Realtime publishers

The Shortcut Guide™ To

Understanding Data Protection from Four Critical Perspectives

sponsored by

CREDANT®

We Protect What Matters

Rebecca Herold

Chapter 4: What IT Operations Need to Know About Data Protection Implementation 62
1980s 62
1990s 63
2000s 63
IT Operations' Data Protection Responsibilities 64
1. Identify IT Security and Privacy Risks 64
2. Identify Common Requirements 64
3. Map Compliance Requirements to Risks 64
4. Establish Systems and Applications Controls 66
Enable System Events (Logging) 66
Log Successful Access Attempts to PII and Mission-Critical Resources 66
Make Data Backups 66
Establish Access Controls Based Upon Job Responsibilities 66
Require Authentication 66
Encrypt PII 67
Restrict Inbound Internet Traffic 67
Limit Unsuccessful User ID Login Attempts After Three Consecutive Unsuccessful Tries 67
Implement Tools to Prevent Malicious Code Attacks 68
Implement Intrusion Detection and Incident Monitoring Tools 68
5. Unify Data Protection Compliance Activities 68
Preventing Common IT Data Protection Blunders 69
Breaches Resulting from Test and Development 69
Legal Restrictions Against Using Production PII 70
For Compliance Sake, Avoid Using PII Whenever Possible 71
Case Studies 71
Case 1: IT Controls to Mitigate Insider Threats 71

Case 2: IT Controls to Mitigate Yet More Insider Threats 73
Key IT Data Protection Deployment Activities 74
Project Envision and Start Up 74
Business Requirements 75
Functional Specifications 75
Technical Specifications and Design 76
Coding 76
Testing 77
Delivery and Deployment 77
Post-Implementation Review 78
Maintenance 78
Retirement 79
IT Data Protection Compliance Commonalities 79

Copyright Statement

Chapter 4: What IT Operations Need to Know About Data Protection Implementation

IT folks used to have the corner on data protection because, long ago and far away, business technology was highly centralized and relatively easy to protect. However, over the past couple of decades, technology has exponentially increased in complexity and openness, creating new and unanticipated data protection challenges for IT leaders and practitioners that must be effectively addressed.

1980s

One of my earlier professions was as a systems analyst and programmer. At that time, in the late 1980s, data protection was relatively "easy." Most systems were closed systems. The network users were on terminals that just glowed green data at them on the screens and did not allow them to install any type of software or data into the network other than through controlled applications input screens.

> **NOTE**
> A "closed system" with regard to a computer network is basically one that has no outside connections, and one on which the network users cannot establish outside connections.

The only feasible way in which end users could take any data off the system was through hardcopy printouts. It was common to use production data for test and development purposes. In fact, if you didn't use production data to test, it was widely considered that your testing would not be as comprehensive as possible and that you could not test for actual business purposes adequately. IT was very isolated.

1990s

Then came the 1990s and the legendary Novell NetWare servers that the business folks loved, ushering in distributed file servers that were managed by personnel in multiple business units outside of the corporate IT area. These servers provided new capabilities for end users to upload files and applications onto the corporate network. The corporate IT departments in most companies at first said, "Oh, we don't support those." So business units created their own IT teams to manage their own file servers. IT silos were born, scattered throughout the enterprise and very disconnected. Much confusion and uncoordinated computing ensued. Much of the latter 1990s was spent trying to get scattered file servers to talk with mainframes, and then to put them all behind firewalls to all Internet connections. The business units all viewed those activities as IT responsibilities, and they basically used what was given to them without really thinking much about information protection issues.

2000s

Then came Y2K, and even more types of technologies, and vastly more mobility. More mobile computers. More mobile storage devices. More mobile working. The silos and separation of IT from business lost effectiveness. Data protection lost effectiveness. IT areas became more important than ever for providing the safeguards for the enterprise data assets.

New technologies and practices will continue to grow over the next few years. Just think about all the new technologies widely used, and increasingly used, within organizations by the population at large, often without the knowledge of business leaders:

- Social networking sites
- Microblogs, such as Twitter
- Voice over IP (VoIP)
- Instant messaging
- Online collaboration sites, such as SharePoint
- Video sites, such as YouTube

In addition to new technologies, mobile computing and mobile data (passing through networks as well as moving on human legs within mobile storage devices) must also be protected. But how can organizations do so effectively? How can IT do so effectively?

