OPENTEXT™

Regulatory Compliance & EIM Requirements Quick Reference Guide

About the Regulation					Enterprise Information Management (EIM) Requirement					
REGULATION OR STANDARD	**SUMMARY DESCRIPTION**	**REGION**	**REGULATORS/ ENFORCERS**	**INDUSTRY**	**DATA PROTECTION & PRIVACY**	**RECORDS MGMT**	**E-DISCOVERY REQS**	**INFORMATION INTEGRITY & AUTHENTICITY**	**REPORTING OBLIGATIONS**	**PROCESS COMPLIANCE**
Dodd-Frank Wall Street Reform & Consumer Protection Act	Implements changes that, among other things, affect the oversight and supervision of financial institutions, create a new agency responsible for implementing and enforcing compliance with consumer financial laws, and regulate corporate governance and executive compensation practices.	US	SEC, FDIC, OCC, Federal Reserve, SIPC, and others	Financial Institutions		**X**			**X**	**X**
FATCA (Foreign Account Tax Compliance Act)	Aimed to prevent tax evasion by US citizens and residents through use of offshore accounts. Requires American citizens (including those living outside the U.S.) to annually report on their non-U.S. financial accounts, and requires all foreign (non-US) financial institutions (FFIs) to search their records for suspected US persons to report their assets and identities to the US Treasury.	US	FINCEN, US Treasury and IRS	Financial Institutions		**X**			**X**	**X**
Basel Accords (II and III)	A set of international banking regulations put forth by the Basel Committee on Bank Supervision, effectively the code of conduct for banks.	Int'l	Basel Committee on Bank Supervision; In USA: OCC, FDIC and Federal Reserve	Financial Institutions		**X**			**X**	**X**

Regulatory Compliance & EIM Requirements Quick Reference Guide

OPENTEXT™

About the Regulation					Enterprise Information Management (EIM) Requirement					
REGULATION OR STANDARD	**SUMMARY DESCRIPTION**	**REGION**	**REGULATORS/ ENFORCERS**	**INDUSTRY**	**DATA PROTECTION & PRIVACY**	**RECORDS MGMT**	**E-DISCOVERY REQS**	**INFORMATION INTEGRITY & AUTHENTICITY**	**REPORTING OBLIGATIONS**	**PROCESS COMPLIANCE**
MiFID II (Markets in Financial Instruments Directive) and MIFIR (Regulation)	MiFID came into force in 2007; is a comprehensive regulatory directive that affects how firms carrying on investment business and ancillary activities will organise their internal systems and controls and how they will conduct business with their customers across Europe. MiFID includes recordkeeping and reporting requirements such as the obligation to keep any records that enable authorities to monitor regulatory compliance, as well as specific retention periods for those records. MIFID II (new version) and MIFIR were issued in 2014.	EU	EU Commission	Financial Institutions		X			X	X
Solvency II (Directive (2009/138/EC)	Codifies and harmonises the EU insurance regulation for all 28 Member States; primarily this concerns the amount of capital that insurance companies must hold to reduce the risk of insolvency.	EU	EU Parliament	Financial Institutions					X	X
FINRA (Financial Industry Regulatory Authority Rule 2210)	Rule 2210 outlines the regulatory recordkeeping requirements for institutional communications (such as emails) including evidence that supervisory procedures have been implemented and carried out.	US	FINRA	Financial Institutions		X				X

