NordPass®

A Beginner's Guide to Data Security Compliance

Learn how to meet the rigorous standards that will improve your compliance posture and protect your business.

Treat this guide as a handy jumping off point, not the final word. For the most up-to-date information on legislative and regulatory compliance standards, consult official sources.

Table of Contents

1. Introduction

1.1 Foreword by NordPass CEO Jonas Karklys

Compliance is a topic near and dear to NordPass. We don't take the public's trust in our product lightly.

As a newer product from Nord Security, we had no interest in sitting on the laurels of our parent brand's legacy. And we don't want anyone taking our word for the fact that we hold our products to the highest global security standard.

That's why we are proud to be officially ISO 27001 and SOC 2 Type 1 certified (and currently working on Type 2) as well as audited by the security experts at Cure53.

And with millions of Nord Security customers worldwide, legislative compliance was already deeply ingrained in our operations from the outset.

But for small and medium-sized businesses, building trust through compliance is not so easy. Even obeying the law grows more complicated by the day as legal codes gradually adapt to the public's demand for consumer privacy.

We created this guide as a resource to help you on your way, to bring you one step closer to achieving the compliance that can unlock a brighter future for your business.

Stay safe,

Jonas Karklys, CEO of NordPass and NordLocker, is a cybersecurity pioneer and co-founder of Nord Security — whose software products protect over 15 million people worldwide. Engaged in web-based projects since the age of 11, Jonas is steadfast in his commitment to helping create a radically better internet for everyone.

When he is not driving innovation, you will find Jonas on the racetracks of the most famous European and global motorsport championships.

2 What is data security compliance?

2.1 The definition of compliance

Compliance means following the rules. And the governing body of those "rules" determines the terms.

In this guide, compliance refers specifically to data security for businesses. Mainly, this is relevant to three, sometimes overlapping, types of compliance that we'll cover in the next section: legislative, regulatory, and certifications.

> **What are the other types of compliance businesses should know about?**
>
> Since compliance can be applied broadly to refer to any rules businesses have to follow to operate, paying taxes, acting in accordance with labor laws, and implementing health and safety measures are all part of being "compliant."

At the core of data security compliance is protecting **sensitive data**. In the digital age, that usually involves increasing cybersecurity measures.

But what is considered "sensitive" varies depending on an organization's industry and mission. It can apply to any information that organizations want to keep private. "Sensitive" can be a subjective designation or it can refer to a formal category defined by the law.

In all cases, "sensitive" suggests that the data has high value, both to its owners and to cybercriminals.

Sensitive data type	Definition	Examples
Personal data	Sometimes called PII, personally identifiable information, this is a broad category that usually includes any nonpublic information which is specific enough to identify an individual.	(personal) telephone number, home address
Health data	Sometimes considered a subset of personal data. In Canada and Australia, laws governing personal data cover include health information. In the US, health data or electronic protected health information (ePHI) is its own category, protected by HIPAA.	medical records, fingerprints
Financial data	Can also be considered a subset of personal data. Includes private financial records as well as information that can be used to complete purchases.	credit card number, bank statement
Other confidential or nonpublic data	In this case, a catchall category for data that its owners do not want made public. For businesses, this could include marketing plans and trade secrets. For governments, this could include military operations.	a secret recipe, a military base location

Get into the nitty-gritty.

Always check the definition and scope in the relevant compliance literature. While understanding the general terms comes in handy, the precise definitions vary.

2.2 Categories of data security compliance

1. Legislative

Legislative compliance means obeying the law. One example is the GDPR, which applies to all businesses offering goods or services to clients located in the European Union.

Since it came into force in 2018, many states and countries have followed with similarly sweeping legislation designed to protect consumers' personal information.

Australia, New Zealand, the UK, Brazil, and South Africa have followed suit, while both the US and Canada remain, for now, in the drafting stage of an equivalent law with nationwide application.

If the currently drafted propositions are passed, the former would be the first federal privacy bill regulating use of consumer data in the US. The latter would replace the arguably outdated Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada.

2. Regulatory

Regulatory compliance may also include legislation but in this context refers to guidance that applies to organizations in specific industries.

PCI DSS, GLBA, and HIPAA are all examples of regulatory compliance. PCI DSS has a global application for all entities that "process, store or transmit cardholder data." The GLBA and HIPAA are laws in the US that apply to organizations in the financial and healthcare sectors correspondingly.

