

The UK Cyber Security and Resilience Bill is not just another regulatory update, it represents a significant expansion of accountability, scope and reporting obligations, for which many organisations are not yet ready

Get *ahead of the* CYBER SECURITY *and resilience* bill

Picture the scenario: A Security Manager of an organisation is responsible for physical access to multiple sites. Visitors and contractors come and go. Employees change roles. Permissions accumulate over time because revoking them manually is slow, error-prone and nobody quite owns the process end-to-end. Meanwhile, the compliance team is trying to produce an audit trail for a regulator and realises that the data is spread across three different systems, none of which talk to each other.

This is the reality for many organisations today and it is precisely the kind of gap that the UK Cyber Security and Resilience (CS&R) Bill, introduced in Parliament in November 2025, is designed to close. It is designed to strengthen the security and resilience of essential and digital services more broadly, not only critical national infrastructure.

"Physical Identity & Access Management (PIAM) platforms are specifically designed to close the gap between physical and digital security."

Broadly aligned with the EU's NIS2 Directive, the Bill dramatically raises the bar for cybersecurity governance, incident



reporting and organisational accountability. For those operating across the UK and EU, compliance with both frameworks is required simultaneously.

The pressure on security and compliance teams

The CS&R Bill is not a distant concern. It is progressing through Parliament and expected to become law in 2026, although full compliance obligations are likely to be phased in over the following years. This means that the organisations it affects, including managed service providers and designated critical suppliers newly brought into scope, are already being asked by clients and auditors to demonstrate compliance readiness.

Fines for non-compliance can reach several million pounds, or a significant percentage of global annual turnover, for serious breaches.

For Security Managers and Compliance Officers, the Bill creates four concrete pressure points:

- **Proving who has access to what and why:** Role-based access controls must be documented, enforced and auditable across all sites and systems.
- **Fast incident reporting:** The Bill requires an early warning to the relevant regulator and the National Cyber Security Centre (NCSC) within a very short window of becoming aware of a significant incident, followed by a fuller report shortly after. Without consolidated, real-time reporting data, meeting these deadlines is extremely difficult.
- **Demonstrating board-level accountability:** Senior leadership must be actively engaged in cyber-risk governance, which also requires them to look into physical access risk. Security teams need to be able to brief the board clearly and produce evidence of oversight across both digital and physical systems.
- **Managing third-party and supply chain risk:** Contractors, visitors and service providers/ suppliers must be managed with the same rigour as employees. Yet in most organisations, they fall through the gaps.

The blind spot: physical security

When organisations think about cybersecurity compliance, they typically focus on firewalls, endpoint protection and access controls within their IT systems. Physical security is often treated as a separate concern, managed by a different team, using different tools and reporting to a different part of the business.

This separation is a compliance risk in itself. An employee whose role changed six months ago may still have physical access to a server room. A contractor whose engagement ended may still hold an active credential. These are not hypothetical edge cases; they are everyday realities in organisations that manage access through disconnected systems and manual processes.

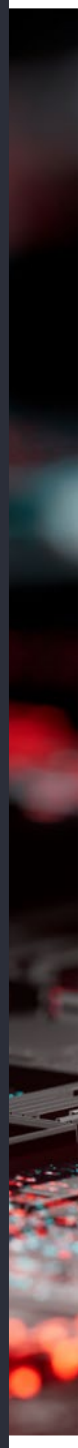
Under the CS&R Bill, these gaps are no longer just operational inconveniences but represent demonstrable failures in risk management and governance.

How a modern PIAM platform addresses these challenges

Physical Identity & Access Management (PIAM) Platforms are specifically designed to close the gap between physical and digital security.

A modern PIAM Platform, such as the PIAM Suite from ID-ware, integrates directly with existing HR and access control systems as well as further third-party system environments, e.g. parking management, payment and locker systems. ▸

> **"The UK Cyber Security and Resilience Bill is a clear signal that siloed approaches to security between physical and digital are no longer adequate."**





When an employee's role changes or a contractor's engagement ends, permissions are updated or revoked automatically, across all connected systems and all sites of an organisation. This eliminates the manual follow-up that security teams currently rely on and rarely have time to complete consistently.

How this directly addresses the four pressure points created by the CS&R Bill:

1. Proving access controls: from spreadsheets to certainty

A PIAM Platform enforces role-based access, ensuring that only authorised persons can enter security-sensitive areas – no matter which access control system from which manufacturer is installed in which building or at which site. Every permission granted, changed, or revoked is logged automatically.

For security managers, this replaces error-prone manual processes with a reliable, auditable system. For compliance officers, it means being able to answer the question "Who had access to what and when?" in minutes rather than days.

2. Meeting tight reporting deadlines

One of the most demanding aspects of the CS&R Bill for compliance teams is the short early-warning deadline. When an incident occurs, there is no time to manually collect and evaluate data from disparate systems.

A PIAM Platform continuously captures data from all connected systems and can generate comprehensive incident reports at speed. Building occupancy data, access logs and identity records are all available in a single place, giving compliance teams the information they need to notify the NCSC and the relevant regulator within the required timeframe.

3. Giving the board what it needs

The CS&R Bill places cybersecurity governance firmly at board level, and that governance is incomplete without visibility into physical access risk: an unmanaged badge or server room credential is as much a route into critical systems as a compromised digital login. Security and compliance teams are expected to brief senior leadership clearly and produce evidence of oversight across both.

> **"Fines for non-compliance can reach several million pounds, or a significant percentage of global annual turnover, for serious breaches."**

A PIAM Platform closes this gap by providing organisation-wide visibility of all physical identities, credentials and access permissions across every site and system, in a format that is clear and auditable. Security managers can demonstrate control, and compliance officers can evidence governance, including the physical dimension of cyber risk that boards often overlook.

4. Closing the third-party gap

External staff, contractors and visitors are among the most common sources of unmanaged physical access risk. A PIAM Platform manages all categories of identity, not just employees, with the same rigour and the same automated workflows.

When a contractor's assignment ends, their access is revoked. When a visitor is registered, their permissions are restricted to the necessary minimum and are time limited. Supply chain risk, one of the CS&R Bill's central concerns, becomes manageable rather than a persistent blind spot.

A practical path to compliance

One of the practical concerns for security and compliance teams is the overhead of deploying and maintaining new infrastructure. When used as a Software-as-a-Service (SaaS) solution, a PIAM Platform removes this burden entirely.

Data is held in a certified European data centre; the system is maintained by the provider; and updates are rolled out automatically. Organisations benefit from enterprise-grade security without the complexity and investments of on-premises deployment.

Security and compliance cannot afford to work in silos

The UK Cyber Security and Resilience Bill is a clear signal that siloed approaches to security between physical and digital are no longer adequate.

Organisations that bring these functions together, underpinned by a PIAM platform that provides a single, authoritative view of physical identities, credentials, access permissions and incidents, will be far better placed to meet the Bill's requirements, respond to incidents under pressure and demonstrate the kind of governance that regulators and boards now expect.

Cyber-physical convergence, the merging of cybersecurity and physical security, is no longer a future ambition. For organisations subject to the CS&R Bill, it is fast becoming a compliance necessity. ■