



EDB POSTGRES® AI · MIGRATIONS

Migrating from Sybase (SAP ASE): A compliance brief

SAP's published maintenance schedule for ASE, mapped to the language your compliance and audit teams already use.

SAP's own schedule sets the clock

ASE 16.0 leaves mainstream maintenance on December 31, 2027. Under PCI DSS, the remediation plan is due well before that.

Most of the pressure to migrate off Sybase gets framed in engineering terms: schema conversion, procedural code, timeline. That framing rarely moves a compliance or audit stakeholder. This brief translates the same fact, SAP's own published maintenance schedule for ASE, into the standards language a PCI assessor or SOX auditor already uses.

The headline is a planning deadline, not an emergency. ASE 16.0 is in mainstream maintenance today and stays there until the end of 2027. PCI DSS asks for an approved remediation plan as soon as a vendor has announced end-of-life dates, and a phased ASE migration typically runs 20 to 44 weeks. The work to plan and fund the move belongs in this year's cycle.

2027

ASE 16.0 end of mainstream maintenance,
December 31

12

Months: PCI DSS v4.0.1 technology review
cycle, Requirement 12.3.4

20–44

Weeks: phased ASE migration planning
range, zero cutover downtime

Sources: SAP Note 1922006; PCI Security Standards Council, PCI DSS v4.0.1; EDB migration engineering estimates, compiled from completed customer engagements, 2026 (internal; actual ranges vary by estate and are confirmed during assessment).



Two versions, two dates, one direction

SAP's published maintenance schedule draws the line by version.

VERSION	END OF MAINSTREAM MAINTENANCE	STATUS, OCTOBER 2026	WHAT IT MEANS
SAP ASE 16.0	December 31, 2027	In mainstream maintenance	About 15 months of standard patches and security fixes remain. Plan the move so it completes inside that window.
SAP ASE 16.1	December 31, 2030	In mainstream maintenance	A longer clock on the same path. Moving to 16.1 defers the platform decision; it does not remove it.

Source: SAP Note 1922006, EoMM Dates for Adaptive Server Enterprise 15.0.3, 15.5, 15.7, 16.0 and 16.1.

If your environment runs ASE 16.0, the table above is the headline finding of this brief: the date is published, it is the vendor's own, and it is close enough to plan against now.

If you have already moved to 16.1, treat the rest of this document as a preview of a conversation you will have again before 2030.

Support package level matters too

Mainstream maintenance covers supported support packages, not every build of a release. SAP KBA 3785425 covers ASE 16.0 SP03 leaving maintenance and recommends SP04 or 16.1.

Confirm which support package each ASE instance runs: an instance on an out-of-maintenance package may already be missing fixes, even though 16.0 itself is still maintained.



PCI DSS asks for the plan now

This section applies only where the ASE environment stores, processes, or transmits cardholder data. Confirm scope with your QSA before assuming it applies.

1 Requirement 12.3.4: annual technology review

At least once every 12 months, review the hardware and software in use, including whether each technology still receives security fixes from its vendor promptly. Where a vendor has announced end-of-life plans, document a remediation plan approved by senior management. Mandatory since March 31, 2025.

2 Requirement 6.3.3: patch timeline

Critical security patches must be installed within one month of release. ASE 16.0 on a maintained support package can meet this today. After December 31, 2027, standard patches stop, and meeting it depends on whatever extended maintenance you can negotiate.

What this means for a 16.0 estate

The two requirements fit together. The next annual review under 12.3.4 records ASE 16.0's published end of mainstream maintenance, which triggers the obligation to document an approved remediation plan. Requirement 6.3.3 is the reason the plan needs a date: once standard patches stop, the patching requirement gets harder to meet with every month the instance stays in place.

This is a reading of the standard's own text, not a subjective risk call. Your QSA makes the final determination for your environment.

Source: PCI Security Standards Council, PCI DSS v4.0.1, Requirements 12.3.4 and 6.3.3. PCI DSS v4.0 was retired on December 31, 2024.



Under SOX, it is an audit conversation

SOX doesn't name specific software, vendors, or patch windows, so there is no equivalent bright-line rule. What Section 404 does require is effective internal control over financial reporting, and patch management, including vendor-supported software status, is one of the standard IT general control areas auditors examine.

If the ASE instance supports a system relevant to financial reporting, its support status is a natural line item in an ITGC discussion. It is not an automatic finding.

