind:

1. This checklist reflects the SPF exposure drafts as of July 2026. The sector codes are still exposure drafts, so specific obligations are "expected to require," not settled law.
2. Each checklist item identifies the evidence you should be able to produce to support your assessment, helping you build a defensible record of the reasonable steps your organization has taken.

©2026 Netcraft Ltd.

Who it's for

Heads of Fraud & Compliance Officers

Responsible for SPF readiness and regulatory evidence

Fraud, Trust & Safety Managers

Responsible for scam detection, disruption, and escalation

Brand Protection leaders

Assessing how impersonation and phishing exposure helps to Prevent, Detect, and Disrupt principles

Key takeaways

- The SPF implementation timeline is already underway. Several preparatory activities, including AFCA membership and readiness planning, fall ahead of the March 2027 commencement date.
- Organizations serving Australian-resident customers should assess whether the SPF applies to them, including where services are provided from outside Australia.
- Prevent, Detect, Disrupt, and Respond carry the highest civil penalty tier, making them a priority for any readiness assessment.
- Readiness depends on both effective controls and the ability to demonstrate the reasonable steps your organization has taken.

©2026 Netcraft Ltd.

Table of contents

1. **Where the SPF stands as of mid-2026**

2. **Who the SPF covers**

3. **Self-assess against the six SPF principles**
   - Govern
   - Prevent
   - Detect
   - Disrupt
   - Respond
   - Report

4. **Score your readiness**
   - Record your scores
   - Interpret your results

5. **Sector-specific obligations to watch**

6. **What to do before the codes are finalized**
   - Build your readiness with Netcraft

7. **Sources**

©2026 Netcraft Ltd.

1 Where the SPF stands as of mid-2026

- The Scams Prevention Framework has moved beyond consultation. The legislation is in force, the designated sectors have been confirmed, and the focus now is preparing your organization for the obligations that take effect on March 31, 2027.
- While the sector codes remain in exposure draft, they already point clearly at what regulators will expect.

What it means for your organization

Feb 2025

The SPF Act commences. The six principles become part of the *Competition and Consumer Act 2010 (Cth).*

May 2026

Banks, telcos, and digital platforms are formally designated. If you're in one of those sectors, your regulatory obligations are no longer theoretical.

Jun 2026

Consultation on the draft sector codes closes. The exposure drafts are the best indication of what regulators are expected to look for when assessing

Sep 2026

Regulated entities that provide regulated services must be AFCA members.

Mar 2027

AFCA begins handling eligible SPF scam complaints that have not been resolved through internal dispute resolution.

Late 2027

Supplementary rules and scam intelligence-sharing obligations are expected to commence.

©2026 Netcraft Ltd.

2 Who the SPF covers

The SPF applies to more than financial services and telecommunications providers. It also covers a broad range of digital platform services and, in some cases, organizations operating outside Australia.

Before working through the checklist, confirm whether your organization falls within the current scope of the framework — or is likely to in the future.

Three questions tell you where you stand.

Are you in a designated sector?

Banks, telecommunications providers, and digital platforms are currently designated under the SPF.

Digital platforms cover three categories where scam activity commonly occurs:

- Social media services: platforms where users create, share, and interact with content.
- Paid search advertising services: platforms where advertisers pay to appear against user search queries.
- Direct messaging services: services that enable private text, media, or voice communications, separate from SMS.

Do you have customers who are Australian residents?

The SPF can apply even if your organization is based outside Australia. If you provide services to Australian-resident customers within a designated sector, the framework's obligations may still apply.

Are you in a sector identified for future designation?

Superannuation, insurance, online marketplaces, and cryptocurrency services are not currently designated, but they have been identified as potential future sectors. If you operate in one of these industries, it's worth reviewing your existing controls against the six SPF principles now, rather than waiting for future designation.

©2026 Netcraft Ltd.

3 Self-assess against the six SPF principles

The six SPF principles form the foundation of the framework. For each checklist item, record whether it is "Met," "Partially met," or "Not met," note the evidence that supports your assessment, and identify the accountable owner.

