WHITE PAPER

Omada

Address Evolving Data Privacy and Cybersecurity Regulations with IGA

Ensure Compliance, Streamline Audits, and Reduce Risk

Contents

Executive Summary

Digital transformation and cloud-based services are helping enterprises accelerate the pace of business and transform economics. But they also create new opportunities for threat actors and new challenges for CISOs and CSOs, including keeping pace with evolving data privacy and cybersecurity regulations. Compliance violations can tarnish a company's reputation, expose the business to costly fines and lawsuits, and sow doubt in customers and business partners. Yet many Information Security organizations rely on risk-prone, manual processes to manage user identities and access privileges, and to enforce, track, and demonstrate compliance. IT and security professionals often squander valuable time and resources sifting through spreadsheets and emails, pulling data from different systems, trying to satisfy auditors.

> "In any era of increased regulatory scrutiny and escalating cyber risk, many boards of directors are forming special cybersecurity committees led by qualified experts."

This paper reviews common data privacy and cybersecurity regulations, and explains how Identity Governance and Administration (IGA) solutions can help CISOs improve compliance, streamline audits, and mitigate risk by automating identity lifecycle management functions, and by gaining granular visibility and tight control over users and their access rights.

In any era of increased regulatory scrutiny and escalating cyber risk, many boards of directors are forming special cybersecurity committees led by qualified experts. Gartner predicts 40% of boards will have a dedicated cybersecurity committee by 2025,[1] further complicating the life of the CISO. IGA solutions can help CISOs strengthen cybersecurity, demonstrate readiness, and earn the board's trust and confidence.

Introduction

Cyberattacks are growing in complexity, frequency, and scale. The typical company was attacked 270 times in 2021, up 31% from 2020, according to a major Accenture survey.[2] Security breaches can lead to costly data theft, business disruptions, and revenue loss. In fact, the average total cost of a data breach is now estimated at $4.24 million.[3]

Record GDPR Fines

- Amazon €746 million
- WhatsApp €225 million
- Google €150 million
- Facebook €60 million

Government and industry regulators are taking notice, strengthening existing rules and introducing new regulations to protect data privacy and defend critical infrastructure against attacks. Compliance violations can result in stiff penalties, legal settlements, reputational damage—even jail time in extreme cases. But complying with data privacy rules and cybersecurity mandates is a real challenge for many Information Security organizations.

Regulations are complicated, numerous, and constantly evolving. For many organizations, implementing consistent access controls, and enforcing and auditing compliance across diverse applications, systems, and IT environments is a manually intensive, error-prone proposition that squanders resources and is fraught with risk. In an era of intelligent automation, many organizations still rely on emails and spreadsheets to garner approvals, manage access rights, and support audits.

Identity Governance and Administration solutions help organizations overcome these challenges by automating identity lifecycle management functions, continuously certifying access rights, enforcing separation of duties, and providing unified visibility across hybrid and multi-cloud environments.

1 January 28, 2001 press release
2 Attempted attacks, State of Cybersecurity Resilience 2021, Accenture
3 IBM Security Cost of a Data Breach Report 2021

Complying with Data Privacy Regulations

Data privacy laws are increasingly common in the digital world. Dozens of countries around the globe already have some form of data privacy rules in place to protect their citizens. Dozens more have legislation in the works. Data privacy mandates are also common in heavily regulated industries like healthcare and financial services. Most data privacy mandates include provisions for governing user identities and access privileges to prevent unauthorized data disclosure and modification.

"Most data privacy mandates include provisions for governing user identities and access privileges to prevent unauthorized data disclosure and modification."

Examples of data privacy regulations with identity governance implications include:

- The General Data Protection Regulation (GDPR) – a European Union directive intended to strengthen and unify data protection for individuals within the EU
- The California Consumer Privacy Act (CCPA) – a California law that aims to prevent the unauthorized disclosure of personal data
- The Payment Card Industry Data Security Standard (PCI DSS) – a global security standard intended to safeguard credit card and debit card data
- The Gramm-Leach-Bliley Act (GLBA) – a U.S. law requiring consumer financial services companies to protect confidential data
- The Health Insurance Portability and Accountability (HIPAA) – a U.S. law intended to protect patient privacy and safeguard personal data

See Appendix A for additional information on these regulations.

Complying with Cybersecurity Regulations

Many businesses are also subject to strict cybersecurity regulations intended to prevent fraud and abuse, and to protect critical infrastructure such as financial and healthcare data networks, and power and transportation systems. Most cybersecurity regulations include provisions for governing user identities and access rights to defend against service-impacting attacks and to prevent data exfiltration.