3. Certifications

The third category of compliance relevant to this conversation is certifications compliance. These certifications are voluntary in the sense that they aren't mandated by law. However, increasingly, they are popping up in vendor agreements and considered a necessary component for building trust.

SOC 2 and ISO 27001 are two examples of certification compliance. Both involve data protection and general cybersecurity best practices.

2.3 Data protection compliance standards: a non-exhaustive directory

Acronym / Full name	Legislative Is it the law?	Regulatory Is it industry-specific?	Voluntary Is it optional?	Data What data is protected	Region Where does it apply?	Industry Which industries?
CCPA California Consumer Privacy Act	✓	-	-	personal data	California, USA	any
	Limitations: Applies to businesses that...	• have gross revenue exceeding $25 millon. • possess the personal information of 50,000 or more consumers, households, or devices. • earn more than half their annual revenue from selling consumers' personal information.				
CDPA Virginia Consumer Data Protection Act	✓	-	-	personal data	Virginia, USA	any
	Limitations: Applies to businesses that...	• control or process the personal data of at least 100,000 consumers during a calendar year, or • control or process the personal data of at least 25,000 consumers and derive at least 50% of its gross revenue from the sale of personal data.				
CIS Benchmarks California Consumer Privacy Act	-	-	✓	general cybersecurity	Global	any
CPA Colorado Privacy Act	✓	-	-	personal data	Colorado, USA	any
	Limitations: Applies to businesses that...	• control or process personal data of 100,000 or more consumers during a calendar year, or • derive revenue or receive discounts from the sale of personal data and control or process data of at least 25,000 consumers.				
CTDPA Connecticut Data Privacy Act	✓	-	-	personal data	Connecticut, USA	any
	Limitations: Applies to businesses that...	• control or process the personal data of 100,000 or more consumers annually, except for personal data controlled or processed solely for the purpose of completing a payment transaction. • derive over 25% of their gross revenue from the sale of personal data and controlled or processed the personal data of 25,000 or more consumers.				
CSA Star Cloud Security Alliance Security, Trust, Assurance and Risk (Levels One and Two)	-	✓	✓	confidential data	Global	cloud computing services
DFARS Defense Federal Acquisition Regulation Supplement	✓	✓	-	USA government data (CUI)	Australia, Belgium, Canada, Denmark, Egypt, Germany, France, Greece, Israel, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, United Kingdom, and Northern Ireland)	institutions handling US government data

Acronym / Full name	Legislative Is it the law?	Regulatory Is it industry-specific?	Voluntary Is it optional?	Data What data is protected	Region Where does it apply?	Industry Which industries?
DPA Data Protection Act	✓	-	-	personal data	UK	any
	Limitations: Applies to businesses that...	• have gross revenue exceeding $25 millon. • possess the personal information of 50,000 or more consumers, households, or devices. • earn more than half their annual revenue from selling consumers' personal information.				
GDPR General Data Protection Regulation	✓	-	-	personal data (PII)	Europe	any
GLBA Gramm-Leach-Bliley Act	✓	✓	-	personal data, financial data	USA	financial institutions
HIPAA Health Insurance Portability and Accountability Act	✓	✓	-	protected health information (PHI)	USA	healthcare institutions
ISO/IEC 27001 International Organization for Standardization/ International Electrotechnical Commission 27001	-	-	✓	general cybersecurity	Global	any
LGPD Lei Geral de Proteção de Dados	✓	-	-	personal data	Brazil	any
NIST CSF National Institute of Standards and Technology Cybersecurity Framework	-	-	-	general cybersecurity	Global	any
	Limitations: Applies to businesses that...	*This guidance is mandatory for US government institutions and is also commonly used by foreign governments, insurance organizations, and other privately owned companies.				
PA (Australia) Privacy Act	✓	-	-	personal data	Australia	any
	Limitations: Applies to businesses that...	• have an annual turnover of more than $3 million, including Australian Government agencies.				
PA (New Zealand) Privacy Act	✓	-	-	personal data	New Zealand	any
PCI DSS Payment Card Industry Data Security Standard	-	✓	-	personal data, financial data	Global	any
	Limitations: Applies to businesses that...	• store, process, and/or transmit cardholder data.				
PIPEDA Personal Information Protection and Electronic Documents Act	✓	-	-	personal data	Canada	any