The principles don't all carry the same regulatory weight. Prevent, Detect, Disrupt, and Respond sit within the highest civil penalty tier, while Govern and Report carry Tier 2 penalties. That doesn't make the latter optional — strong governance and reporting underpin the other four principles — but the tiers indicate where the financial exposure is greatest.

©2026 Netcraft Ltd.

Govern

Tier 2 (up to AUD $10 million)

Governance establishes how scam prevention is managed across the organization. It defines accountability, oversight, and the processes that support the other five principles.

- [ ] **Is there a documented scam governance framework with clear ownership, reporting lines, and defined success measures?**

  Evidence to look for: Governance framework, reporting dashboard, executive sign-off
  Suggested owner: Compliance

- [ ] **Is responsibility for scam risk embedded within broader organizational risk management and executive oversight?**

  Evidence to look for: Risk committee charter, board reporting, governance documentation
  Suggested owner: Compliance/Legal

- [ ] **Do employees receive regular training on scam identification and prevention?**

  Evidence to look for: Training records, completion rates, awareness programme documentation
  Suggested owner: Compliance/HR

- [ ] **Is your scam risk assessment updated to reflect your services, customers, and recent activity?**

  Evidence to look for: Current scam risk assessment, review schedule, risk register
  Suggested owner: Fraud Operations/Risk

©2026 Netcraft Ltd.

Prevent

Tier 1 (up to AUD $50 million)

The Prevent principle focuses on reducing customers' exposure to scams before harm occurs. That includes protecting your own services as well as reducing opportunities for criminals to impersonate your organization.

☐ **Are customer accounts, systems, and data protected through appropriate technical and operational controls?**

Evidence to look for: Security controls, penetration test reports, vulnerability management records

Suggested owner: Security

☐ **Do you monitor and act against lookalike domains, phishing infrastructure, and brand impersonation targeting your customers?**

Evidence to look for: Brand monitoring records, takedown requests, phishing investigations

Suggested owner: Fraud Operations/Security

☐ **Is third-party and supply-chain scam exposure included within your prevention programme?**

Evidence to look for: Third-party risk assessments, supplier assurance documentation

Suggested owner: Security/Vendor Risk

Netcraft insight

Preventing scams isn't limited to protecting your own environment. Draft sector codes make clear that organizations are also expected to reduce opportunities for criminals to impersonate their brands.

In practice, that means monitoring and disrupting phishing sites, lookalike domains, and other malicious infrastructure before customers encounter them.

©2026 Netcraft Ltd.

Detect

Tier 1 (up to AUD $50 million)

Detection is about identifying scam activity early enough to reduce customer harm and support timely disruption.

☐ **Can you identify scam activity before it is reported by customers?**

Evidence to look for: Detection workflows, monitoring dashboards, alerting rule
Suggested owner: Fraud Operations

☐ **Can you determine which customers have already been exposed to a detected scam?**

Evidence to look for: Case management records, customer impact assessments
Suggested owner: Fraud Operations

☐ **Do you measure how quickly scam activity is detected and escalated for action?**

Evidence to look for: Detection metrics, SLA reporting, incident timelines
Suggested owner: Security Operations

Netcraft insight

Detection only creates value if it leaves time to act. The sooner phishing infrastructure or impersonation campaigns are identified, the more of the response window remains.

Industry takedown times set a useful benchmark: Netcraft records a median of **33 minutes** to remove phishing sites through its registrar-backed programs. Measuring your own detection-to-takedown time against a figure like that shows whether your response window is measured in minutes, hours, or days.

©2026 Netcraft Ltd.

Disrupt

Tier 1 (up to AUD $50 million)

Once a scam has been identified, organizations need clear processes for reducing or removing the infrastructure behind it.