Examples of cybersecurity regulations with identity governance implications include:

- The Sarbanes-Oxley Act (SOX) – a U.S. law enacted to fight financial fraud in the wake of several prominent corporate scandals
- The Society of Worldwide Interbank Financial Telecommunication (SWIFT) Customer Security Controls Framework (CSCF) – a regulation intended to secure the global interbank messaging network
- The EU Directive on Network and Information Systems – an EU-wide cybersecurity regulation that provides guidelines for securing IT infrastructure and reporting cybersecurity incidents
- The North American Electric Reliability (NERC) Critical Infrastructure Protection (CIP) specification – a regulation that aims to protect the integrity of the U.S. and Canadian electric power grid
- The Federal Information Security Modernization Act (FISMA) – a U.S. regulation intended to strengthen the security of federal government IT systems

See Appendix B to learn more about these regulations.

Cybersecurity Frameworks

Auditors often use standard information security frameworks and architectures to evaluate cyber-readiness, assess risk, and review compliance. Some regulations like the EU NIS Directive map individual technical requirements to specific security frameworks and architectures. Other regulations like SOX don't specify technical requirements and instead give auditors the freedom to choose an appropriate security framework.

Some of the cybersecurity frameworks and architectures auditors commonly use to assess risk and evaluate readiness include:

- COBIT IT Governance Framework
- COSO Internal Control and Enterprise Risk Management Frameworks
- ISO/IEC 27001 Information Security Management Standard
- NIST Cybersecurity Framework
- NIST Framework for Improving Critical Infrastructure Cybersecurity
- NIST SP 800-207 Zero Trust Architecture

IGA Solutions Address Key Compliance Requirements

While the detailed requirements may vary from specification to specification, most cybersecurity regulations, frameworks, and architectures specify fundamental identity and access management controls, and fundamental logging, monitoring, and reporting requirements organizations must adhere to.

As a general rule, to comply with the regulations described in this paper you may need to:

- Define and document distinct roles and responsibilities for your user community
- Enforce the principles of least privilege and separation of duties
- Implement systems and practices to manage user identities and access rights throughout the lifecycle
- Regularly validate user rights to prevent privilege creep and abuse
- Produce proof of compliance to auditors

During the course of an audit, you may need to:

- Provide evidence of well-defined user roles, responsibilities, and policies
- Demonstrate robust processes and mechanisms for authenticating and authorizing users, enforcing policies, and ensuring the right users have access to the right systems and data for the right reasons
- Provide records of permission request, justification, and approval workflows to demonstrate proper oversight

Enforcing compliance and supporting audits is a struggle for many organizations. Many rely on disjointed manual processes that are inherently fallible. IT and security teams are often forced to comb through spreadsheets and email messages to cobble together evidence of compliance for auditors—an inefficient and unreliable approach, that hardly inspires confidence.

Identity Governance and Administration solutions are specifically designed to help Information Security and IT organizations efficiently manage digital identities, access rights, and entitlements across heterogenous IT environments. They can help you comply with the data privacy and cybersecurity regulations described in this paper and streamline audits by:

- Improving visibility and oversight
- Tightly controlling access to IT systems, applications, and data
- Ensuring all access rights are properly assigned and continually certified
- Providing detailed evidence of compliance to auditors

More specifically, IGA solutions can help you:

- Strengthen security and reduce risk by implementing role-based and policy-based access controls and enforcing separation of duties and least-privilege access
- Continually certify access rights are proper for each identity with template-driven certification campaigns that help to minimize the total number of questions and mitigate survey fatigue
- Improve readiness and simplify attestation with comprehensive audit trails, governance reports, and dashboards
- Simplify operations, accelerate IT service agility, and streamline onboarding by automating identity lifecycle management and provisioning functions, and unifying identity and access management across systems

The table below summarizes the key features, functions, and benefits of an IGA solution.

Feature	Function(s)	Benefits
Identity lifecycle management	• Manage user identities and access privileges throughout their tenure • Oversee rights of employees, contractors, interns, partners, etc.	• Streamline user onboarding, role changes, and exits • Avoid entitlements creep when people change roles • Identify, remove, and/or assign orphaned accounts • Easily tag and assign access rights to individual systems or data records
Continuous certification of access privileges	• Continually verify access is required and relevant • Control access to resources based on policy • Implement role-based and policy-based access controls	• Automatically validate access controls based on access surveys • Demonstrate the right people have access to the right resources for the right reasons • Prevent fraud and abuse • Adhere to least-privilege, zero-trust principles • Prevent unauthorized data disclosure and exfiltration
Separation of duties	• Segregate access privileges	• Prevent toxic combinations of access privileges[4] • Detect and resolve violations and conflicts

4 By way of example, authorizing a single accounts payable user to both approve invoices and pay invoices is often considered a toxic combination of privileges because it avoids checks and balances, and opens the door for fraud.

