WHITEPAPER

Streamline regulatory compliance to protect sensitive data

imprivata®

Executive summary: Why regulatory compliance matters to you

The continued threat from cyberattacks and the potential impact on critical infrastructure is forcing many countries and individual industries to introduce regulations and legislations to provide common levels of cybersecurity.

To address enhanced and evolving cybersecurity issues, regulations are particularly targeted at operators of essential services which provide such services into critical sectors such as healthcare, energy, transport, banking, and digital infrastructure who must comply with enhanced cybersecurity and incident reporting requirements.

The major elements of cybersecurity regulation which may affect your organisation include:

- Industry sectors are covered so your organisation may be affected and required to be compliant
- Rigorous cybersecurity and risk management requirements including coverage of supply chain security and risks
- Strict cybersecurity incident reporting and deadlines
- Personal liability and costly sanctions if the rules are not followed

Cybersecurity obligations for organizations include risk and supply chain management, cyber incident reporting, and information sharing. To comply with these requirements, organizations will need to deepen and widen their focus on cybersecurity and implement new policies, procedures, and solutions.

A short summary of the evolution cybersecurity regulations

Our usage and reliance on IT systems in all parts of society, the economy, and our personal lives has grown rapidly in the last decade. Our increasing dependence on these networks and information systems, which often cross organisational and national boundaries, has been recognised by industry regulators and national governments. The services provided by such systems underpin the functioning of today's society. It is clear that protecting their security and reliability is essential.

With this aim in mind, governments and regulators have established cybersecurity standards defining minimum levels of security and also protecting the functioning of the markets that these organizations serve. Many of these regulations are also enshrined in, or in the process of being adopted in, countries' respective legal frameworks including within the USA and EU.

The challenge for organizations

The level of fines and personal liability for executives that regulation can bring means that cybersecurity should be firmly on the board agenda, not as a one-off item but as an ongoing topic to be regularly monitored, managed, and funded. Failure to do this could result in security breaches leading to large fines, lost business, and reputational damage.

With the clock ticking to implement minimum levels of cybersecurity protection, here are the key challenges for organizations:

- Many more organizations, by size and industry sector, are now being covered by regulations and will therefore be forced to give more serious focus to cybersecurity, some perhaps for the first time, requiring new policies, procedures, solutions, and skills
- Organizations will need to cast a wider net to look at supply chain risks, resilience, and security
- There will be a need to manage vendors and other third parties more stringently
- To keep or win business, organizations will need to be able to show their cybersecurity credentials to customers
- Organizations will have to keep abreast of what is required where and when and of updates and changes as regulation is introduced and evolves
- Organizations based outside of, but supplying, certain industries and/or countries may need to comply with specific regulation as well as those from their own nation/industry which may be different and diverge further over time