What is your IT area doing to protect the confidentiality, integrity, and accessibility of sensitive information that may be located in, or accessed by, these new technologies? You cannot provide effective data protection unless you know where data resides. In all locations. And in all forms. Safeguards are critical in all places where information is accessed and stored, both inside the corporate walls and, very importantly, in all locations outside the four walls.

IT Operations' Data Protection Responsibilities

IT leaders, administrators, developers, architects, and others who are the digital information custodians of the enterprise and are responsible for implementing security controls must understand the criticality and importance of their roles to ensuring data protection safeguards are effectively implemented and maintained.

A simple but effective roadmap for IT to follow to help them address important IT data protection requirements includes the following steps:

1. Identify IT security and privacy risks
2. Identify common data protection compliance requirements
3. Map the compliance requirements to the risks
4. Establish systems and applications controls
5. Monitor, manage, and update the IT data protection practices

1. Identify IT Security and Privacy Risks

Perform information security risk assessments, preferably in conjunction with a privacy impact assessment (PIA), to determine and rank, as much as possible, identified IT risks. A common link within most compliance requirements is to establish controls that are appropriate for the organization's identified information security and privacy risks, so risk identification is a critical component of IT data protection activities, but is unfortunately too often overlooked.

2. Identify Common Requirements

When the information security, privacy, and compliance officers and/or the legal counsel direct the IT area to "Get the systems in compliance!" what should IT leaders do? They should identify common requirements throughout all the applicable laws, regulations, standards, and contractual requirements.

3. Map Compliance Requirements to Risks

They should map the commonalities within a matrix that can then be used for easy reference to clearly see all the commonalities. Table 4.1 lists many, but far from all, the activities IT areas can perform to support compliance throughout the indicated laws and standard.

IT Activities Supporting Compliance	Laws & Standard (See legend below)							
	A	B	C	D	E	F	G	H
Enable system events (logging)	X	X	X	X	X	X	X	X
Log successful access attempts to mission-critical resources	X	X	X	X	X	X		
Make data backups		X	X	X	X	X	X	X
Establish access controls based upon job responsibilities	X	X	X	X	X	X	X	X
Require authentication	X	X	X	X	X	X	X	X
Encrypt personally identifiable information (PII)		X	X		X		X	X
Restrict inbound Internet traffic to the DMZ		X	X	X	X	X		
Limit unsuccessful user ID login attempts after three consecutive unsuccessful tries		X	X	X	X			
Implement tools to prevent malicious code attacks		X	X	X	X			
Implement intrusion detection and incident monitoring tools	X	X	X	X	X	X		

Table 4.1: Windows server common data protection compliance requirements.

Legend

A—Sarbanes Oxley (SOX) Act

B—Gramm-Leach-Bliley Act (GLBA)

C—Payment Card Industry Data Security Standard (PCI DSS)

D—Federal Information Security Management Act (FISMA)

E—Health Insurance Portability and Accountability Act (HIPAA)

F—Fair and Accurate Credit Transactions Act (FACTA)

G—Canada's Personal Information Protection and Electronic Data Act (PIPEDA)

H—European Union's Data Protection Directive

This matrix may look slightly different from organization to organization. Go over this table with your legal counsel or information security department. Whether you need to undertake these activities for compliance will depend upon your own unique organization and your lawyer's interpretation of the law as it applies to your business and industry.

4. Establish Systems and Applications Controls

Once the risks and compliance requirements for data protection are identified, establish and implement appropriate controls. There are significant common core requirements across the many laws, regulations, and industry standards that organizations should recognize and use as keystones within their information security and privacy programs. IT leaders can use internationally-accepted as well as industry standards to address the requirements in a unified way to reduce costs, save time, and increase the effectiveness and scope of information security and privacy programs. The following sections highlight common data protection activities that IT areas must undertake to provide the most effective data protection for electronic business assets.

Enable System Events (Logging)

Almost every data protection law, regulation, and standard requires that organizations be able to determine who has accessed sensitive business assets, such as PII, along with the details around that access. Not only is this a compliance requirement, it is a necessity for ensuring effective data protection.

