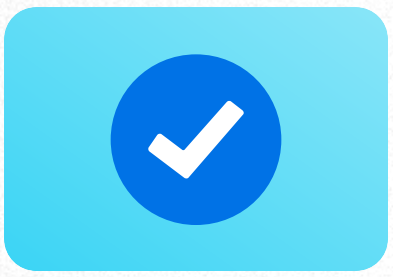
RECORDPOINT

APRA TFN Compliance Checklist

Is your organisation ready for APRA's 2026 TFN records requirements?

APRA's focus on Tax File Number (TFN) records management is intensifying. Under CPS 230, CPS 234, and CPG 235, regulated entities must demonstrate they can locate, retain, and defensibly destroy TFNs — mechanically, on an ongoing basis, and with full auditability.

This checklist helps compliance, records, and IT teams assess their current posture across four critical areas.



How to use this checklist:

1. Work through each section and tick every item your can confidently answer YES to.
2. Count your ticks at the end to determine your compliance rating.

1. Discovery and visibility

We have a complete, real-time inventory of every system or platform that may contain TFNs (SharePoint, OneDrive, Teams, Exchange, file shares, CRM, structured databases, and others). ☐

APRA expects visibility across all platforms, not just the obvious ones.

We can search for and locate TFNs across structured, unstructured, and semi-structured data in a single query, without having to manually check each system. ☐

Manual, per-system searches are not scalable and will not satisfy APRA's operational resilience requirements.

Our TFN discovery process covers image-based content (JPEGs, TIFFs, scanned PDFs) as well as text-based documents. ☐

Many TFNs enter s via scanned forms. OCR-based detection is required for complete coverage.

Our TFN detection uses algorithmic validation (not just keyword matching) to minimise false positives. ☐

Context-based validation i.e. checking for proximity of terms like 'TFN', 'Tax File Number' alongside the number, significantly improves accuracy.

New content is scanned for TFNs automatically at the point of creation or modification and not on a periodic batch basis. ☐

Real-time detection is required to demonstrate operational resilience.

We can produce a report showing the current volume and location of all TFNs across our data estate within 24 hours. ☐

If this takes longer, you are not APRA audit-ready.

Score ☐ **/6**

2. Classification and retention

- [ ] TFNs are automatically classified and assigned a retention category at the point of ingestion, without requiring end users to tag or declare content.

  End-user-dependent classification will fail at scale. Automation is essential.

- [ ] Retention periods for TFNs are tied to a specific triggering event (e.g. application date, onboarding completion), not just a fixed date from document creation.

  APRA requires TFNs to be retained only for as long as they are needed to perform their designated function.

- [ ] Retention schedules are consistently applied across all platforms, not just our primary document management system.

  A TFN in a OneDrive folder must be subject to the same retention rules as one in your CRM.

- [ ] We have a documented and enforceable retention schedule for TFNs that is aligned to APRA guidance and the Privacy Act.

  Policy documentation alone is insufficient as the schedule must be operationally enforced.

- [ ] We can demonstrate that our retention process has been running continuously, not just in response to an APRA inquiry.

  Operational resilience under CPS 230 requires ongoing, automated processes, not ad hoc responses.

Score ☐ /5

3. Disposal and auditability

- [ ] When TFNs reach the end of their retention period, they are routed through a formal disposal workflow with designated approvers, not deleted manually or informally.

  Defensible disposal requires a documented, auditable process — not a delete key.

- [ ] Every disposal event is logged with a full audit trail: who approved it, when it occurred, what was destroyed, and why.

  This log must be retained even after the content is destroyed.

- [ ] A stub or record of each destroyed item is retained post-disposal so we can demonstrate to APRA that we held the content, retained it appropriately, and destroyed it for documented reasons.

  'We deleted it' is not a sufficient answer. You need to show why and when.

- [ ] Our disposal process reaches into all connected platforms, not just our primary records system to remove content from SharePoint, OneDrive, file shares, CRMs, and other systems simultaneously.

  Destroying a document in one system while it remains accessible in another creates ongoing exposure.

- [ ] We have disposed of ROT (redundant, obsolete, and trivial) data that contains TFNs and can demonstrate this to APRA.

  Organizations carrying excess TFN records have a larger breach surface and greater regulatory exposure.

Score ☐ /5

4. Reporting and APRA audit readiness

We have a real-time dashboard showing our current TFN risk posture — including volume by platform, risk score, and trend over time. ☐

APRA wants to see that you are actively monitoring, not just reacting.

We can generate an APRA-ready evidence package, including TFN inventory, risk profile, disposal records, and retention schedule within 24 hours of a request. ☐

If this takes weeks, you are not operationally resilient by APRA's definition.

We can demonstrate that our TFN risk profile has improved over time. ☐

Trend data is one of the most powerful indicators of a mature, proactive governance programme.

Our TFN compliance posture is visible to senior leadership (e.g. CRO, CDAO, Board), not just to the records or IT team. ☐

APRA expects board-level accountability for information security and data governance.

We have documented evidence that our TFN governance processes have been tested under our BCP and scenario analysis requirements (for institutions subject to the January 2026 CPS 230 deadline). ☐

Business continuity testing of data governance processes is now an explicit APRA requirement.

All third-party service provider contracts that involve TFN handling have been updated to align with APRA's 2026 requirements. ☐

The January 2026 deadline for pre-existing contractual arrangements applies to all regulated entities.

Score ☐ **/6**

Your compliance rating

Total score ☐ **/22**

High Risk	0 – 10 (below 50%)	Significant exposure. Immediate action required before your next APRA interaction.
Moderate Risk	11 – 16 (50–72%)	Gaps exist that APRA is likely to identify. Prioritise the areas where you scored lowest.
Low Risk	17 – 19 (77–86%)	Strong foundation. Address remaining gaps to reach full audit readiness.
Audit Ready	20 – 22 (90–100%)	You are operating at best practice. Maintain and evidence your processes continuously.