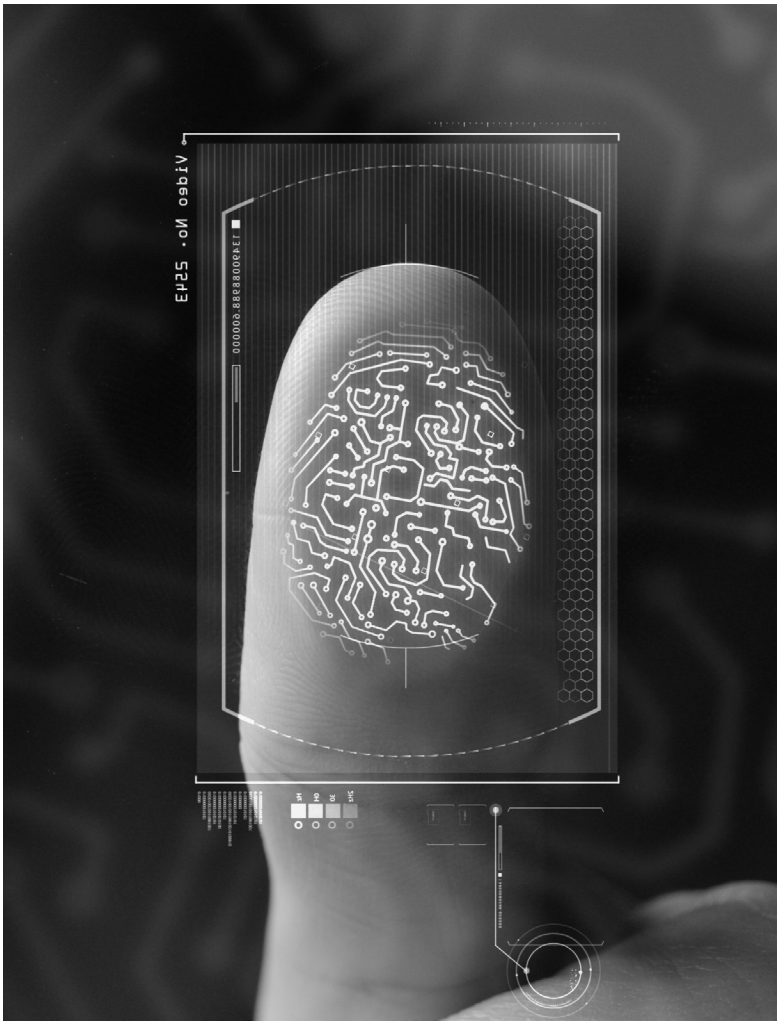
Organizations need to get ahead of the game and start now to be able to comply with the upcoming legal changes, and even to gain competitive advantage by being able to prove the quality of their cyber credentials over other suppliers.

"2023 has already seen cyber threats to supply chains and data compromised by attacks via third-party suppliers. Perhaps the most high-profile attack saw hackers using a critical flaw in Progress Software's MOVEit file transfer tool, used by thousands of organizations and as many as 3.5 million software developers.

As of August 2023, it has been reported that over 950 organizations and well over 50 million individuals all around the world have been affected. Organizations include Deutsche Bank, British Airways, SNCF, Siemens Energy, BBC, and Aer Lingus. In many cases, organizations' own systems were not compromised but their data was stolen and held to ransom due to the use of the third-party tool."

Andy Wilcox, Senior Product Marketing Manager, Imprivata

Identity is the key to cybersecurity



Building a cybersecurity strategy can often feel like a daunting task due to the fact that cyber threats are constantly evolving and expanding in scope. However, many of the greatest threats are based on identity and involve attacks that exploit vulnerabilities related to user identities, credentials, and access rights – so a focus on identity management is a good anchor for an enhanced cybersecurity strategy.

According to the 2023 Trends in Securing Digital Identities report from the Identity Defined Security Alliance (IDSA), 90% of organizations experienced at least one identity-related breach in the past year. Insider threats, phishing and identity spoofing are just some of the types of identity-related attack methods that require constant vigilance to protect identity and ensure that only the right people gain access to systems and data.

There is now an increased importance in identity as it expands beyond humans to include machine and device identity as the number of connections increases, supercharged by the Internet of Things (IoT). The increase in remote working, use of cloud applications, and inter-connected supply chains expands the threat horizon beyond organisational boundaries. Weaknesses can and will be exploited by bad actors.

Common cybersecurity threats related to identity

Phishing	Phishing attacks involve sending fraudulent emails or messages that appear to be from a legitimate source, with the goal of tricking users into revealing their credentials, personal information, or financial details.
Credential theft	Attackers may use various methods, such as keyloggers, malware, or social engineering to steal usernames and passwords. Once stolen, these credentials can be used to gain unauthorised access to systems and sensitive data.
Password spraying and brute force attacks	Attackers attempt to guess passwords by systematically trying common or weak passwords. In password spraying attacks, they target a large number of accounts with a few common passwords. Brute force attacks involve trying all possible combinations until the correct one is found.
Insider threats	Insiders with malicious intent or inadvertently compromised credentials can pose a significant threat. This can include employees, contractors, or partners who abuse their access privileges to steal data, introduce malware, or disrupt systems.
Identity spoofing	Attackers might impersonate legitimate users or devices by using stolen or forged credentials, aiming to gain unauthorised access or bypass security measures.
Man-in-the-middle (MitM) attacks	In such attacks, attackers intercept communications between two parties, potentially stealing sensitive information, such as login credentials or payment details.
Session hijacking	Also known as session fixation, this attack occurs when an attacker takes over an active user session to gain unauthorised access to a system or application.
Credential reuse	If users reuse passwords across multiple accounts, a breach in one system can lead to attackers gaining access to other accounts as well.

