Regulations

This appendix highlights a number of regulations; many of them are mentioned in this book and provide the framework for establishing an EIA vision that is aligned with the organization's strategic goals. In addition to addressing the specific business pain points of the organization, these regulations often act as the compelling driver for the execution of key enterprise and LOB-level IT initiatives that directly involve one or more components of the EIA. To help understand the relevant regulations and their scope, we have collected some information on each regulation, including:

- The name and country of the regulation where the regulation applies.
- The industries affected by the regulation, because many regulations apply to a broad base of organizations.

Regulation	Industry	Link	Notes
17 CFR Part 210, 1985, United States	Cross-industry, publicly held companies in the United States	http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title17/17cfr210_main_02.tpl	17 CFR Part 210 regulates the issuing of financial statements for all publicly held companies. The regulation covers areas such as the format and content of the statements, independence of auditors and independent reviews, and retention of records used in the production of the financial reports.
Bank Secrecy Act of 1970 (BSA or Currency and Foreign Transactions Reporting Act), United States	Banking and financial services, retail	http://www.fincen.gov/reg_main.html	This act is also known as the Currency and Foreign Transactions Reporting Act, and it requires financial institutions in the United States to assist government agencies to detect and prevent money laundering. Specifically, the act requires financial institutions to keep records and file reports of cash purchases of these negotiable instruments of $10,000 or more (daily aggregate amount) and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities. The BSA requires businesses to keep records and file reports that are determined to have a high degree of usefulness in criminal, tax, and regulatory matters. The reporting and record keeping requirements of the BSA regulations create a paper trail for law enforcement to investigate money laundering schemes and other illegal activities. This paper trail operates to deter illegal activity and provides a means to trace movements of money through the financial system. This law also covers the retail industry.
Basel II (2004), International	Banking and financial services	http://www.bis.org/publ/bcbs128.htm	Basel II, issued by the Basel Committee on Banking Supervision, enhances the recommendations of the Basel I Accord by defining three pillars that promote greater stability in the financial system. These pillars are: **1.** Basel II strengthens the measures used to assess the minimum amount of capital a financial institution must hold to mitigate against risk (market, credit, and operational). Operational risks require master data on customers, accounts, and contracts. **2.** Clarity on the steps that are used to control, manage, and monitor risk. A Supervisory Review specifies the internal controls to follow similar to those found in Sarbanes-Oxley sections 302 and 404 (specifically section 744 of Basel II). **3.** The transparency of public reports issued by the financial institutions. A Market Discipline framework provides guidance on the type of events and financial disclosures that should be provided by regulated companies to give insight into the financial state of the company. A newly expanded Basel Committee issued the latest package of measures to enhance the three pillars of the Basel II framework in July 2009.

Regulation	Industry	Link	Notes
Bundesdatenschutz-Gesetz (BDSG or Germany's Federal Data Protection Act), 1977, Germany	Government, companies in Germany	http://books.google.com/books?id=qulwlMLtwMQC&pg=PA14&lpg=PA14&dq=bdsg+germany&source=web&ots=8zhvsOOMw3&sig=vsSpP5vilBYLaFyiuNm5H29DwsU#PPA9,M1 http://www.privacy.de/recht/de/bdsg/bdsg01_eng.htm	BDSG imposes strong controls over the collection and dissemination of personally identifiable information by government and private businesses, and it is one of the oldest European data protection laws. These controls define how the information must be protected and the need for a data privacy officer. BDSG's strong guidelines define the rights of data subjects and how and when organizations should be allowed to collect and use personal information. BDSG was amended in 2005 to reflect the privacy controls specified by EU Data Protection Directive 95/46/EC.
California Security Breach Information Act (SB 1386), 2003, California, United States	Government, business, and any person that has computerized personally identifiable information on California residents	http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html	This is a California state law requiring organizations that maintain personal information about individuals to inform those individuals if the security of their information is compromised. The legislation considers a data breach to have occurred when unencrypted personal information has been acquired or can reasonably believed to have been acquired by an unauthorized person or organization. The Act, which went into effect July 1, 2003, was created to help stem the increasing incidence of identity theft. SB 1386 is the first law in the United States for data breach disclosures and is considered a model for similar laws in other states.
California's ePedigree law, 2009, California, United States	Pharmaceutical	http://www.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20071009005843&newsLang=en http://law.onecle.com/california/business/4034.html	In effect since January 2009, the California ePedigree law requires pharmaceutical manufacturers to create unique identifiers for drug information, track each product's pedigree, and maintain electronic records of the transactions in the supply chain. In January 2007, EPCglobal ratified the Pedigree Standard as an international standard that specifies an XML description of the life history of a product across an arbitrarily complex supply chain.
Data Protection Act of 1984, United Kingdom (updated in 1998)	All industries and businesses that maintain information on data subjects in the UK	http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1 http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx	The Data Protection Act 1998 (DPA), enacted by the UK Parliament, is the main piece of legislation that governs the protection of personal data in the UK. This legislation describes the rights of individuals to determine what information is being collected on them and how it is used and prescribes the principles that organizations must follow in handling personal information.