Regulatory Compliance & EIM Requirements Quick Reference Guide

OPENTEXT™

About the Regulation					Enterprise Information Management (EIM) Requirement					
REGULATION OR STANDARD	SUMMARY DESCRIPTION	REGION	REGULATORS/ ENFORCERS	INDUSTRY	DATA PROTECTION & PRIVACY	RECORDS MGMT	E-DISCOVERY REQS	INFORMATION INTEGRITY & AUTHENTICITY	REPORTING OBLIGATIONS	PROCESS COMPLIANCE
SEC 17a-4	Requires that transaction records be retained and indexed on indelible media with immediate accessibility for a period of six months, and with non-immediate access for a period of at least two years. Duplicate records must also be kept within the same time frame at an off-site location.	US	SEC	Financial Institutions		X				
Bank Secrecy Act (aka Anti-Money Laundering [AML] law)	Requires financial institutions in the US to collaborate with U.S. government agencies to detect and prevent money laundering. Requires banks to report transactions involving more than $10,000 in cash from one customer as a result of a single transaction or two or more related transactions that occur within a 24-hour period. Also requires banks to report suspicious activity that might indicate possible money laundering or fraud.	US	SEC	Financial Institutions		X	X		X	
KYC (Know Your Customer)	The process used by a business to verify the identity of their clients. The objective of KYC guidelines is to prevent banks from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC processes are also employed by companies outside of the financial sector for the purpose of ensuring their third party partners' anti-bribery compliance.	Int'l	SEC	Financial Institutions and others		X			X	X

Regulatory Compliance & EIM Requirements Quick Reference Guide

OPENTEXT™

About the Regulation					Enterprise Information Management (EIM) Requirement					
REGULATION OR STANDARD	**SUMMARY DESCRIPTION**	**REGION**	**REGULATORS/ ENFORCERS**	**INDUSTRY**	**DATA PROTECTION & PRIVACY**	**RECORDS MGMT**	**E-DISCOVERY REQS**	**INFORMATION INTEGRITY & AUTHENTICITY**	**REPORTING OBLIGATIONS**	**PROCESS COMPLIANCE**
Gramm-Leach-Bliley	Requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. Consumers have the right to opt out of sharing their information. Act also requires a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' non-public personal information.	US	Several agencies including FFIEC, Federal Reserve, NCUA and OCC	Financial Institutions	**X**	**X**				**X**
PCI DSS	Developed by credit card companies as a collaborative effort to achieve a common set of security standards for the protection of (credit card) cardholder data *anywhere it resides within, or is transmitted by,* a merchant's system.	US and Int'l	PCI Security Standard Council	Retail	**X**					
Information Technology Act (ITA-2000 or IT Act)	The primary law in India dealing with cybercrime and electronic commerce. The Act also provides legal framework for electronic governance by giving recognition to electronic records and digital signatures, as well as includes recordkeeping obligations.	India	Indian Parliament	All	**X**	**X**		**X**		

Regulatory Compliance & EIM Requirements Quick Reference Guide

OPENTEXT™

About the Regulation					Enterprise Information Management (EIM) Requirement					
REGULATION OR STANDARD	**SUMMARY DESCRIPTION**	**REGION**	**REGULATORS/ ENFORCERS**	**INDUSTRY**	**DATA PROTECTION & PRIVACY**	**RECORDS MGMT**	**E-DISCOVERY REQS**	**INFORMATION INTEGRITY & AUTHENTICITY**	**REPORTING OBLIGATIONS**	**PROCESS COMPLIANCE**
USA Patriot Act (Uniting & Strengthening America by Providing Appropriate Tools Required to Intercept & Obstruct Terrorism)	AKA the Anti-Terrorism Law, the Act was passed in the wake of the Sept 11, 2001 terrorist attacks in the USA; its goals are to strengthen domestic security and broaden the powers of law-enforcement agencies with regards to identifying and stopping terrorists. This includes enforcement agencies ability to demand for the release of information and paperwork related to a US citizen person under investigation, order files from banks and from providers of communications services with details about specific customers' use of the service.	US	US Gov including Dep of Justice, FBI and INS	Horizontal		X	X			X
FCPA (Foreign Corruption Practices Act)	Comprised of two sections: (1) The Anti-Bribery Provisions make it a crime for any US person, business entity or employee of a US business entity to offer or provide, directly or through a 3rd party, anything of value to a foreign government official with corrupt intent to influence an award or continuation of business or to gain an unfair advantage. (2) The Accounting Provisions make it illegal for a company that reports to the SEC to have false or inaccurate books or records or to fail to maintain a system of internal accounting controls.	US and Int'l	SEC and Dept of Justice	All		X		X		