Acronym / Full name	Legislative Is it the law?	Regulatory Is it industry-specific?	Voluntary Is it optional?	Data What data is protected	Region Where does it apply?	Industry Which industries?
POPI Protection of Personal Information Act	✓	-	-	personal data	South Africa	any
SOC 2 Service Organization Control 2	-	✓	✓	confidential data	Global	applied services
SOC 3 System and Organization Control 3	-	✓	✓	confidential data	Global	service providers
UCPA Utah Consumer Privacy Act	✓	-	-	personal data	Utah, USA	any

Limitations:
Applies to businesses that...

- have an annual revenue of $25,000,000 or more, and either: control or process the personal data of 100,000 or more consumers annually.

2.4 Fundamentals of compliance

Meeting compliance standards is sometimes compared to “checking a box,” wherein only the minimum standard must be met. But, it’s just as important to fulfill the spirit of the law as it is the letter of the law.

After all, compliance is based on mitigating risk — by decreasing the likelihood and the impact of suffering an incident that would compromise your information security. At its core, meeting compliance standards is about preventing a worst case scenario, a fear.

This fear could be that confidential information is exposed, that the data will be altered in some way that disrupts its utility, or that a critical data source will become inaccessible. Consider the impact, for example, of the publication, corruption, or deletion of personal health records.

On how to subdue this fear, it’s useful to start with the fundamentals. The CIA triad is an information security acronym used as a model for identifying vulnerabilities and developing secure systems.

The three letters stand for confidentiality, integrity, and availability.

Confidentiality protects access to the data. A concept akin to privacy, this principle ensures that intruders or unauthorized members are kept out.

Integrity protects the data itself. This principle states that the data should be of good quality — consistent, reliable, and unaltered.

Availability is the counterpart to confidentiality, protecting authorized users' access to data. The essence is that those who need it have easy access. This also presupposes that the data is not destroyed or deleted — it exists.

When creating a security program to protect sensitive data, all three of these elements should be addressed. In doing so, a business will be well on its way to being compliant with the industry's best data (or information) security practices.

Principle	What does it mean? (Definition)	What promotes it? (Example)	What threatens it? (Example)
Confidentiality	Only authorized users have access to the data.	Restricting access — with strong passwords, end-to-end encryption.	A data breach
Integrity	The data can be trusted. It is accurate and complete.	Processes and tools that ensure the consistency of the data — like input validation.	A bug
Availability	Those who need it get seamless access to the data.	Having redundancies and backups — for both the data and the systems that host it.	A DDoS attack

What's the difference between information security and cybersecurity?

Cybersecurity is a general term used to describe any type of protection against digital attacks. It can be applied to systems, networks, and programs. Information security refers broadly to the protection of any data or information that's digital, physical, or intellectual. When we refer to protecting data in digital spaces, these goals overlap even though they are distinct.

2.5 Consequences of non-compliance

The consequences for non-compliance are as varied as the regulations themselves. They depend on their respective governing bodies: laws by governments, regulatory compliance by a combination of legislators and industry experts, and certifications by globally accredited institutions.

Business interruption

Compliance is a mandatory requirement for doing business in certain industries. Usually, businesses and organizations responsible for handling especially sensitive data, for whom the risk of a cyber attack is high, or both.

DFARS, the Defense Federal Acquisition Regulation administered by the Department of Defense (DoD) in the United States, for example, must be met by any institution or business handling US government data.

In other cases, failure to comply can simply limit the reach of your business. While certifications are technically voluntary, it is more and more common for external audits such as a SOC report to appear as a requirement in contractual agreements.

Financial penalties

For violations of legislative compliance, fines are common. They are set by the bodies that govern them. Severe GDPR violations are subject to penalties up to 20 million euros, or 4% of the business' earnings from the previous year — whichever is higher.

In some cases, individuals can also claim compensation against businesses, to be paid in addition to penalties issued by the government. If a health institution's HIPAA violation has left protected health information exposed, the patients can sue for compensation. The most common scenario is a class-action lawsuit. Notably, plaintiffs do not have to have suffered material damage to file a claim. Individuals can seek compensation for future or possible harm.