Pharming	Attackers manipulate the domain name system (DNS) to redirect users to fraudulent websites, where their login credentials and personal information can be stolen.
Identity and access management (IAM) vulnerabilities	Poorly managed user identities and access controls can lead to unauthorised users gaining access to sensitive systems and data. Misconfigured IAM settings can also expose organizations to risks.
Ransomware	Ransomware attacks can lock users out of their systems until a ransom is paid. Attackers might gain initial access through compromised credentials or other means.

To address such threats, organizations should adopt strong cybersecurity practices, including multifactor authentication (MFA), regularly updated security training and alerts for employees and supply chain partners, least privilege access policies, continuous monitoring of user activities, and robust identity and access management systems.

The EU Agency for Cybersecurity, **enisa, has identified the top 10 emerging global cybersecurity threats in the years up to 2030**:

- Supply chain compromise of software dependencies
- Advanced disinformation campaigns
- Rise of digital surveillance authoritarianism/loss of privacy
- Human error and exploited legacy systems within cyber-physical ecosystems Targeted attacks enhanced by smart device data
- Lack of analysis and control of space-based infrastructure and objects
- Rise of advanced hybrid threats
- Skills shortage
- Cross-border ICT service providers as a single point of failure
- Artificial intelligence abuse

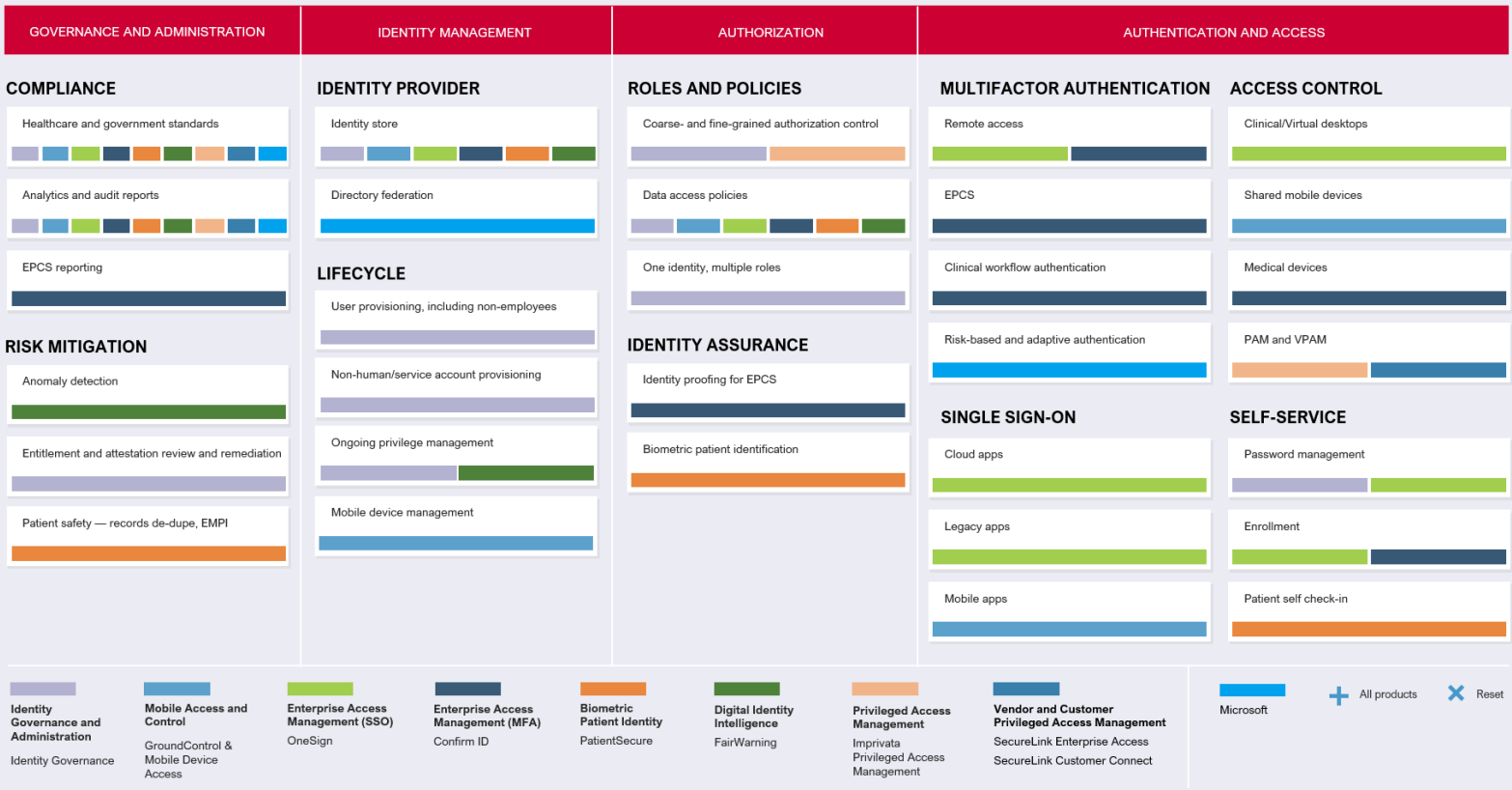
Many of these emerging threats feature identity at their heart, and so keeping the focus on identity management will help your cybersecurity strategy stay on track well into the future.