Log Successful Access Attempts to PII and Mission-Critical Resources

Even if individuals have authorized access to network resources, organizations must be able to determine when those individuals used that access and what they did with it.

Make Data Backups

Another key component for data protection compliance is ensuring the availability of PII and other mission-critical resources. IT must make backups of PII and related data to comply with availability requirements.

Establish Access Controls Based Upon Job Responsibilities

A common compliance requirement is to restrict access to applications, data files, and other network resources to only those who have a specific business need to have that access.

Require Authentication

Across the board, laws, regulations, and industry standards require organizations to implement authentication, allowing only one person to use each user ID. They do so not only to establish accountability for access activities but also to be able to track and determine when individuals have been in systems with PII.

Encrypt PII

Laws in Massachusetts and Nevada, along with the recently implemented HITECH Act, require PII to be encrypted. Most other laws and regulations also list encryption as a PII-protection method that organizations must consider. In addition, multiple regulatory oversight guidance documents encourage organizations to encrypt PII. Additionally, PCI DSS requires encryption in certain situations. IT should encrypt PII whenever possible to meet current and emerging legal, regulatory, industry standard, and contractual requirements.

RESOURCES

See the Massachusetts law at http://www.mass.gov/Eoca/docs/idtheft/201CMR17amended.pdf

See the Nevada law at http://www.leg.state.nv.us/73rd/bills/SB/SB347_EN.pdf

See the HITECH Act requirements at http://waysandmeans.house.gov/media/pdf/111/hitech.pdf

Restrict Inbound Internet Traffic

Many data protection requirements advise organizations to establish barriers into the corporate networks from outside public networks, such as the Internet. For example, PCI DSS specifically states in Requirement 1, "All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employees' Internet access through desktop browsers, employees' email access, dedicated connection such as business to business connections, via wireless networks, or via other sources."

Limit Unsuccessful User ID Login Attempts After Three Consecutive Unsuccessful Tries

Some regulations, laws, and industry standards require user accounts to be locked after a specific number of unsuccessful attempts, such as six within PCI DSS. However, others require accounts to be locked according to best practices, such as indicated within NIST documents, which specify that accounts should be locked after three unsuccessful attempts.

RESOURCES

Just two of many NIST documents that address ID and password security include:

NIST Special Publication 800-53 Revision 3 "Recommended Security Controls for Federal Information Systems and Organizations" from http://csrc.nist.gov/publications/drafts/800-53/800-53-rev3-FPD-clean.pdf

NIST Special Publication 800-118 (Draft) "Guide to Enterprise Password Management" from http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf

Implement Tools to Prevent Malicious Code Attacks

Many data protection requirements specify that organizations must implement technologies and procedures to guard against, detect, and report malicious code. IT leaders must ensure up-to-date antivirus and malicious code prevention systems are implemented and appropriately managed.

Implement Intrusion Detection and Incident Monitoring Tools

Most data protection requirements indicate that organizations must implement tools and procedures to prevent network intrusions. For example, GLBA requires organizations to implement, based upon the results of risk analysis, intrusion detection and incident monitoring tools to be used for "detecting, preventing and responding to attacks, intrusions, or other systems failures."

5. Unify Data Protection Compliance Activities

By implementing a core set of controls throughout the enterprise network and computer devices, IT can help the organization meet compliance with numerous applicable laws, regulations, and industry standards. The bottom line to make IT compliance responsibilities and activities as effective, efficient, and manageable as possible is to:

- Configure systems to disallow all access to PII and mission-critical data and allow access to only those with specific job responsibilities
- Create procedures to support compliance with the most applicable laws, regulations and industry standards, and contractual requirements as possible based upon topics and not based upon taking a piecemeal approach
- Speak with the information security, privacy, and/or compliance departments to continue documenting the list of common compliance requirements that I started for you in Table 4.1
- Document all decisions for your IT systems settings; auditors always want to see documentation of this type for all types of compliance reviews
- Check out the existing matrices showing common compliance requirements at sites such as the IT Unified Compliance site (www.unifiedcompliance.com); be sure to check with your information security, compliance, privacy, or legal counsel to ensure the suggested compliance activities are, indeed, necessary for your own organization based upon their interpretation
- Install encryption solutions on mobile endpoint devices, such as laptops, USB storage drives, and smart phones. These types of devices often contain PII and other sensitive information, and they are often lost or stolen, putting the data on them at risk. In addition to protecting the data, growing numbers of laws, such as those from Massachusetts and Nevada, require PII on these types of devices to be encrypted.
- Implement procedures and tools to monitor PII, and other types of sensitive information, and keep it from being copied to mobile devices and external locations.

