Regulations and IT Compliances Requirements.

The table below illustrates the most common regulations and standards to which organizations are most likely to seek compliance with. Refer to this table if you are interested in understanding what a particular regulation enacts as well as the IT compliance requirements related to it.

Regulation/ Standard	What does it mean?	IT Compliance Requirements
HIPAA (Health Insurance Portability and Accountability Act)	HIPAA seeks to establish standardized mechanisms for electronic data interchange (EDI), security, and confidentiality of all healthcare-related data.	1. Make data backups 2. Establish access controls based on job responsibilities 3. Log successful access attempts to mission-critical resources 4. Limit unsuccessful user ID login attempts after consecutive unsuccessful tries 5. Require authentication 6. Enable system events (logging) 7. Encrypt information 8. Keep data physically and electronically secure from unauthorized access (implement security tools to prevent malicious attacks or detect intrusions, restrict Internet access to DMZ)
FDA Part 11	Part 11, as it is commonly called, deals with the Food and Drug Administration (FDA) guidelines on electronic records and electronic signatures in the United States. It requires drug makers, medical device manufacturers, biotech companies, biologics developers, and other FDA-regulated industries to implement controls, including audits, system validations, audit trails, electronic signatures, and documentation for software and systems involved in processing electronic data.	
EU Annex 11	EU Annex 11 is the European equivalent of FDA's Part 11. Defines the criteria under which electronic records and electronic signatures are considered to be trustworthy, reliable and equivalent to paper records.	
The Gramm-Leach Bliley Act (GLBA)	The GLB Act is the Financial Modernization Act of 1999. It includes provisions to protect consumers' personal financial information held by financial institutions.	
PCI DSS	The PCI Security Standards Council's mission is to enhance payment account data security by driving education and awareness of the PCI Security Standards. The organization was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc	
CA Assembly Bill No. 1950	This bill require a business that owns or licenses personal information about a California resident to implement and maintain reasonable security procedures and practices to protect personal information from unauthorized access, destruction, use, modification or disclosure including data destruction and data protection. Since A.B. 1950 does not further define these reasonableness standards, it leaves businesses struggling to understand their scope and to implement business practices sufficient to avoid liability under A.B. 1950. Thus, in order to avoid liability that might arise from failure to provide "reasonable security" under A.B. 1950, businesses should consider using HIPAA and the GLBA as guidelines for their own security practices and procedures.	

Asigra.

Regulation/ Standard	What does it mean?	IT Compliance Requirements
Sarbanes-Oxley Act	SOX or Sarbox, is designed to "protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws." Section 302 of the Sarbanes-Oxley Act on corporate responsibility for financial reporting requires certification of financial statements by both the CEO and the CFO. This means that all financial reporting must be thoroughly verified by management with more acuity than ever before. IT departments supporting financial systems will also have to ensure the accuracy of these records.	1. Establish access controls based on job responsibilities 2. Log successful access attempts to mission-critical resources 3. Require authentication 4. Enable system events (logging) 5. Keep data physically and electronically secure from unauthorized access 6. Data retention : 7 years retention for audit reports and related materials 7. Immutability: Prevent the alteration, destruction, mutilation, concealment, falsification, of any record/document*. *SOX implies the need for encryption to protect the integrity and confidentiality of financial information.
EU Data Protection Directive (EUDPD)	The EUDPD declares that data protection is a fundamental human right. It standardizes protection of data privacy for EU citizens	1. Make data backups 2. Establish access controls based on job responsibilities 3. Require authentication 4. Enable system events (logging) 5. Encrypt personal information
Basel II Capital Accord	Requires that banks put in place Business Continuity and Disaster Recovery plans to ensure continuous operation and to limit losses.	1. Make data backups 2. Archiving, retrieval and restoration capabilities should be in place 3. Data retention of 3-7 years of data history.
MA 201 CMR 17	Requires any business that collects personal information about a MA state resident to encrypt all portable devices, wireless transmissions and public networks. This mean that if you have data on a resident of Massachusetts on your hard drive, for example, you still must encrypt the data even if you do not send it via email or over the Internet.	1. Data encryption

