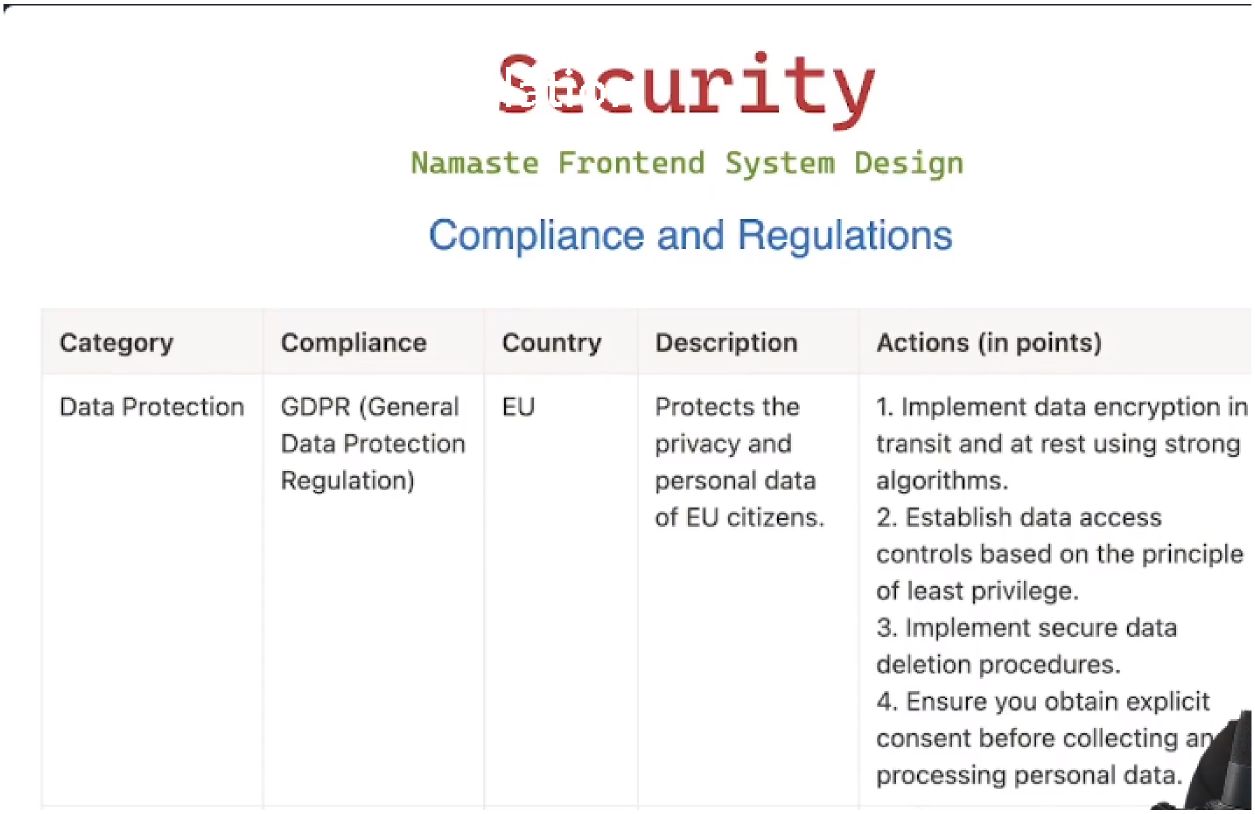
Compliance and Regulation

You might have read many articles on biggest companies paying fines in million dollars for violating some rules and regulations.

Example - Websites have started taking consent for storing the cookies.