Preventing Common IT Data Protection Blunders

It is important to establish IT requirements and manage data protection technologies to support business as well as to address compliance. When IT leaders ensure a comprehensive, risk-based data protection plan is implemented, they will avoid many common IT blunders. Let's consider just a few of them.

Breaches Resulting from Test and Development

Privacy breaches involving production PII used for test and development purposes are increasing in number, as are the associated risks. Additionally, legal restrictions against using production PII for test and development purposes are on the rise and increasingly being enforced.

IT test environments are inherently less secure than in production because data is typically exposed to a wider variety of "insider" sources without a clear business need for access, including in-house testing staff, outside contractors and consultants, partners, and increasingly offshore development shops. Although many of the incidents by insiders is a result of malicious intent, a large number of breaches is caused by the developers being unaware of the basic security that needs to be in place, or as a result of accidents and negligence. No matter the reasons, these insider incidents can be very costly to both the company and the individuals involved.

Consider just one of the many incidents where privacy breaches resulted from using production PII for test and development. In June 2006, a programmer hired to create an application for the Sentry Insurance Company in Wisconsin was sentenced to 60 months in prison and fined $519,859 for attempting to sell more than 111,000 individuals' Social Security Numbers and other PII to an undercover US Secret Service agent. The programmer had taken the data from the insurance company where he was working as a business software consultant and had been given the data to use for development and testing. The programmer had also sold the data to others before being caught.

Test data is vulnerable to not only malicious intent but also basic unawareness and mistakes. A couple of years ago, an e-discovery company was at a conference I attended and giving a demonstration of their product to a large number of folks in the vendor exposition area. The data they were using was the actual sensitive employee and customer PII from one of their large clients. Following the presentation, the vendor reps told me they hadn't thought about the privacy or legal issues involved with using actual PII.

Multiple studies confirm that the insider threat is the cause of the majority of information security incidents and privacy breaches that occur. The current abysmal US economy provides even more motivation for insiders with access to sensitive information to purposefully do bad things. A December 2008 report by IBM's ISS X-Force research team reported a 30% increase in network and Web-based security incidents during the last half of 2008, much of this increase attributed to economic fear.

Another December 2008 report by Cyber-Ark Software also confirmed this upturn in insider-caused incidents. It reported 56% of workers are worried about job loss, and that 58% of U.S. workers said they have "already downloaded competitive corporate data and plan to use the information as a negotiating tool to secure their next post." 71% indicated that if they were laid off, they would definitely take company data with them to their next employer, with the most likely data being "customer and contact databases, with plans and proposals, product information, and access/password codes."

Legal Restrictions Against Using Production PII

Most data protection laws throughout the world are designed to protect the privacy of individuals by placing significant and specific restrictions on the ways in which organizations can use PII. For example, any organization that collects PII from citizens in the 27 EU countries must abide by Data Protection Directive 95/46/EC and any additional restrictions each member country has established.

It is common for organizations to use PII in ways that breach the EU Data Protection Directive requirements. The financial consequences of such breaches can be significant, and if a security incident occurs that results in PII being misused, the consequences are dramatically increased.

These restrictions, as well as the restrictions in most data protection laws outside the US, are based upon eight privacy principles. The principles that are directly applicable to restricting use of PII for test purposes include the following:

- Principle 1—Fair and Lawful Processing. To be 'fair' individuals must be given notice about why their PII is collected and how their PII will be used. These notices rarely state the PII will be used for testing purposes. So, when organizations use their existing customer PII to do such testing and development, they are violating the data protection laws. There is usually a legal obligation to mask or de-identify PII when possible for testing.

- Principle 3—Excessive Data. This requires organizations to process only the minimum data necessary for the business reasons for which it was collected. So, even when PII can be justified for testing, the quantity of PII must be limited. Using a sub-set of PII is more likely to comply with data protection requirements than is using an entire database.