Regulation/ Standard	What does it mean?	IT Compliance Requirements
Canada's Personal Information Protection & electronic Data Act (PIPEDA)	This law requires organizations to obtain consent when they collect, use or disclose their personal information. It also declares that organizations should supply an individual with a service or product even if they refuse consent for the collection, use or disclose of your personal information unless that information is essential to the transaction. It also enacts that Information should be collected by fair and lawful means; and personal information policies must be clear, understandable and readily available.	1. Make data backups 2. Establish access controls based on job responsibilities 3. Require authentication 4. Enable system events (logging) 5. Encrypt personal information
Health Information Technology for Economic and Clinical Health Act (HITECH)	The HITECH Act includes measures designed to broaden the scope and increase the rigor of HIPAA compliance. In terms of management and protection of Protected Health Information (PHI) data, four key areas are especially important : a) Expansion of HIPAA rules to business associates b) Stricter requirements for breach notifications c) Encryption as a recognized methodology for protecting PHI	1. Data destruction 2. Data encryption
Federal Information Security Management Act (FISMA)	The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or manmade threats	The National Institute of Standards and Technology (NIST) outlines nine steps toward compliance with FISMA: 1. Categorize the information to be protected. 2. Select minimum baseline controls. 3. Refine controls using a risk assessment procedure. 4. Document the controls in the system security plan. 5. Implement security controls in appropriate information systems. 6. Assess the effectiveness of the security controls once they have been implemented. 7. Determine agency-level risk to the mission or business case. 8. Authorize the information system for processing. 9. Monitor the security controls on a continuous basis.

Regulation/ Standard	What does it mean?	IT Compliance Requirements
Expedited Funds Availability Act (EFA)	Enacted in 1987 by the United States Congress, the Expedited Funds Availability Act's (EFA or EFAA) purpose is to standardize hold periods on deposits made to commercial banks and to regulate institutions' use of deposit holds. Requires federally chartered financial institutions to have a demonstrable business continuity plan to ensure prompt availability of funds.	1. Business Continuity 2. Disaster Recovery Plans
Federal Energy Regulatory Commission (FERC)	The Federal Energy Regulatory Commission, or FERC, is an independent agency that regulates the interstate transmission of electricity, natural gas, and oil. Mandates recovery plans for utilities.	
Financial Industry Regulatory Authority (FINRA)	Formed by consolidating redundant rules under NASD (Rule 3510) and NYSE (Rule 446). Under NASD 3510, members are required to maintain business continuity and contingency plans to satisfy obligations to clients in the event of an emergency or outage. It requires members to create, test, and update business continuity plans to satisfy obligations to clients in the event of an emergency or outage.	
Securities and Exchange Commission (SEC) 17-a 3,4	In combination, Rules 17a-3 and 17a-4 require broker-dealers to create, and preserve in an easily accessible manner, a comprehensive record of each securities transaction they effect and of their securities business in general. Rule 17a-4 defines that term as "any digital storage medium or system." Paragraph (f)(2)(ii)(A) of Rule 17a-4 requires that the electronic storage media preserve the records exclusively in a non-rewriteable and non-erasable format. Retention is required for a specific period of time.	1. Make data backups 2. Data encryption 3. Data retention

How Asigra Addresses Compliance Requirements.

The IT compliance requirements for most of regulations/standards can be categorized into four key sections. The table below shows how Asigra addresses each one of them.