Criminal penalties including jail time

It is rare, but not unheard of, for data privacy laws to have criminal penalties. Such is the case with the US financial industry's GLBA, where violators can be punished with up to five years in prison.

As laws race to catch up with technological advances, it may become more common to have jail time on the line. Legislators face mounting pressure to hold executives criminally accountable in situations where the cost for failure is high. Because problems with cyber-physical systems like self-driving cars can cause serious injury to people, Gartner predicts that by 2024, 75% of CEOs will be personally liable for security incidents in this sector.

To be clear, high cost doesn't have to mean life or death. Back in 2019, US Senator Elizabeth Warren proposed the Corporate Executive Accountability Act — a bill that could hold executives of large corporations criminally responsible for, among other things, data privacy violations that threaten civil rights.

Reputational damage

Reputational damage is a byproduct of non-compliance. It's not usually the result of the compliance failure itself but what has happened as a result.

Failing to meet what is essentially the agreed-upon best practice for data security comes with risks. A high-profile data breach, for example, can make your business a household name for all the wrong reasons.

In fact, though data breaches cost businesses millions in recovery, loss of customer trust was identified as the top consequence. And the impact can be long-lasting, carrying on in public consciousness well after the breach-causing vulnerability is patched.

The bright side is that the reverse is also true, that achieving compliance certifications can fast-track trust-building with prospective clients — helping them adopt your product or service more readily.

2.6 State of compliance in 2023

In the future, your business will be up against increasingly stringent compliance measures. And no matter how you look at it, the cost for failure is steep.

In Europe, GDPR fines issued have reached an all-time high, a staggering seven times increase year-over-year. In the United States, CCPA claims are already seeing an uptick during the law's second year. Increasingly strict regulatory compliance failures could threaten your operations. And lacking a compliant security program makes your business more vulnerable to a devastating cyberattack.

That's especially relevant today, given the rise in cost and frequency of data breaches and ransomware events since the start of the global pandemic.

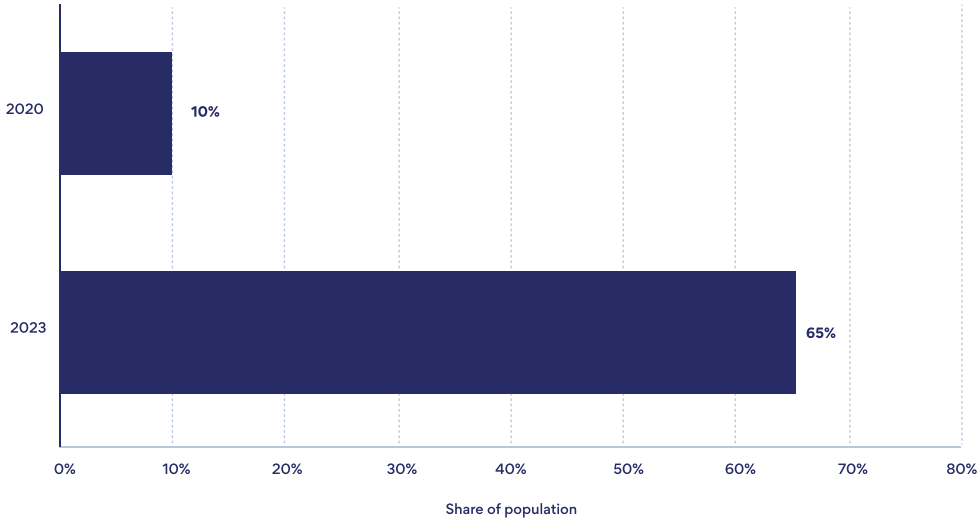
What's more, our experts predict the following two major trends for the not-so-distant future that further underscore the relevance of compliance for all businesses in 2023 and beyond.

1. Regulations will become more prescriptive.

The global data privacy legislative landscape is undergoing a huge paradigm shift — from harm prevention to rights protection. In the United States, Colorado, Connecticut, Utah, and Virginia have followed California's lead in enacting GDPR-esque laws restricting businesses' ability to collect and use personal information. This represents a break from the country's previous data privacy laws, such as the GLBA and HIPAA which are restricted to specific types of sensitive data — financial and health, respectively.

Not unique to the United States, it's expected that this is reflective of a larger global trend, with Statista forecasting that the share of the global population that have data covered under modern privacy regulations will balloon this year, up to 65%.