Reporting, logging, and monitoring	• Audit trails • Compliance dashboards • Centralized reports • Customizable reporting • Automated request and approval workflows	• Reduce risk by gaining visibility into compliance issues, violations, and irregularities • Streamline audits by providing evidence of compliance including privilege justifications through dashboards and reports • Increase insights by tracking evolving access rights over time • Improve planning by identifying applications, systems, and data subject to specific regulations • Track access request /approval flows • Identify who requested access, when, and why; and who approved/denied access, for how long, and for what reason

Conclusion

Complying with data privacy and security regulations is a burden for many CISOs. Tracking requirements, implementing the right security controls and reporting mechanisms, and dealing with auditors takes time and effort, and diverts valuable staff from other important business tasks. Compliance violations can lead to steep fines and costly lawsuits, and tarnish a company's reputation.

Identity Governance and Administration solutions can help you improve compliance, streamline audits, and mitigate risk by eliminating ineffective manual administrative processes, implementing strong access controls, and providing unified visibility over identities and access privileges.

Best-of-breed, modern IGA solutions can help you:

- Confidently comply with evolving data privacy and cybersecurity regulations
- Easily demonstrate compliance to internal and external auditors and attestation firms
- Instill confidence and trust in customers, business partners, corporate leaders and board members
- Foster a security-first culture and optimize productivity with self-service processes, automated workflows, and uniform access controls
- Improve governance, insights, and readiness with comprehensive compliance dashboards, audit trails, and reports

Learn More

Omada provides a full-featured Identity Governance and Administration solution, delivered as a Service or on-premises for ultimate simplicity, which helps customers reduce time-to-value and future-proof their organizations' identity and governance needs. The enterprise-grade, end-to-end solution lets customers automate identity lifecycle management for all identity types (employees, contractors, business partners, customers, privileged users, service accounts, and more) and govern access to all on-premises and cloud-based resources from a unified platform.

Omada provides a standards-driven IGA approach based on best-practice processes and workflows that can be easily tailored to meet specific compliance, security, and business requirements. A unique integration model with an intuitive configuration wizard lets you quickly and effortlessly connect the Omada solution to hundreds of applications, systems, and authoritative sources. The solution includes informative dashboards, including the Compliance Workbench, reports, and audit trails to help you assess risk, improve readiness, and demonstrate compliance.

To learn how Omada solutions can help your organization ensure compliance, streamline audits, and reduce risk, check us out at OmadaIdentity.com/solutions/compliance.

Appendix A: Data Privacy Regulations

EU Government Data Protection Regulations

General Data Protection Regulation (GDPR) is a European Union directive intended to strengthen and unify data protection for individuals within the EU. Enacted in 2018, GDPR is one of the first and most well-known consumer data privacy regulations. Articles 25 and 32 of the directive mandate that any entity that collects or processes data from EU residents must implement appropriate technical and organizational measures to safeguard personal data. Any company that offers consumer goods or services in the EU must comply with the regulation and should conduct regular compliance audits as a best practice. GDPR violations have resulted in some of the largest compliance fines in history, including a record €746 million ($888 million) fine levied against Amazon in 2021.

US Government Data Protection Regulations

Data privacy is regulated at the state level in the United States. In 2020, California became the first state to legislate consumer data protection with the introduction of the California Consumer Privacy Act (CCPA). Among other requirements, the law compels businesses to put controls in place to prevent the unauthorized disclosure of personal data.

Virginia, Colorado, and Utah all passed data privacy regulations in the wake of CCPA. A dozen other states have legislation in progress. The International Association of Privacy Professionals Tracker keeps tabs on the status of data privacy legislation in all 50 states.

Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) is an international security standard intended to safeguard credit card and debit card data. Any business that accepts major payment cards and stores, processes, or transmits cardholder data electronically must follow the PCI DSS guidelines. PCI DSS Version 4.0, introduced in 2022, specifies a series of network and system security best practices including strong access control measures and multifactor authentication methods to prevent threat actors from breaching IT systems and stealing cardholder data.

All of the major payment card brands require large merchants to conduct an annual compliance audit and demonstrate they properly identify and authenticate users, and restrict access to system components and cardholder data on a need-to-know basis. Smaller businesses must complete an annual self-attestation questionnaire to demonstrate compliance.

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA) is a 1999 U.S. federal law requiring businesses offering consumer financial services such as loans, investment advice, or insurance to protect confidential data. Businesses covered by GLBA must follow the relevant U.S. Federal Trade Commission (FTC) guidelines for safeguarding customer information. The guidelines define a variety of strong authentication and access control requirements to prevent unauthorized data disclosure or modification. Financial institutions can be fined up to $100,000 per incident for GLBA violations. Any financial institution that manages consumer data should perform periodic GLBA compliance audits as a best practice.