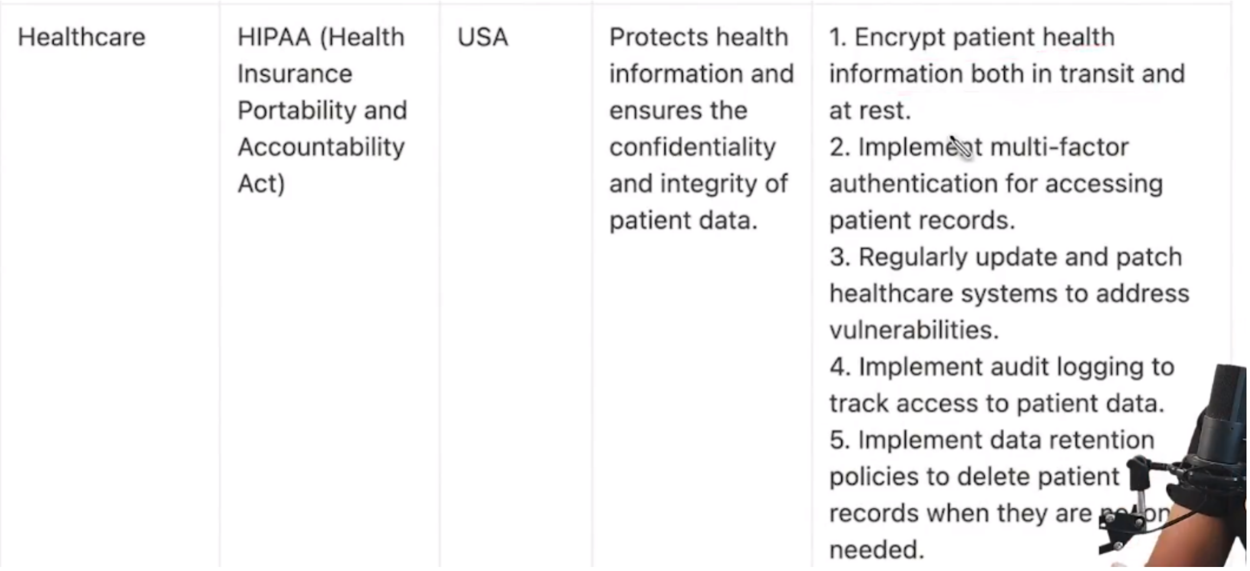


Security

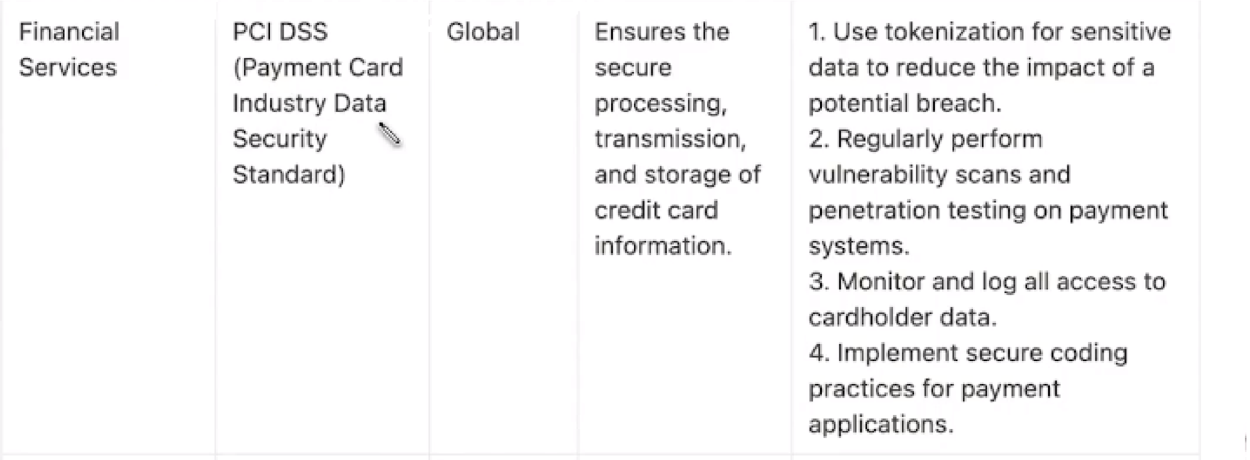
Namaste Frontend System Design

Compliance and Regulations

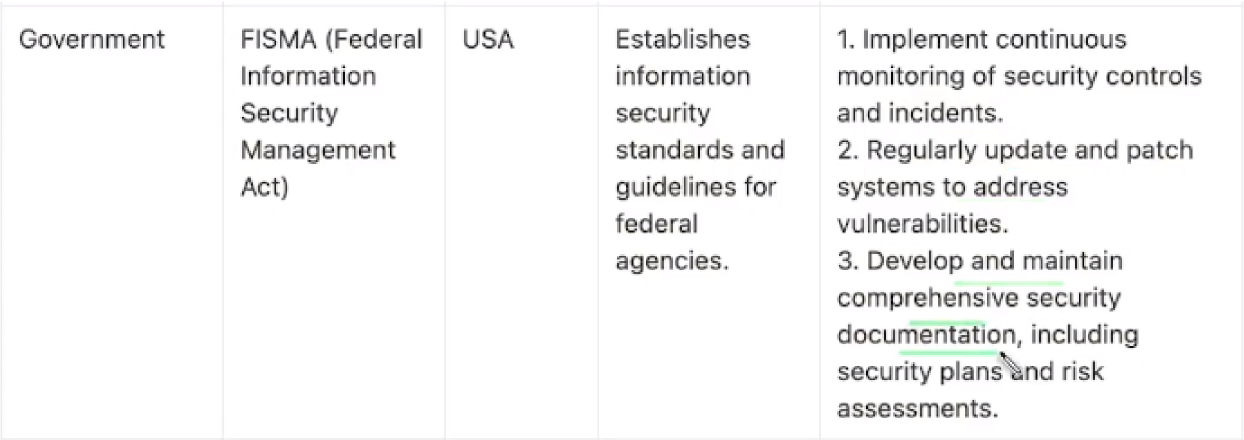
Category	Compliance	Country	Description	Actions (in points)
Data Protection	GDPR (General Data Protection Regulation)	EU	Protects the privacy and personal data of EU citizens.	1. Implement data encryption in transit and at rest using strong algorithms. 2. Establish data access controls based on the principle of least privilege. 3. Implement secure data deletion procedures. 4. Ensure you obtain explicit consent before collecting an processing personal data.



