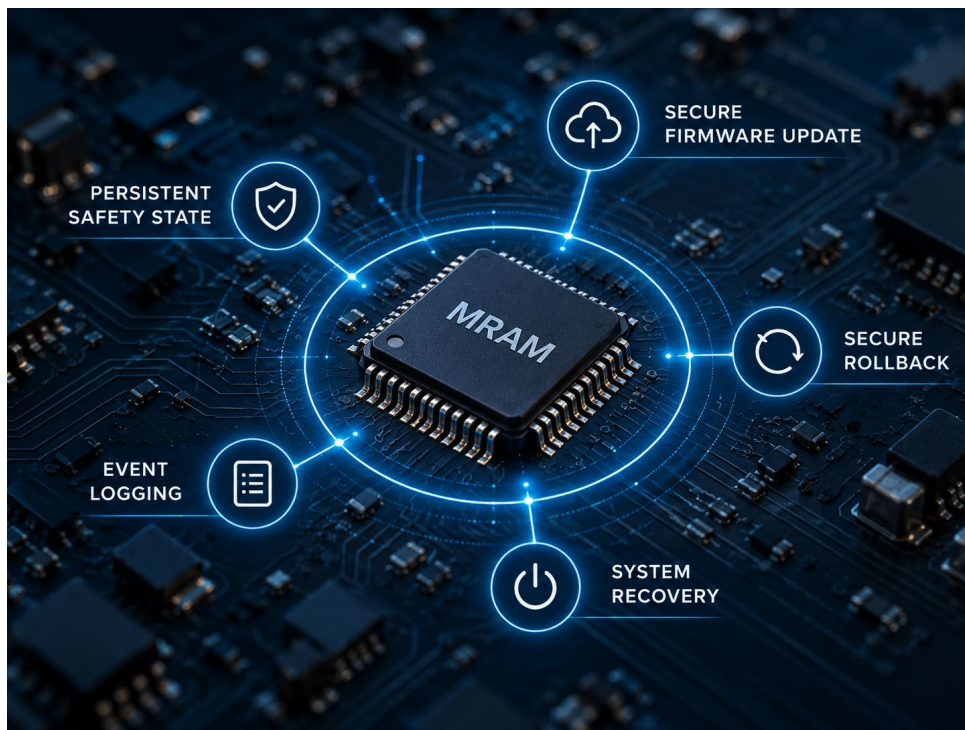


Memory Chips and the Cyber Resilience Act: What Manufacturers Need to Know and Where MRAM Helps



The EU Cyber Resilience Act has moved from something teams were watching to something they are actively planning for. Reporting obligations took effect on Sept. 11, 2026, and the main product requirements apply beginning Dec. 11, 2027. If you build products with digital elements for the EU market, the CRA is now a practical design consideration.

For engineers selecting memory, that raises a practical question: does the CRA mean every memory component now needs its own cybersecurity certification?

The short answer is no, and it is worth understanding why.

Do Memory Chips Require Third-Party Assessment under the CRA?

Memory chips are explicitly listed by the European Commission as an example of the CRA's default product category. For products in that category, manufacturers may use self-assessment rather than a mandatory third-party assessment by a notified body; see the Commission's official conformity-assessment guidance.

That does not mean an in-scope memory chip is exempt from the CRA. The manufacturer can use self-assessment to demonstrate conformity, and the associated obligations still apply.

The CRA also recognizes that component suppliers and finished-product manufacturers have different roles. When an in-scope product is intended for integration into another product with digital elements, the CRA calls for information that the integrator needs to address the applicable cybersecurity and documentation requirements. The manufacturer of the finished product remains responsible for demonstrating that the product it places on the market conforms.

For the system designer, the bigger CRA challenge is the finished product and how it implements applicable cybersecurity requirements across the architecture. That is where memory selection starts to become relevant.

Where Memory Enters the System Design

The CRA's essential requirements are about product cybersecurity outcomes. Among other things, and where applicable based on the manufacturer's risk assessment, products with digital elements are expected to protect the integrity and confidentiality of stored data, protect the availability of essential functions and record or monitor relevant security-related activity. Products must also be able to address vulnerabilities through updates over the support period.

None of those requirements name a memory technology. The CRA does not mandate MRAM, flash or anything else. Instead, it leaves implementation to the engineer, and some requirements raise system-level questions about how critical information is retained, how recovery is handled after an interruption, and how security-relevant data is recorded.

Memory architecture can be part of that discussion, alongside software, processor-level security and other system controls. The way a system stores configuration, logs events, tracks state and recovers after a power loss is shaped in part by the memory underneath it.

How can MRAM Support CRA-Related System Requirements?

MRAM does not provide CRA compliance on its own. What it can provide is a persistent memory layer for frequently updated state, recovery information, event logs and other data the larger system may depend on.

This is where Everspin's MRAM solutions matter. Everspin's Toggle and xSPI STT-MRAM products retain committed data through power loss or reset while supporting high write endurance and fast writes. Everspin's xSPI STT-MRAM also supports byte-

level writes in persistent-memory mode without requiring an erase before rewriting the same location.

In practical terms, those characteristics can support several functions that show up repeatedly in resilient system design:

- Retaining configuration and recovery state. Persistent memory can hold configuration data, recovery checkpoints and security-relevant state so the system can return to a known condition after a power loss or reset.
- Recording events and activity. High write endurance makes MRAM well suited to workloads that frequently update persistent data, such as event, fault and diagnostic records, without the erase-cycle and endurance-management considerations that frequently updated flash designs may require.
- Committing critical data quickly. Fast writes can shorten the time needed to commit state to non-volatile memory before a power interruption, assuming the system detects the event and has enough time and energy to complete the write.
- Simplifying frequent persistent updates. Write-in-place behavior lets a design update individual locations directly, without requiring an erase before rewriting the same location, as frequently updated flash designs may.

The common thread is that MRAM can persistently store the frequently updated state, configuration, recovery information and event data a system architecture may depend on.

What the Memory Provides and What the System Completes

It is worth being clear about the boundary between the memory and the rest of the system, because both matter. MRAM contributes useful physical characteristics to a secure system design. Because it is non-volatile, committed data remains available through power loss or reset. Its high write endurance and fast writes also make it well suited to counters, logs and system state that may be updated frequently over the life of the product.

What MRAM does not do on its own is complete the security functions those properties support. A full secure boot, a hardware root of trust, tamper detection and cryptographic integrity are realized at the system level, where the processor, bootloader and security software authenticate firmware, verify signatures, enforce policy and perform cryptographic operations. MRAM can store a cryptographic key; protecting how that key

is used is a system responsibility. In other words, MRAM can strengthen the foundation these functions are built on, but it does not replace them.

And demonstrating CRA conformity remains the responsibility of the manufacturer placing the finished product on the market. That manufacturer performs the cybersecurity risk assessment, implements the applicable Annex I measures, prepares the technical documentation and completes the conformity process for the product it places on the market. Memory selection is one input to that work, not a substitute for it.

The Practical Takeaway

For memory chips in the CRA's default category, manufacturer self-assessment is permitted rather than mandatory third-party assessment.

The remaining question is whether the memory architecture supports the functions the finished system needs, including persistent state, recovery information or frequently updated event data. When the system must reliably retain data, recover after an interruption or record relevant events, the underlying memory matters. MRAM's non-volatility, endurance and write performance can simplify implementation of some of those functions, while the system-level security controls and the manufacturer's conformity work remain where the CRA puts them.

If you are working through what the Cyber Resilience Act means for the memory in your design, our team is happy to talk through where MRAM does and doesn't fit.