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability (HIPAA) Act is a U.S. law primarily intended to protect patient privacy. HIPAA defines administrative and technical safeguards for monitoring and controlling access to protected health information (PHI) in electronic health record (EHR) systems and other IT systems. The statute also lays out recommended processes and best practices for auditing system and user activity, and assessing risk.

Any U.S. healthcare provider, plan administrator, or clearinghouse that stores or transmits PHI electronically must comply with HIPAA data security rules. Violations can result in fines of up to $50,000 per offense, totaling up to $1.5 million per year. The Health Information Technology for Economic and Clinical Health (HITECH) Act, signed into law in 2009, strengthens the enforcement of HIPAA privacy and security rules, and directs the Department of Health and Human Services to conduct periodic HIPAA compliance audits.

Appendix B: Cybersecurity Regulations

Sarbanes-Oxley Act Financial Fraud Controls

The Sarbanes-Oxley Act (SOX) is a 2002 U.S. law enacted to fight financial fraud. It specifies mandatory record-keeping and reporting practices for all publicly traded U.S. companies. Under Section 906 of the law, executives can be fined up to $5 million and sentenced to up to 20 years in prison for certifying a misleading or fraudulent financial report.

SOX Section 404 defines internal controls corporations must implement to detect and deter financial fraud. It instructs corporations to institute appropriate technical measures to prevent unauthorized access to IT systems and safeguard confidential data. The law requires all public companies to undergo an annual Section 404 attestation performed by an independent external auditor. Auditing firms typically use standard frameworks like COSO[5] (Committee of Sponsoring Organizations of the Treadway Commission) or COBIT (Control Objectives for Information and Related Technologies) to assess the efficacy of a corporation's information security controls.

SWIFT Customer Security Controls Framework

The Society of Worldwide Interbank Financial Telecommunication (SWIFT) Customer Security Controls Framework (CSCF) is intended to secure the global interbank messaging network. First introduced in 2016, the framework includes provisions to safeguard IT operating environments, control access to systems, and detect and respond to anomalous activity. Every year SWIFT network members must have their security controls assessed by an independent auditor and provide evidence of compliance with mandatory CSCF requirements. Penalties for non-compliance vary from country to country.

EU NIS Directive

The EU Directive on Network and Information Systems is an EU-wide cybersecurity regulation that applies to operators of digital services and essential services such as utility companies, telecommunications service providers, financial services organizations, food and agriculture companies, and healthcare organizations. In effect since 2016, the NIS Directive provides guidelines for securing IT infrastructure and reporting cybersecurity incidents.

5 The Public Company Accounting Oversight Board (PCAOB), which assists in implementation and oversight of SOX, endorses COSO, but auditors are free to use any security framework.

The EU CyberSecurity Agency (ENISA) breaks out the specific requirements for each sector (energy, finance, healthcare, etc.) and maps them to industry standards from NIST, ISO, ANSI, and other standards bodies. As a general rule, all operators of essential services are advised to implement strong identity and access management controls, and monitoring and reporting capabilities. Any EU-based essential service operator should perform regular NIS Directive compliance audits as a best practice. Non-compliance penalties from Member State to Member State.

NERC Critical Infrastructure Protection Standards

The North American Electric Reliability (NERC) Critical Infrastructure Protection (CIP) standards apply to any company that owns or operates facilities that are part of the U.S. or Canadian electric power grid. The latest specification defines a series of mandatory system security controls intended to prevent unauthorized access to critical systems and defend against service-impairing attacks. The spec includes rules for authenticating and authorizing users, implementing and managing passwords, and monitoring and logging access activity.

Any company subject to the CIP regulations must regularly provide evidence of compliance as part of routine audits and self-reporting processes. Compliance violations can result in multimillion dollar fines for major transgressions.

US Federal Information Security Modernization Act

The Federal Information Security Modernization Act (FISMA) is a 2014 law intended to strengthen the security of U.S. federal government IT systems and networks. All federal agencies and private government contractors must adhere to FISMA guidelines and conduct annual audits to review compliance and assess risks. Violators are subject to Congressional censure and potential loss of all federal funding.

FISMA guidelines are described in several publications including NIST SP 800-53, which defines strong authentication methods and access controls to defend government information systems against attack and protect data privacy. As a general rule, FISMA does not mandate specific technical requirements. Instead, it advises organizations to implement the SP 800-53 controls that are most relevant for their particular environment.

Omada, a global market leader in Identity Governance and Administration (IGA), offers a full-featured, enterprise-grade, cloud native IGA solution that enables organizations to achieve compliance, reduce risk, and maximize efficiency. Founded in 2000, Omada delivers innovative identity management to complex hybrid environments based on our proven best practice process framework and deployment approach.

06072022