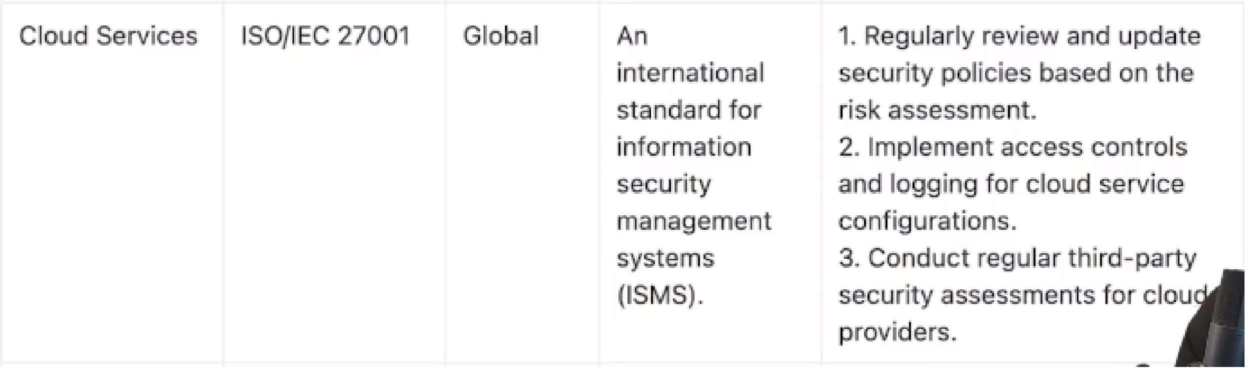
Healthcare	HIPAA (Health Insurance Portability and Accountability Act)	USA	Protects health information and ensures the confidentiality and integrity of patient data.	1. Encrypt patient health information both in transit and at rest. 2. Implement multi-factor authentication for accessing patient records. 3. Regularly update and patch healthcare systems to address vulnerabilities. 4. Implement audit logging to track access to patient data. 5. Implement data retention policies to delete patient records when they are no longer needed.