How can Imprivata help

Imprivata can help organizations meet compliance and regulatory requirements in critical industries.

Imprivata provides an overarching proactive framework of security and preparedness which is already trusted in many critical, highly regulated industries such as healthcare, financial services, and government. As a result, Imprivata can assist organizations in improving their overall security posture, reducing the risk of regulatory fines and penalties associated with regulation, and maintaining the trust of customers and stakeholders.

Imprivata Digital Identity Framework



With Imprivata, organizations can address key IAM requirements within the regulations including:

- Managing the supply chain
- Implementing basic cybersecurity hygiene
- Using role-based access controls
- Multifactor authentication

Imprivata's strong track record of working with organizations in highly regulated industries has developed a deep expertise in navigating complex regulatory environments. As a result, Imprivata can offer its customers not only industry-leading solutions, but also the guidance and support needed to implement solutions that help address key requirements of regulations.

By implementing solutions from a single vendor, such as Imprivata, organizations can simplify management, reduce the burden on IT and provide a seamless and efficient end user experience while still providing a high level of cybersecurity.

Imprivata solutions will help organizations become better placed to demonstrate regulatory compliance. This is essential as customers look for evidence that their supply chain partners are taking cybersecurity seriously. The ability to show cybersecurity preparedness can safeguard existing business relationships and help win new orders.

Why choose Imprivata for IAM to help meet regulatory requirements

A proven, comprehensive IAM solution from a single vendor providing multifactor authentication, privileged access management, identity lifecycle management, and password policy enforcement requirements.
User-friendly workflows which help deliver security without sacrificing efficiency for users, which helps eliminate shared passwords and workarounds.
Flexible authentication workflows without the need for third-party products.
Automated provisioning for appropriate, day one role-based user access to systems and data ensures that users do not inherit inappropriate access levels.
Management of privileged users and privileged access for both internal users and external vendors that need access to support and maintain critical systems.
Access management across all devices including thick client, thin client, mobile, and IoT devices ensuring users always use their own credentials.

Next steps

It is essential that organizations review their IAM strategy now, as it is a key component of a broader cybersecurity strategy, and many organizations and executives will be exposed to fines, penalties, and reputational damage if they have not put in place suitable policies, processes, and technology to meet the requirements of regulatory compliance.

Act now to assess the effectiveness of your digital identity strategy, based on current-state tools and processes, and ensure that you have adequate time to plan, prepare and implement an IAM platform to support your ongoing compliance requirements.

TAKE ASSESSMENT

imprivata®

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at 1 781 674 2700 or visit us online at www.imprivata.com

EAM-DS-streamline-regulatory-compliance-0124