Regulatory Compliance & EIM Requirements Quick Reference Guide

OPENTEXT™

About the Regulation					Enterprise Information Management (EIM) Requirement					
REGULATION OR STANDARD	**SUMMARY DESCRIPTION**	**REGION**	**REGULATORS/ ENFORCERS**	**INDUSTRY**	**DATA PROTECTION & PRIVACY**	**RECORDS MGMT**	**E-DISCOVERY REQS**	**INFORMATION INTEGRITY & AUTHENTICITY**	**REPORTING OBLIGATIONS**	**PROCESS COMPLIANCE**
FDA 21 CFR Part 11	Requires most drug makers, medical device manufacturers, biotech companies, biologics developers, CROs, 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	US	FDA	Life Sciences		**X**		**X**		**X**
HIPAA (Health Insurance Portability and Accountability Act)	Privacy Rule (2003) of the Act regulates the use and disclosure of Protected Health Information (PHI) including in paper and electronic form held by "covered entities". Security Rule (2006) deals specifically with Electronic Protected Health Information (EPHI). It lays out three types of security safeguards required for compliance: administrative, physical, and technical.	US	US Gov	Healthcare	**X**					**X**

Regulatory Compliance & EIM Requirements Quick Reference Guide

OPENTEXT™

About the Regulation					Enterprise Information Management (EIM) Requirement					
REGULATION OR STANDARD	**SUMMARY DESCRIPTION**	**REGION**	**REGULATORS/ ENFORCERS**	**INDUSTRY**	**DATA PROTECTION & PRIVACY**	**RECORDS MGMT**	**E-DISCOVERY REQS**	**INFORMATION INTEGRITY & AUTHENTICITY**	**REPORTING OBLIGATIONS**	**PROCESS COMPLIANCE**
HITECH (Health Information Technology for Economic and Clinical Health) Act	HITECH is part of the American Recovery and Reinvestment Act of 2009 (ARRA). ARRA contains incentives related to health care information technology and specific incentives designed to accelerate the adoption of electronic health record (EHR) systems among providers. The Act also widens the scope of privacy / security protections for electronic protected health information (ePHI) available under HIPAA, increases the potential legal liability for non-compliance, and provides for more enforcement. The *Meaningful Use* provision is defined by the use of certified EHR technology in a meaningful manner (e.g. electronic prescribing); ensuring that the certified EHR system is connected in a way that provides for the electronic exchange of health info to improve the quality of care.	US	Department of Health and Human Services (HHS)	Healthcare	**X**	**X**				**X**
EU Pharmacovigilance	Protects public health by strengthening the current European-wide system for monitoring the safety of medicines. In particular, the new legislation aims to make the reporting of adverse drug reactions (or side effects) easier and introducing special provisions for medicines that need additional monitoring. The legislation also aims to ensure that members of the public become better informed about the benefits and risks of taking medicines.	EU	EU Commission	Life Sciences	**X**	**X**			**X**	**X**