Share of global population that have personal data covered under modern privacy regulations



Source: Statista, 2023

2. Consumers will demand more transparency regarding data privacy.

A more prescriptive legal framework is likely to raise the bar on consumers' and businesses' expectations of privacy. At the same time, a number of large scale household brand breaches from the past year have put the importance of information security into sharp focus for all.

Accordingly, businesses and organizations will have to go farther to build trust among increasingly anxious consumers and business partners — driving demand for certifications compliance.

Frustration regarding slow-moving regulatory standards will apply pressure on the governing bodies to update them, as the current reporting standard is due for a reckoning. Breach notification lingers, for example, and is often being reported days and months after the fact.

Soon, such delays will be considered intolerable, with a collective push toward more transparency.

3 How can businesses become compliant?

3.1 Creating a culture of compliance inside your organization

The first challenge in achieving compliance is a philosophical one. Getting buy-in at every level is an important step. What's key while building trust with internal teams is making sure that security and compliance are positioned as enablers in your organization, not blockers.

The most straightforward way of stressing the importance of security and compliance is to have these principles integrated into your roadmap from day one. Ideally, the initiatives should go hand in hand with your corporate strategy.

The goal is getting to the point where adhering to the best practices that keep you compliant are mundane and part of your team's daily routine.

However, if you're reading this, it's likely that you are either considering compliance for the first time or looking to step up your game in order to gain certification compliance or enter a new market. In this case, the process will involve introducing new practices to your team.

To be clear, it's never too late to start and it's still possible to get enthusiastic buy-in from your team with the right steps. Software can help.

Specifically, software that makes secure behavior the default while making other aspects of work easier. For example, deploying a business password manager with user-friendly features that improve collaboration and efficiency.

The NIST's Digital Identity Guidelines warn against the vulnerability of user-chosen passwords. Users tend to choose passwords that are easy to remember but that makes them also easy to hack.

Actually, the adoption of weak and reused passwords is so ubiquitous that even C-suite executives are guilty of it. "123456" or a variation of it regularly tops the list of the most common passwords for this group. It's likely not a lack of awareness, but a lack of software that's to blame.

With NordPass Business' company-wide password policy, you can set the rules for what constitutes a strong password. From your team's perspective, compliance is easy thanks to the Password Generator. It instantly incorporates your password policy requirements when generating strong, unique credentials. And because those strong passwords populate fields automatically, a good memory is not necessary.

3.2 Managing compliance outside your organization

Compliance doesn't stop where your business ends. There needs to be a process wherein vendors are validated as secure partners.

Remember that your own compliance certifications have trickle-down effects. If your business has a certain compliance mandate then, you have a responsibility to ensure that your vendors and third parties are holding their own practices to the same standard.

Here, certification compliance comes in as a convenient short-hand. This process is especially important for businesses that will be trusted with your sensitive data.

The bottom line is due diligence. Should a time come when a regulator or attorney asks your business about its vendor onboarding process, you want to have the documentation to validate that you were not negligent.

Consider making this a requirement up front by including it in the request for proposal phase of your vendor recruitment process.

If you are new to this process, remember that you can get assistance from outside your organization. Don't hesitate to seek help. There are a lot of resources available to help with vendor validation, depending on your industry.

4 Next steps

4.1 Key takeaways

Compliance standards will continue to grow more strict in the coming years as awareness of cyber threats and their potentially devastating outcomes becomes more mainstream.

While consumers are increasingly mindful of the importance of personal data privacy, organizations are beginning to prioritize compliance and information security initiatives to avoid making the headlines for the wrong reasons.

In this climate, certifications compliance will become a requisite for building trust among collaborators and clients alike — to an ever greater extent than they are today.

For businesses that haven't integrated compliance into their operations from the outset, the idea of increasingly strict measures can be daunting. But if you start with an understanding of the fundamentals of information security upon which many compliance standards are based, meeting these measures can be achieved step by step.

To help along your journey, be sure to have the right resources and tech stack in place to make adherence as easy as possible for your team. Remember to frame compliance as an enabler and not a roadblock to achieving your goals.

Ultimately, to future-proof your plan, you will want to go beyond checking boxes to meet the minimum requirement and strive to stay ahead of compliance trends. A proactive security posture can help.