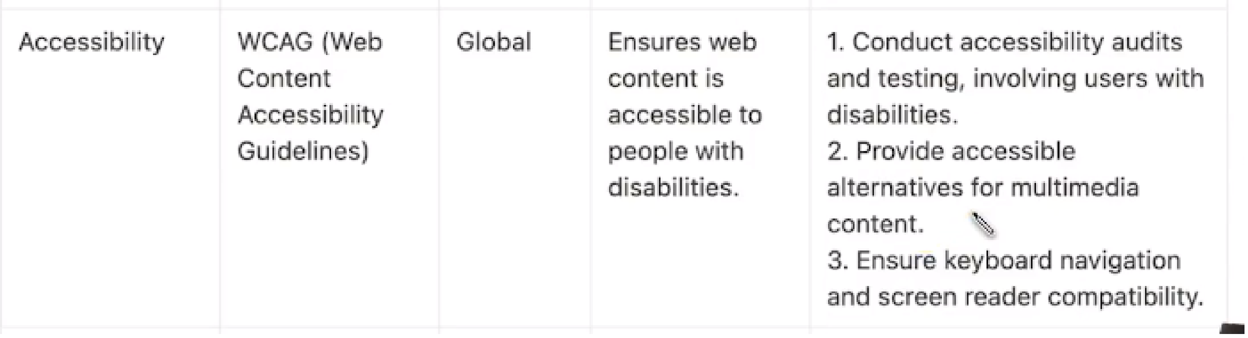
Financial Services	PCI DSS (Payment Card Industry Data Security Standard)	Global	Ensures the secure processing, transmission, and storage of credit card information.	1. Use tokenization for sensitive data to reduce the impact of a potential breach. 2. Regularly perform vulnerability scans and penetration testing on payment systems. 3. Monitor and log all access to cardholder data. 4. Implement secure coding practices for payment applications.



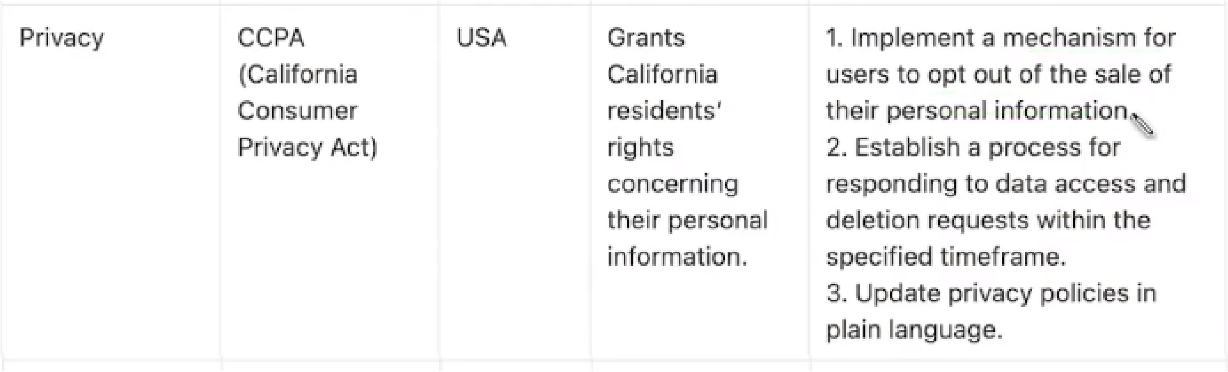
Government	FISMA (Federal Information Security Management Act)	USA	Establishes information security standards and guidelines for federal agencies.	1. Implement continuous monitoring of security controls and incidents. 2. Regularly update and patch systems to address vulnerabilities. 3. Develop and maintain comprehensive security documentation, including security plans and risk assessments.