For illustration only: the 2017 Equifax breach exploited a known Apache Struts vulnerability for which a patch had been available for months, as the U.S. Government Accountability Office documented in 2018. It shows how unpatched infrastructure becomes a board and audit conversation; it is not a claim that any two situations carry the same risk.

The honest framing

Neither SOX nor PCI DSS sets a migration date. PCI DSS 12.3.4 requires a documented, approved plan; SOX asks whether your controls are effective.

An auditor asking about patch management is likely to ask about ASE's support status directly, and "we know, and here is our documented plan" is a materially better answer than not having one.

Where EDB fits

- **Documented tooling for schema and data.** EDB Migration Toolkit supports SAP ASE 15.7 and 16.0 as a source, migrating into EDB Postgres® AI (EDB PG AI). It moves schemas, tables, constraints, indexes, and data. Stored procedures, triggers, and views are rewritten in PL/pgSQL, and an assessment scopes that rewrite, which is the timeline input a 12.3.4 remediation plan needs.
- **A published support lifecycle.** EDB publishes support end dates for each EDB PG AI release, generally five years from availability, so the next version decision is one you can plan for.
- **A path to AI, not just off ASE.** The same migration lands transactional workloads on a platform that already supports vector search and agentic AI: one move, not two.

Sources: EDB Migration Toolkit documentation (supported platforms; object migration support by source database); EDB platform compatibility and database version policy.



Suggested next steps

1

Confirm scope

Check with your compliance or QSA team whether the ASE environment is in scope for PCI DSS (cardholder data) or supports a SOX-relevant financial reporting system.

2

Start the remediation plan now

PCI DSS 12.3.4 requires a senior-management-approved plan once a vendor has announced end-of-life dates, whichever target platform you choose. This step isn't EDB-specific and doesn't need to wait on a vendor decision.

3

Run a schema assessment

Scope the migration effort against your real estate. That scope, especially the size of the procedural tier, becomes the timeline in the remediation plan.

4

Bring in a migration architect

Review the assessment findings with an EDB migration architect before committing to a date.

Request an assessment

Contact your EDB account team, or reply to the EDB representative who sent you this brief.

enterprisedb.com/contact

Sources

- SAP Note 1922006, EoMM Dates for Adaptive Server Enterprise 15.0.3, 15.5, 15.7, 16.0 and 16.1 — SAP ASE 16.0 end of mainstream maintenance December 31, 2027; SAP ASE 16.1 end of mainstream maintenance December 31, 2030.
- SAP KBA 3785425 — SAP ASE 16.0 SP03 end of maintenance; recommends SP04 or 16.1.
- PCI Security Standards Council, PCI DSS v4.0.1, Requirements 12.3.4 and 6.3.3.
- Sarbanes-Oxley Act of 2002, Section 404, and standard IT general controls (ITGC) audit practice.
- U.S. Government Accountability Office, Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach (GAO-18-559), August 2018.
- EDB Migration Toolkit documentation — supported platforms and databases; overview and object migration support (enterprisedb.com/docs/migration_toolkit).
- EDB platform compatibility — product support end dates (enterprisedb.com/resources/platform-compatibility).
- EDB migration engineering estimates, compiled from completed customer engagements, 2026 (internal; actual ranges vary by estate and are confirmed during assessment).



Put the plan on paper before the patches stop.

SAP's schedule is published. The plan PCI DSS asks for is due now, and the runway to finish the move is long enough only if it starts this year.

This brief is provided for informational and internal-planning purposes only and does not constitute legal, audit, or compliance advice. EDB is not a law firm, auditor, or Qualified Security Assessor. Consult your own compliance, legal, and QSA advisors to determine how PCI DSS, SOX, or any other regulatory framework applies to your environment. Timeline ranges are planning estimates that vary by environment. SAP, Sybase, and SAP ASE are trademarks of SAP SE. PCI DSS is a trademark of PCI Security Standards Council, LLC. Postgres and PostgreSQL are registered trademarks of the PostgreSQL Community Association of Canada and used with their permission. EDB Postgres® AI is a trademark of EnterpriseDB Corporation. © EnterpriseDB Corporation 2026. All rights reserved.

EDB Postgres® AI is the first open, enterprise-grade sovereign data and AI platform, with a secure, compliant, and fully scalable environment, on premises and across clouds. Supported by a global partner network, EDB Postgres AI unifies transactional, analytical, and AI workloads, enabling organizations to operationalize their data and LLMs where, when, and how they need them. For more information, visit enterprisedb.com.