☐ **Do takedowns and account restrictions follow a documented approval and escalation process?**

Evidence to look for: Phishing takedown procedures, escalation workflows, case records
Suggested owner: Fraud Operations

☐ **Do you share information with other regulated sectors when scam activity crosses organizational boundaries?**

Evidence to look for: Information-sharing procedures, partnership records
Suggested owner: Fraud Operations/Compliance

☐ **Can your disruption capability scale to respond to high-volume campaigns?**

Evidence to look for: Automation workflows, response metrics, operational runbooks
Suggested owner: Security Operations

Netcraft insight

Effective disruption depends on more than identifying malicious infrastructure. Organizations also need repeatable processes, trusted reporting channels, and the ability to act consistently at scale.

Success rate and volume are two ways to test whether disruption holds up under pressure: across more than 50,000 takedowns, Netcraft records a 99.8% success rate through direct registrar partnerships and automated workflows. Figures like these are a useful reference for whether your own disruption capability can match the pace and scale of active campaigns.

©2026 Netcraft Ltd.

Respond

Tier 1 (up to AUD $50 million)

The Respond principle focuses on how your organization supports customers affected by scams and manages dispute resolution.

☐ **Do customers have access to a documented internal dispute resolution (IDR) process for scam-related complaints?**

Evidence to look for: IDR policy, complaint handling procedures
Suggested owner: Customer Operations/Compliance

☐ **Where required, has your organization established an external dispute resolution pathway through AFCA?**

Evidence to look for: AFCA membership, dispute resolution documentation
Suggested owner: Compliance

☐ **Do you have documented procedures for coordinating across sectors during multi-sector scam incidents?**

Evidence to look for: Incident response plans, coordination procedures
Suggested owner: Fraud Operations

©2026 Netcraft Ltd.

Report

Tier 2 (up to AUD $10 million)

Reporting supports coordinated scam prevention by making actionable scam intelligence available to regulators and other organizations.

- [ ] **Can you provide actionable scam intelligence to the relevant regulator in the required format?**

  Evidence to look for: Reporting templates, submission records
  Suggested owner: Compliance

- [ ] **Can you produce scam reporting records and supporting evidence when requested?**

  Evidence to look for: Audit trail, evidence repository, reporting history
  Suggested owner: Compliance

How to use this checklist

Know your gaps. Then close them.

Use this checklist to find where you stand, then see how a brand protection program runs detection, disruption, and takedown day to day.

Read the Brand Protection Field Guide

©2026 Netcraft Ltd.

4 Score your readiness

For each checklist item, assign:

Met: 1 point | **Partially met:** 0.5 points | **Not met:** 0 points

Record your scores

Date	Your score	Maximum score
Govern		4
Prevent		3
Detect		3
Disrupt		3
Respond		3
Report		2
Overall		**18**

©2026 Netcraft Ltd.

Interpret your results

Read your results by principle, not just the total. Two organizations with the same overall score can have very different exposure profiles.

80–100%

Well positioned

Your organization has many of the controls expected under the SPF already in place. Focus on validating your supporting evidence, confirming ownership, and addressing any items marked **"Partially met."**

60–79%

Progress underway

You've established a solid foundation, but there are likely gaps that should be addressed before the framework comes into effect. Prioritize the **Tier 1 principles** while continuing to strengthen governance and reporting.

Below 60%

Additional preparation needed

Your assessment suggests there are significant gaps in your current readiness. Use your results to **prioritize remediation, assign ownership,** and **develop an implementation plan** ahead of the commencement date.

©2026 Netcraft Ltd.

5 Sector-specific obligations to watch

The six SPF principles provide the common foundation for the framework. Each designated sector also has its own exposure draft code, setting out more detailed expectations alongside a dedicated enforcement regulator.

Sector	Enforcement regulator
Banking	Australian Securities and Investments Commission (ASIC)
Telecommunications	Australian Communications and Media Authority (ACMA)
Digital platform services	Australian Competition and Consumer Commission (ACCC)

©2026 Netcraft Ltd.

Banking

The draft Banking Sector Code places particular emphasis on reducing payment scams, protecting customers, and strengthening fraud controls throughout the payment journey.