Regulation	Industry	Link	Notes
European Union (EU) Directive 95/46/EC on the Protection of Personal Data, 1995, European Union	Cross-industry	http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm	This is a European Union directive that regulates the processing of personal data within the union, and it is an important component of EU's privacy and human rights law. The directive was implemented in 1995 by the European Commission. This directive states that anyone processing personal data must comply with the enforceable principles of good practice it outlines that include: • Transparency • Legitimate purpose • Proportionality Data subjects are also given the right to view data collected on them and to object to the use of private data by a particular entity. The directive also states that the personal information must be protected from destruction, loss, and unauthorized disclosure and modification. The protection includes data as it as transmitted and while it is at rest.
EuroSox (EU), 2002-2006, European Union	Cross-industry, publicly held companies in the EU	http://www.copenhagencompliance.com/eurosox/WhatisEuroSox.pdf	EuroSox (the European version of SOX) is the nickname for a collection of legislation enacted between 2002 and 2006 targeted at improving transparency in corporate governance and increasing public confidence in European companies. The directives closely follow the U.S. regulations and affect only publicly traded companies. Some of the focus areas of the legislation are: • Strong internal controls on data used for financial reporting • Stricter corporate governance and reporting • Risk management • Independence and liabilities of auditors
Fair and Accurate Credit Transactions Act (FACTA), 2003, United States	Banking and financial services	http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ159.108.pdf	The Fair and Accurate Credit Transaction Act of 2003 (FACTA) added new sections to the federal Fair Credit Reporting Act (FCRA, 15 U.S.C. 1681 et seq.) which is intended primarily to help consumers fight the growing crime of identity theft. Accuracy, privacy, limits on information sharing, and new consumer rights to disclosure are included in FACTA. The act allows consumers to request and obtain a free credit report once every 12 months from each of the three nationwide consumer credit reporting companies. It furthermore mandates business processes to detect and mitigate against identity theft, such as using information from consumer reporting agencies and identifying suspicious documents and potentially suspicious use of personally identifiable information, such as handling problems reported when an individual changes addresses.

Regulation	Industry	Link	Notes
Health Insurance Portability and Accountability Act (HIPAA) of 1996, United States	Healthcare (including prescription drugs), insurance, and federal agencies dealing with patient information	http://www.hhs.gov/ocr/hipaa/	HIPAA was enacted by the U.S. Congress in 1996. It mandates the use of standards for the electronic exchange of medical records and regulations that protect health information, and it is intended to protect health insurance coverage for workers and their families when they change or lose their insurance. HIPAA ensures the confidentiality, integrity, and availability of Electronic Person Health Information (EPHI) received, created, or transmitted by: • Creating protection against any reasonably anticipated threats and risks to the security or integrity of EPHI • Requiring providers to create privacy policies and notify patients of those policies that give patients control over the use and disclosure over their health information • Protecting against uses or disclosures of EPHI that are not approved by the privacy rules and policies
Homeland Security Information Sharing Act (HSISA, H.R. 4598), February 2002, United States	Public sector	http://fas.org/sgp/congress/2002/hr3825.html	HSISA aims to provide for the sharing of homeland security information by federal intelligence and law enforcement agencies with sate and local entities. HSISA mandates that sensitive information deemed critical to the protection of the United States be shared among government security agencies and maintained in a secure fashion (for example, made available only to those who have a need to know) using a well-defined set of procedures. Many other nations have passed similar acts for sharing homeland security information by national intelligence agencies with local authorities and for determining the criteria about who should be considered a terrorist risk.
International Financial Reporting Standards (IFRS), International Accounting Standards Board (IASB), 2001	Cross-industry	http://www.iasb.org/IFRS+Summaries/Technical+Summaries+of+International+Financial+Reporting+Standards.htm	IFRS is a principles-based set of standards that establish broad rules and dictate specific treatments and the reporting measures used in the financial statements. IFRS goals include: • To develop a single set of high quality, understandable, enforceable, and globally accepted international financial reporting standards (IFRS) through its standard-setting body, the IASB • To promote the use and rigorous application of those standards • To take account of the financial reporting needs of emerging economies and small and medium-sized entities (SMEs) • To bring about convergence of national accounting standards and IFRSs to high quality solutions