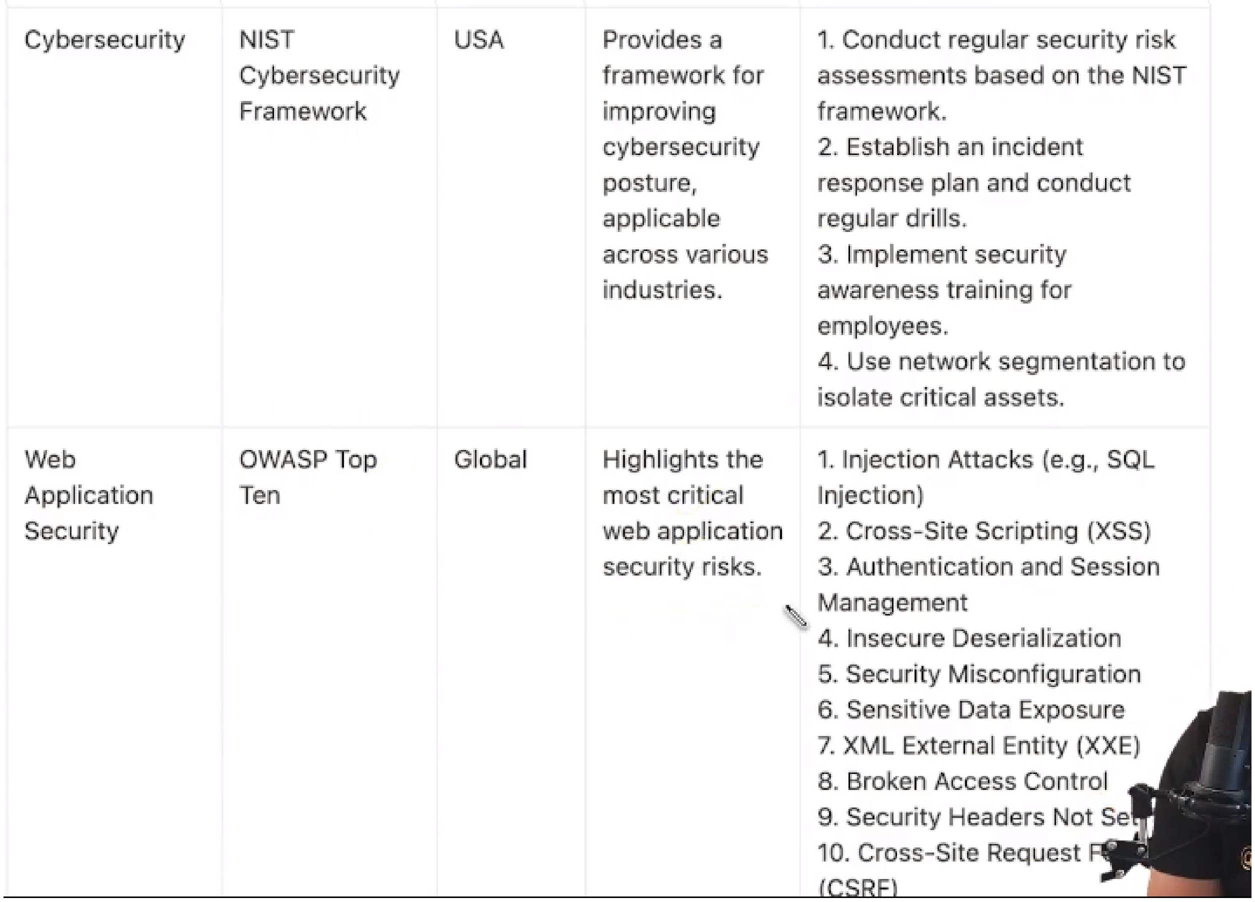
Cloud Services	ISO/IEC 27001	Global	An international standard for information security management systems (ISMS).	1. Regularly review and update security policies based on the risk assessment. 2. Implement access controls and logging for cloud service configurations. 3. Conduct regular third-party security assessments for cloud providers.



Accessibility	WCAG (Web Content Accessibility Guidelines)	Global	Ensures web content is accessible to people with disabilities.	1. Conduct accessibility audits and testing, involving users with disabilities. 2. Provide accessible alternatives for multimedia content. 3. Ensure keyboard navigation and screen reader compatibility.



Privacy	CCPA (California Consumer Privacy Act)	USA	Grants California residents' rights concerning their personal information.	1. Implement a mechanism for users to opt out of the sale of their personal information. 2. Establish a process for responding to data access and deletion requests within the specified timeframe. 3. Update privacy policies in plain language.



Cybersecurity	NIST Cybersecurity Framework	USA	Provides a framework for improving cybersecurity posture, applicable across various industries.	1. Conduct regular security risk assessments based on the NIST framework. 2. Establish an incident response plan and conduct regular drills. 3. Implement security awareness training for employees. 4. Use network segmentation to isolate critical assets.
Web Application Security	OWASP Top Ten	Global	Highlights the most critical web application security risks.	1. Injection Attacks (e.g., SQL Injection) 2. Cross-Site Scripting (XSS) 3. Authentication and Session Management 4. Insecure Deserialization 5. Security Misconfiguration 6. Sensitive Data Exposure 7. XML External Entity (XXE) 8. Broken Access Control 9. Security Headers Not Se 10. Cross-Site Request F (CSRF)