Regulatory Compliance & EIM Requirements Quick Reference Guide

OpenText™

About the Regulation					Enterprise Information Management (EIM) Requirement					
REGULATION OR STANDARD	**SUMMARY DESCRIPTION**	**REGION**	**REGULATORS/ ENFORCERS**	**INDUSTRY**	**DATA PROTECTION & PRIVACY**	**RECORDS MGMT**	**E-DISCOVERY REQS**	**INFORMATION INTEGRITY & AUTHENTICITY**	**REPORTING OBLIGATIONS**	**PROCESS COMPLIANCE**
FDASIA (FDA Safety and Innovation Act)	Title 7 Section 706 Sec. 706, Records for Inspection: Allows the FDA to obtain certain records from a drug manufacturer in lieu of or in advance of an inspection. The request for records must include a description of the records requested, and the records shall be provided within a reasonable timeframe, within reasonable limits, and in a reasonable manner.	US	FDA	Life Sciences			X			
FSMA (FDA Food Safety Modernization Act)	Updates the role of the FDA in food safety in five key ways: 1. A shift of focus from reaction to prevention including thwarting intentional contamination. 2. More authority to scrutinize and assure compliance with inspection frequencies based on risk. 3. Mandatory recall authority. 4. Mandate to strengthen import safety to assure that US food safety standards are met 5. Stronger partnerships with other govt agencies and private entities.	US	FDA	Food Companies and Facilities		X			X	

Regulatory Compliance & EIM Requirements Quick Reference Guide

OPENTEXT™

About the Regulation					Enterprise Information Management (EIM) Requirement					
REGULATION OR STANDARD	**SUMMARY DESCRIPTION**	**REGION**	**REGULATORS/ ENFORCERS**	**INDUSTRY**	**DATA PROTECTION & PRIVACY**	**RECORDS MGMT**	**E-DISCOVERY REQS**	**INFORMATION INTEGRITY & AUTHENTICITY**	**REPORTING OBLIGATIONS**	**PROCESS COMPLIANCE**
FERC 18 CFR Part 35 & Part 284 and Compliance Order No. 717 (Federal Energy Regulatory Commission)	Compliance Order No. 717 requires that all emails, voicemail, text messages and other communication between energy companies' transmission and marketing functions must be retained for five years. Regulations 18 CFR Part 35 & Part 284 states that an electronic data retention policy is required for each entity under its jurisdiction. Data must be archived encrypted to WORM (write once read many) media. This data must be archived and available for 5 to 6 years.	US	FERC	Public Utilities, Natural Gas Companies, Electric Producers, Gas & Oil Production and Training.		X				X
Dodd-Frank Act Conflict Minerals Rule 1502	Rules requiring certain companies to disclose their use of conflict minerals if those minerals are "necessary to the functionality or production of a product" manufactured by those companies. Under the Act, those minerals are tantalum, tin, tungsten and gold (also known as 3TG).	US	SEC	Manufact-uring		X			X	

Regulatory Compliance & EIM Requirements Quick Reference Guide

OPENTEXT™

About the Regulation					Enterprise Information Management (EIM) Requirement					
REGULATION OR STANDARD	**SUMMARY DESCRIPTION**	**REGION**	**REGULATORS/ ENFORCERS**	**INDUSTRY**	**DATA PROTECTION & PRIVACY**	**RECORDS MGMT**	**E-DISCOVERY REQS**	**INFORMATION INTEGRITY & AUTHENTICITY**	**REPORTING OBLIGATIONS**	**PROCESS COMPLIANCE**
TSCA (Toxic Substances Control Act)	Regulates the introduction of new or already existing chemicals. Has reporting, record-keeping and testing requirements, and restrictions relating to chemical substances and/or mixtures. Certain substances are excluded from TSCA, including, among others, food, drugs, cosmetics and pesticides. Addresses the production, importation, use, and disposal of specific chemicals including polychlorinated biphenyls (PCBs), asbestos, radon and lead-based paint.	US	EPA	Manufact-uring		X			X	
Evidence Act	Regulates the rules of evidence in court proceedings under federal law. Section 31 refers to the requirements to prove authenticity and integrity of electronic records.	Canada	Gov Canada	All				X		
Data Protection Directive	Sets out the general principles with regard to the processing of personal information and free movement of such information; implemented in the national law of every EU member state.	EU	EU Commission	All	X					X
POPI (Protection of Personal Information Act)	Regulates the processing of personal information including collection, usage, storage, dissemination, modification or destruction.	South Africa	South African Gov	All	X					X