Banks are expected to:

- ☐ Implement **Confirmation of Payee** to help customers verify account names before making payments.
- ☐ Use risk-based transaction monitoring to identify high-risk payments and introduce targeted warnings or payment delays where appropriate.
- ☐ Implement biometric verification or equivalent identity controls when opening new online accounts.
- ☐ Maintain 24/7 capability to receive scam reports and act quickly to protect compromised accounts.

Focus here if you scored lower in: Prevent • Detect • Respond

©2026 Netcraft Ltd.

Telecommunications

The draft Telecommunications Sector Code focuses on reducing scam activity before fraudulent calls and messages reach consumers.

Telecommunications providers are expected to:

- [ ] Block and filter spoofed SMS messages associated with smishing campaigns.
- [ ] Monitor high-risk traffic to identify scam messaging and fraudulent call activity.
- [ ] Block spoofed inbound voice calls, including those disguising international traffic as Australian numbers.
- [ ] Maintain trace-back capabilities to identify the origin of scam communications across providers.

Focus here if you scored lower in: Prevent • Detect • Disrupt

©2026 Netcraft Ltd.

Digital Platform Services

The draft Digital Platform Services Sector Code focuses on reducing opportunities for scams to reach users through advertising, messaging services, and platform abuse.

Digital platform providers are expected to:

- ☐ Verify Australian Financial Services Licences (AFSLs) before accepting financial and investment advertising.
- ☐ Implement identity verification for advertisers and other high-risk accounts.
- ☐ Detect and remove scam advertisements, fraudulent accounts, and deceptive infrastructure in a timely manner.
- ☐ Maintain processes for responding to scam reports and sharing relevant information where required.

Focus here if you scored lower in: Prevent • Detect • Report

Using your assessment

The sector codes add detail to the six principles rather than replacing them. Your results show which draft expectations to weigh most heavily.

©2026 Netcraft Ltd.

6 What to do before the codes are finalized

Now

- [ ] Complete this readiness assessment.
- [ ] Review the exposure draft code relevant to your sector.
- [ ] Identify gaps across the six SPF principles.
- [ ] Assign an owner to every remediation activity.

Before March 2027

- [ ] Complete outstanding remediation activities.
- [ ] Confirm evidence is available for each control.
- [ ] Validate governance, reporting, and escalation processes.
- [ ] Ensure relevant teams understand their responsibilities under the SPF.

©2026 Netcraft Ltd.

Build your readiness with Netcraft

From detecting phishing campaigns to disrupting malicious infrastructure, we work with the world's largest financial institutions, technology companies, and governments to reduce online fraud and protect customers.

We help organizations put the SPF principles into practice by::

- ☐ Detecting phishing sites, impersonation campaigns, and malicious infrastructure targeting your customers.
- ☐ Disrupting attacks through direct relationships with registrars, hosting providers, and internet infrastructure providers.
- ☐ Providing actionable scam intelligence to support investigations, governance, and reporting.
- ☐ Reducing customer exposure before scams reach victims

Whether you're preparing for the March 2027 commencement date or assessing existing controls, our team can help you identify gaps, prioritize remediation, and improve operational readiness, with more than 20 years of internet threat disruption experience.

Find out how Netcraft can support your SPF program.

©2026 Netcraft Ltd.

7 Sources

The six SPF principles provide the common foundation for the framework. Each designated sector also has its own exposure draft code, setting out more detailed expectations alongside a dedicated enforcement regulator.

- Scams Prevention Framework Act 2025
- Treasury exposure drafts for the Banking Sector Code
- Treasury exposure drafts for the Telecommunications Sector Code
- Treasury exposure drafts for the Digital Platform Services Sector Code
- Guidance published by the Australian Treasury
- Guidance published by the Australian Securities and Investments Commission (ASIC)
- Guidance published by the Australian Communications and Media Authority (ACMA)
- Guidance published by the Australian Competition and Consumer Commission (ACCC)

Note: This checklist reflects the regulatory position as of July 2026. Organizations should review the latest legislation, sector codes, and regulatory guidance when assessing their SPF readiness.

©2026 Netcraft Ltd.

Connect with Netcraft today for a
faster, safer brand security strategy.

netcraft