Category of compliance	How Asigra addresses
• Privacy/confidentiality of information - Protect data from unauthorized disclosure. - Implies technologies such as encryption and access control to restrict access to data.	• Data is encrypted (AES 256, 196, 128-bit), before being transmitted over the WAN. • Data stored in the DS-System and/or BLM is encrypted. • Encryption is FIPS 140-2 certified • Access control to data with full audit trail and reporting logs
• Integrity of data - Protect data from unauthorized modification ensuring its accuracy. - Implies technologies such as encryption and access control (authentication). - Integrity checks. - Audit trails (logging system events and physical access).	• Data is encrypted (AES 256, 196, 128-bit), before being transmitted over the WAN. • Data is stored encrypted. • Encryption is FIPS 140-2 certified • Access control to data with full audit trail and reporting logs • Data integrity validation through Autonomic Healing and Restore Validation
• Availability of information - Ensure that information is available when needed through business and service uptime assurance. - Data protection. - Business Continuity and Disaster Recovery technologies and plans.	• N+1 and grid architecture ensures high availability through failover in case of system disruptions • Disk based retention for fastest recovery • Automated and verifiable backup/recovery process with built-in SLA module for reporting and auditing purposes. • Built-in data replication capability for DS-System and BLM storage enables emergency plans for business continuity • Asigra's architecture implements fast and reliable backup/recoveries at off-site location for DR purposes. • Asigra's Value Beyond Software provides best practices and support for Business Continuity plans and Disaster Recovery Drills implementation and auditing purposes.
• Retention - Preservation of information in an unalterable form for specified periods of time. - With or without requirements for data destruction. - Ability to set policies and manage the lifecycle of data.	• Asigra's BLM provides long term disk based retention with data destruction certificate. • Intuitive GUI makes it easy to implement and manage retention rules and policies. • Long term data is stored encrypted.

Asigra.

Quick Reference Guide.

What is addressed by Asigra in terms of regulatory mandates.

Regulation	Compliance Requirements	Addressed by Asigra?	
		Yes	N.A.
1 - HIPAA (Health Insurance Portability and Accountability Act) 2 - EU Annex 11 3 - The Gramm-Leach Bliley Act 4 - PCI DSS 5 - CA Assembly Bill No. 1950	a) Make data backups	√	
	b) Establish access controls based on job responsibilities	√	
	c) Log successful access attempts to mission-critical resources	√	
	d) Limit unsuccessful user ID login attempts after consecutive unsuccessful tries	√	
	e) Require authentication	√	
	f) Enable system events (logging)	√	
	g) Encrypt information	√	
	h) Keep data physically and electronically secure from unauthorized access (implement security tools to prevent malicious attacks or detect intrusions, restrict Internet access to DMZ)		√
6 - Sarbanes-Oxley Act	a) Establish access controls based on job responsibilities	√	
	b) Log successful access attempts to mission-critical resources	√	
	c) Require authentication	√	
	d) Enable system events (logging)	√	
	e) Keep data physically and electronically secure from unauthorized access (implement security tools to detect intrusions)		√
	f) Data retention : 7 years retention for audit reports and related materials	√	
	g) Encrypt information	√	
7 - EU Data Protection Directive (EUDPD)	a) Make data backups	√	
	b) Establish access controls based on job responsibilities	√	
	c) Require authentication	√	
	d) Enable system events (logging)	√	
	e) Encrypt personal information	√	
8 - Basel II Capital Accord	a) Make data backups	√	
	b) Archiving, retrieval and restoration capabilities should be in place	√	
	c) Long-Term data retention (3-7 years of data history)	√	
9 - MA 201 CMR 17	a) Data Encryption	√	

Asigra.

Regulation	Compliance Requirements	Addressed by Asigra?	
		Yes	N.A.
10 - Canada's Personal Information Protection & electronic Data Act (PIPEDA)	a) Make data backups	√	
	b) Establish access controls based on job responsibilities	√	
	c) Require authentication	√	
	d) Enable system events (logging)	√	
	e) Encrypt personal information	√	
11 - Health Information Technology for Economic and Clinical Health Act (HITECH)	a) Data destruction	√	
	b) Data Encryption	√	
12 - Federal Information Security Management Act (FISMA)	a) Categorize the information to be protected.	√	
	b) Select minimum baseline controls.	√	
	c) Refine controls using a risk assessment procedure.		√
	d) Document the controls in the system security plan.		√
	e) Implement security controls in appropriate information systems.		√
	f) Assess the effectiveness of the security controls once they have been implemented.		√
	g) Determine agency-level risk to the mission or business case.		√
	h) Authorize the information system for processing.		√
	i) Monitor the security controls on a continuous basis.		√
13 - Expedited Funds Availability Act (EFA) 14 - Federal Energy Regulatory Commission (FERC) 15 - Financial Industry Regulatory Authority (FINRA)	a) Business Continuity	√	
	b) Disaster Recovery Plan	√	
16 - Securities and Exchange Commission (SEC) 17-a 3,4	a) Make data backups	√	
	b) Data encryption	√	
	c) Data retention	√	