Regulation	Industry	Link	Notes
Markets in Financial Instruments Directive (MiFID)	Banking and financial services	http://www.fsa.gov.uk/Pages/About/What/International/EU/fsap/mifid/index.shtml	MiFID is a core part of the EuroSox collection of regulations. The directive provides a harmonized regulation for investment services across the 30 member states of the European Economic Area (the 27 member states of the European Union plus Iceland, Norway, and Liechtenstein). The main objectives of the directive are to increase competition and consumer protection in investment services by fighting financial crimes in financial markets, especially dealing with *best execution*. (Stock brokers must strive to get the best possible results for their clients.) MiFID also requires that critical information is disclosed to investors at the right time and that conflicts of interests are avoided.
Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury and the Specially Designated Nationals (SDN) List, United States	Cross-industry, public sector	http://www.ustreas.gov/offices/enforcement/ofac/	The Office of Foreign Assets Control of the U.S. Department of the Treasury administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy, or economy of the United States. OFAC acts under presidential national emergency powers and authority granted by specific legislation to impose controls on transactions and freeze assets under U.S. jurisdiction. The Specially Designated Nationals (SDN) List is a publication of OFAC that lists individuals and organizations with whom U.S. citizens and permanent residents are prohibited from doing business. The SDN is related to aspects of Know Your Client (KYC) to verify that the customer is not on lists of known fraudsters, terrorists, or money launderers. OFAC publishes, updates, and maintains an integrated and comprehensive list of designated parties with whom U.S. persons are prohibited from providing services or conducting transactions and whose assets are blocked.
Part 7 of the Proceeds of Crime Act 2002 (PoCA), July 2002, United Kingdom	Banking and financial services	http://www.opsi.gov.uk/acts/acts2002/ukpga_20020029_en_22#pt7	Part 7 of PoCA defines money-laundering crimes. It lists the disclosures required by financial entities when dealing with cash or security transfers. PoCA tries to prevent the use of the commercial and banking system to would-be money launderers and establishes criminal penalties for noncompliance.

Regulation	Industry	Link	Notes
Personal Information Protection Law (PIPL) of 2003, Japan	Cross-industry, Japanese businesses, including foreign companies with operations in Japan	http://www.freshfields.com/publications/pdfs/places/11704.pdf	PIPL regulates the collection and handling of personal information by businesses in Japan, mandating specific controls around: • Using personal information only for clearly disclosed purposes • Protecting the security of the personal information • Acquiring personal information in a lawful fashion • Enabling individuals access to personal information collected by businesses • Ensuring that information is accurate and up to date • Protecting the security of the personal information • Restricting distribution of personal information to third parties PIPL is similar in nature to other data protection laws (such as UK Data Protection Act and EU Directive 95/46).
Personal Information Protection and Electronic Documents Act (PIPEDA) of 2000, Canada	Cross-industry, Canadian businesses, including foreign companies with operations in Canada	http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp	The purpose of the act is to establish rules to govern the collection, use, and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. PIPEDA requires companies to: • Obtain the clear consent of an individual before you collect, use, or disclose personal information about that individual. • Use the information only for the purposes for which you have consent. • Protect the information from unauthorized access and use. • Keep the information up to date and correctly filed so that decisions are based on correct information. • Destroy information when you no longer need it for the original purpose. • Implement accountability mechanisms in your organizations to ensure compliance with the previous.