4.2 Get started now

As the ancient proverb goes: the best time to plant a tree is a hundred years ago, and the second best time is right now. You could say the same about your business compliance plan.

Achieve compliance with the help of NordPass Business

- [x] NordPass Business can help you to ensure the **confidentiality, integrity, and availability** of your credentials, passwords, personal information, and notes.

    - Each member's vault is end-to-end encrypted with the ultra secure XChaCha20 encryption algorithm, supporting zero-knowledge architecture. That means no one, not even NordPass, has access to the information stored in your NordPass Business vault — a measure that significantly decreases vulnerability.

- [x] NordPass can help you **control access** to sensitive data and corporate accounts.

    - By making strong credentials the new standard: NordPass makes creating strong, hard-to-hack credentials seamless and offers multi-factor authentication — which are two common compliance standards. You will find one or both mentioned in HIPAA, GLBA, PCI DSS, and NIST guidance as well as CIS benchmarks.

    - With member management and permissions: When a contractor or an employee leaves or changes roles, preventing sensitive information going with them is easy. Granting, revoking, or reassigning access is swift, simple, and secure. And granular access control allows administrators to share logins and payment information with full or limited rights — ensuring that each member of your team only has access to what they need. For additional privacy, members can share credentials without reading or editing access.

NordPass Business can help you **prevent and mitigate the damage of data breaches**.

- Given that almost half of all breaches depend on stolen credentials, storing them securely is an essential step in preventing a leak that may lead to non-compliance.

- In the event that your company's sensitive data or domain is exposed in a breach, NordPass Business' Data Breach Scanner and Breach Monitoring features will ensure that you're the first to know. Use the Data Breach Scanner to detect whether your corporate credentials, payment information, or company domains have been breached. With Breach Monitoring, your team members will get immediate notification if their email credentials appear in a data breach. Reducing the time between breach and discovery will give you the time you need to mitigate damage and remain compliant.

To learn more about how NordPass Business can help you achieve strict data security compliance standards, contact us.

Contact us

Ieva Labutytė, NordPass:
ieva.labutyte@nordsecbusiness.com
+370 674 75363

Simas Žvirblis, NordPass:
simas.zvirblis@nordsecbusiness.com
+370 681 27735

5 Appendix

5.1 Internal resources

- Overcome Compliance Challenges | NordPass Webinar: NordPass invited four compliance and security experts to participate in a webinar on compliance. Together, the specialists provided their best advice for businesses facing increasingly strict compliance standards. Their insights inspired this guide.
- NordPass compliance experts
- NordPass blog and website

5.2 External resources

Studies and statistics

- Akin Gump's Second Annual CCPA Report Finds Uptick in Claims with Trend Towards Settlement
- Cost of a Data Breach Report 2022
- Fines for breaches of EU privacy law spike sevenfold to $1.2 billion, as Big Tech bears the brunt
- Gartner Predicts 75% of CEOs Will be Personally Liable for Cyber-Physical Security Incidents by 2024
- Global population with personal data covered under regulations 2023 | Statista
- The top 10 data breaches of 2022 | Security Magazine
- U.S. data privacy laws to enter new era in 2023 | Reuters
- Verizon's 2022 Data Breach Investigations Report

Legislative compliance standards by country

Australia

- The Privacy Act - Home

Brazil

- Brazilian General Data Protection Law (LGPD, English translation)

Canada

- Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)

European Union

- GDPR

New Zealand

- Privacy Act 2020 No 31 (as at 30 November 2022), Public Act Contents – New Zealand Legislation

South Africa

- The PoPI Act

United Kingdom

- The Data Protection Act - GOV.UK

United States

- Bill: Corporate Accountability Act
- DFARS | Acquisition.GOV
- HIPAA Home | HHS.gov
- Gramm-Leach-Bliley Act | Federal Trade Commission
- California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General
- Code of Virginia Code - Chapter 53. Consumer Data Protection Act
- Colorado Privacy Act (CPA) Rulemaking
- The Connecticut Data Privacy Act

Other compliance standards

- CIS Benchmarks
- Framework Documents | NIST
- ISO/IEC 27001 and related standards — Information security management
- NIST Special Publication 800-63-3: Digital Identity Guidelines
- PCI Security Standards Council