Regulatory Compliance & EIM Requirements Quick Reference Guide

OPENTEXT™

About the Regulation					Enterprise Information Management (EIM) Requirement					
REGULATION OR STANDARD	**SUMMARY DESCRIPTION**	**REGION**	**REGULATORS/ ENFORCERS**	**INDUSTRY**	**DATA PROTECTION & PRIVACY**	**RECORDS MGMT**	**E-DISCOVERY REQS**	**INFORMATION INTEGRITY & AUTHENTICITY**	**REPORTING OBLIGATIONS**	**PROCESS COMPLIANCE**
Sarbanes-Oxley Act (aka SOX)	Designed to protect shareholders and the public from accounting errors and fraudulent practices. Several sections of the Act related to document processing and retention: • Section 302 mandates that executives be held personally responsible for financial reports, requiring them to sign the documents. • Section 404 requires both the management of publicly held companies and outside auditor firms to report on the effectiveness of the company's internal controls. • Section 802 prohibits management from knowingly altering or destroying any documents related to a federal investigation or bankruptcy. In addition, external auditors must retain audit paperwork for five years.	US	SEC	All public companies		**X**		**X**		**X**

Regulatory Compliance & EIM Requirements Quick Reference Guide

OPENTEXT™

About the Regulation					Enterprise Information Management (EIM) Requirement					
REGULATION OR STANDARD	**SUMMARY DESCRIPTION**	**REGION**	**REGULATORS/ ENFORCERS**	**INDUSTRY**	**DATA PROTECTION & PRIVACY**	**RECORDS MGMT**	**E-DISCOVERY REQS**	**INFORMATION INTEGRITY & AUTHENTICITY**	**REPORTING OBLIGATIONS**	**PROCESS COMPLIANCE**
UK Bribery Act	Covers (1) the offering, promising or giving of a bribe (active bribery) and (2) requesting, agreeing to receive or accepting of a bribe (passive bribery), and commercial bribery (3) bribery of a foreign public official in order to obtain or retain business or an advantage in the conduct of business and (4) new form of corporate liability for failing to prevent bribery on behalf of a commercial organisation.	UK	UK Gov	All		**X**				**X**
Presidential Memorandum: Managing Government Records Directive	Requirements: • All permanent records must be managed in electronic format by 2019 • Email must be managed in electronic format in a Records Management system by 2016. • Increased visibility of privacy and compliance requirements such as FOIA and Privacy Act.	US	US Gov	Government	**X**	**X**		**X**		

Regulatory Compliance & EIM Requirements Quick Reference Guide

OPENTEXT™

About the Regulation					Enterprise Information Management (EIM) Requirement					
REGULATION OR STANDARD	SUMMARY DESCRIPTION	REGION	REGULATORS/ ENFORCERS	INDUSTRY	DATA PROTECTION & PRIVACY	RECORDS MGMT	E-DISCOVERY REQS	INFORMATION INTEGRITY & AUTHENTICITY	REPORTING OBLIGATIONS	PROCESS COMPLIANCE
FOIA (Freedom of Information Act)	Provides that any person has a right, enforceable in court, to obtain access to federal agency records, except to the extent that such records (or portions of them) are protected from public disclosure by one of nine exemptions or by one of three special law enforcement record exclusions. A FOIA request can be made for any agency record. The Act also requires that agencies automatically disclose certain information, including frequently requested records.	US	US Gov	Government	X		X			
E-Verwaltung or "OkeVa"	OkeVa stands for "Organisationskonzept Elektronische Verwaltungsarbeit", translated to "Organizational concept for electronic administration." The common name is "E-Verwaltung", or in English "E-Administration". Regulations and standards for records management, archiving and segregation for electronic files. It replaced the former DOMEA regulation.	Germany	Federal Ministry of the Interior	Government	X	X				X
GOBD	Principles on accounting rules for data access and retention of financial ledgers, recordings and documentation in electronic form. GOBD replaced GoBS and GDPdU rules in January 2015.	Germany	Federal Ministry of Finance	All	X	X				