Regulation	Industry	Link	Notes
Sarbanes-Oxley Act of 2002 (SOX or Public Company Accounting Reform and Investor Protection Act), United States	Cross-industry, publicly traded companies in the United States	http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.tst.pdf	The Sarbanes-Oxley Act of 2002 (SOX) is legislation enacted to protect shareholders and the public from accounting errors and fraudulent practices in the enterprise. The act is administered by the SEC, which sets deadlines for compliance and publishes rules on requirements. The legislation not only affects the financial side of corporations, but it also affects the IT departments in charge of storing the corporation's electronic records. SOX states that all business records, including electronic records and electronic messages, must be saved for "not less than five years." Of the many components of SOX, some of the ones that have received the most attention in the IT community include: Section 404, which mandates that management is responsible for establishing adequate internal controls and processes for financial reporting and that an independent assessment be produced yearly of those controls (along with Section 302, which requires company officers to certify the correctness of financial reports). The SEC guidance on Section 404 is derived from the COSO framework on internal controls. Section 401, which requires companies to list balance sheet arrangements (such as leases, long-term purchase agreements, long-term debt obligations, and so on) that have a material effect on the financial health of the company. Section 409, which requires real-time disclosure of material changes in the course of business that might significantly affect the health of the business. The SEC interpreted this section as adding 11 new events (such as new or terminated significant material agreements, off balance sheet obligations, and so on) to the nine existing events that would trigger a disclosure. Sections 802(a), 802(a)(1), and 802(a)(2) that affect the management of electronic records including destruction, alteration, or falsification of records and the retention period for records storage. J-SOX, The Financial Instruments and Exchange Law, was enacted in June 2006, and it is the main statute codifying securities law and regulating securities companies in Japan.

Regulation	Industry	Link	Notes
Solvency II, European Union	Insurance	http://ec.europa.eu/internal_market/insurance/solvency/index_en.htm	Solvency II includes the set of regulatory requirements for insurance firms that operate in the European Union, and it is often considered as the equivalent to Basel II for the Insurance Industry. Solvency II derives from the Financial Services Action Plan (FSAP). This regulation introduces a comprehensive framework for risk management for defining required capital levels and to implement procedures to identify, measure, and manage risk levels. Solvency II has three pillars representing risk assessment and capital reserves, pro-active risk management, and accurate disclosure of relevant financial information.
The Do-Not-Call Implementation Act of 2003, United States and 2006, Canada	Cross-industry, telecommunication, public sector	http://www.ftc.gov/bcp/edu/microsites/donotcall/index.html https://www.lnnte-dncl.gc.ca/index-eng	The Do-Not-Call List is a registry intended to give U.S. consumers an opportunity to limit the telemarketing calls they receive. Telemarketers are required to subscribe to the National Do Not Call list and abide by citizen requests, including updating their lists every 31 days. In Canada, the Canadian Radio-Television and Telecommunications Commission enacted the National Do Not Call List (DNCL) Act in 2006 to give consumers a choice about whether to receive telemarketing calls. As in the United States, Canada's National DNCL Rules introduce new responsibilities for telemarketers.
The Third European Money Laundering Directive (3 MLD)	Banking and financial services, legal, gaming	http://www.hm-treasury.gov.uk/media/D/5/200509RIA1.pdf	This directive, enacted by the European Union in 2005, is focused on discovering money laundering before the money is used to finance a terrorist operation. It enhances the due diligence ("Know Your Customer") required of the affected industries and increases the number of affected industries by specifically: • Imposing identity checks on customers opening accounts • Applying identity checks to any check transactions over €15,000 • Forcing stricter checks on politically exposed persons • Specifying penalties for failure to report suspicious transactions to national financial intelligence units
Financial Crimes Enforcement Network (FinCEN), 1990, United States	Banking and financial services	http://www.fincen.gov/	FinCEN is a bureau of the United States Department of the Treasury established in 1990 to safeguard financial systems from abuse by promoting transparency in the United States and international financial systems. In 1994, FinCEN's responsibilities were broadened to include the facilitation of the Bank Secrecy Act (BSA) of 1970, which is the main U.S. anti-money laundering legislation. To uncover and prevent money laundering, FinCEN, under the auspices of the BSA, requires financial institutions to record and report suspicious activity that might signify money laundering and fraud.

Regulation	Industry	Link	Notes
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, USA PATRIOT Act, 2001, USA	Cross-industry	http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.03162:	The PATRIOT Act increases the capabilities of law enforcement agencies to search telephone, e-mail communications, medical, financial, and other records. It eases restrictions on foreign intelligence gathering in the United States. It expands the Secretary of the Treasury's authority to regulate financial transactions, particularly those involving foreign individuals and entities. It gives law enforcement and immigration authorities discretion in detaining and deporting immigrants suspected of terrorism-related acts. The Act enhances existing regulations on businesses around Anti-Money Laundering (AML), Know Your Customer (KYC), and Customer Due Diligence (CDD). Core requirements of the legislation for the financial industry are that institutions must keep stricter records on transactions, must increase their efforts to identify the true owners of accounts, keep track of political figures associated with accounts where there is a strong possibility of corruption, and limit or deny certain types of activities.