- Principle 7—Security. Organizations must use appropriate security measures to protect PII. What is 'appropriate' will depend on many factors, such as the organization's size, type of PII used, and so on. Generally, the larger the organization, the more security that is expected to be used. Similarly, the more 'sensitive' the data, and the more databases used, the more security organizations are expected to implement. This security includes required training and awareness activities for the personnel with PII access. When an outsourced company is used, most data protection laws require contracts to include specific security requirements for the vendor to follow, including training.

- Principle 8—Cross Border Data Transfer. Organizations cannot send PII across country's borders unless it is for 1) legitimate business purposes, and 2) it goes to a county considered as "safe," or a specific cross-border agreement is in place between the organization and the applicable countries. The EU does not consider the US a "safe" country.

For Compliance Sake, Avoid Using PII Whenever Possible

The bottom line is, to comply with worldwide data protection laws, it is most effective for IT developers and testers to not use PII unless it has been de-identified or masked. In circumstances where using PII is unavoidable, the quantity of PII should be reduced to the bare minimum necessary for testing. When a third party does development and/or testing, make sure the appropriate contracts and safeguards are in place.

Case Studies

It is often helpful to look at the information security incidents that have actually occurred to try to identify the possible reasons things went wrong, then use those lessons to implement controls within your own organization to keep similar incidents from occurring. The following sections highlight case studies that demonstrate the importance of IT controls for data protection.

Case 1: IT Controls to Mitigate Insider Threats

In May 2008, Lending Tree got slapped with a civil suit alleging their personnel allowed mortgage lenders access to customers' PII and other confidential information because of poor application controls, which required customers to access their personal account information online using a user ID and password (single-factor authentication). The suit charged that Lending Tree did not have appropriate or adequate information safeguards in place, resulting in the lenders using customer names, addresses, phone numbers, Social Security Numbers, income information, and assorted other personal information, to market their own mortgage loans to the Lending Tree customers. What are some IT controls that can be used to prevent employees, contractors, or anyone outside of the organization for that matter, from accessing and stealing sensitive customer information?

- Some of the inappropriate access may have occurred by the employees, contractors, and/or lenders using customer IDs and either knowing or guessing the customer's passwords used to access accounts. This situation shows how customers depending upon single-factor authentication (a password only, in this case) can be easily defeated by trusted insiders or by simple password cracking. Some ways to mitigate the related risks:
    - Require strong passwords that cannot be found in dictionaries or be easily guessed
    - Encrypt passwords in storage
    - Mask passwords on computer screens
    - Encrypt passwords in transit through all networks
    - Require multi-factor authentication for customer accounts to help ensure others cannot just guess passwords
- Some of the inappropriate access could have occurred by employees and contractors directly accessing customer data in storage. Some ways to mitigate the related risks:
    - Encrypt customer data encrypted in storage
    - Log all accesses to customer data in storage
- Some of the inappropriate access could have occurred by having inappropriate access controls set for the applications that access the customer data. Some ways to mitigate the related risks:
    - Allow only those employees and contracted personnel access to customer files through the application that have a documented and valid business need to fulfill job responsibilities
    - Program the application to log the ID, password, date, and time of each access to a customer file
    - Do not allow customer information to be printed

These are just a few of the ways in which the risks could be mitigated. What other IT controls can you think of?

Case 2: IT Controls to Mitigate Yet More Insider Threats

In March 2008, the presidential candidates' passport files were widely reported as being breached on government computers because they were inappropriately accessed by contracted workers, who then are suspected of sending the files, or file details, to others. The State Department's computer system had flagged each incident, but IT did not notify senior department officials until after reporters asked the senior department officials if the files had been improperly accessed. There were many information security and privacy issues involved with this incident. Some questions that IT personnel could answer include:

- Why did the peeping personnel have access to the files? Did they have applications and/or systems authorization? Were they using someone else's account? Did the applications that controlled access to the passport files not have appropriate security built in?
- It was reported the peepers were contract workers from Analysis Corp. of McLean, Va., and Stanley Inc., of Arlington, Va. Did the State Department contract require the workers to have appropriate training? Did the contracted company have information security policies as part of a comprehensive information assurance program? Did the State Department provide training to the contract workers prior to giving them access to the network and data?
- Will the State Department cancel the contracts with Analysis Corp. and Stanley Inc.? Should they? Why or why not?
- What groups of personnel should have access to the passport files? How is access authorization determined? Do policies exist, along with supporting procedures?
- Why were a couple of the contractors fired and the other was not? What problems could this inconsistent application of sanctions cause?
- Hillary Clinton's file was accessed during a training session. Discuss the legal implications of using production data for test, development, and training. Discuss what this case points out to be poor training practices.
- The passport files reportedly contained date and place of birth, occupation, family status, physical characteristics, copies of birth or baptismal certificates, medical, personal and financial reports or arrest warrants, and the individual's Social Security Number. Discuss the ways in which these types of information could be used maliciously. Think about not only how such information can be used maliciously for any individual but also for individuals who are running for president.

- The inappropriate access was flagged as a result of a "software system that alerts supervisors when files of a 'high-profile person' are searched." Should such alerts be generated for all persons, not just for high-profile persons? Why or why not?
- Shouldn't the PII be encrypted in storage? If not, under what circumstances?
- What safeguards should be considered to prevent this type of privacy breach?
- What responsibilities should the State Department have for this privacy breach? Should they be sanctioned? In what ways?

Key IT Data Protection Deployment Activities

IT operations leaders can dramatically improve upon information security for their electronic systems, applications, and data by incorporating information security and privacy checks, controls, and safeguards throughout the entire systems and applications life cycle. By identifying risks at each stage and then implementing the appropriate security controls to address them, the result will be a much more secure digital enterprise.

Project Envision and Start Up

When making a decision about implementing or updating a system or application, think about and document the related data protection requirements. Typical objectives for this phase include:

- The project is envisioned and approval requested
- A sponsor and budget are identified
- Resources to support the project are identified
- Preliminary project plan estimates are made
- Management review and approval will occur if the project is going forward

Key IT data protection activities:

- Determine whether PII is involved; if it is, there are legal requirements for protecting it
- Determine whether PII is stored or sent outside of your controlled corporate network; if it is, plan to use encryption for data in transit and in storage locations
- Communicate risks and related mitigation costs, such as for encryption solutions, upfront to the business sponsor for the application and/or system

Business Requirements

When identifying the business requirements, keep in mind any related data protection and privacy issues. A business requirements team will typically be involved that should have the business requirements documented. The typical objectives for this phase include:

- Document business requirements
- Document types of information involved

Key IT data protection activities:

- Document data protection safeguards that will be needed for sensitive data, such as PII
- Identify the information security and privacy policies and standards that will need to be followed to support the business requirements
- Identify groups of applications and systems users that will need privacy and security training
- Perform a preliminary risk assessment and security categorization showing information items, applicable legal requirements, and identified threats

Functional Specifications

After the business requirements have been determined, it is time to start digging deeper into details for the functional specifications. This point is critical for identifying IT security and privacy issues. Unfortunately, such issues are often not considered during this phase, leading to unsafe applications and systems after they have gone into production. The typical objectives for this phase include:

- Finalize business requirements and related functional specifications
- Develop use cases and finalize process flows
- Obtain business owner approval

Key IT data protection activities include:

- Reviewing functional specifications to determine necessary confidentiality, integrity, and availability safeguards
- Determining costs and feasibility of safeguards
- Incorporating information security and privacy checks into IT use cases and story boards
- Incorporating the preliminary information security technical architecture
- Addressing emerging technologies that may be associated with the functional specifications, such as cloud computing, online collaboration tools, Twitter, instant messages, VoIP, social networking, videos, photos, and so on

Technical Specifications and Design

After knowing the functional specifications and identifying the related technologies, IT can identify the technical specifications and designs necessary to support them. The typical objectives for this phase include:

- Engage the development team to review the business specifications and map to corresponding technical specifications and design requirements
- Create a preliminary technical infrastructure design
- Create any necessary database design
- Create any necessary data conversion plan
- Perform a detailed design review

Key IT data protection activities include:

- Identifying and documenting the specific security and privacy policies and standards that cover the proposed technical specifications
- Documenting necessary IT security and privacy requirements and technologies specific to the specifications, such as encryption, authentication mechanisms, access controls, digital signatures, and so on
- Documenting IT business continuity and disaster recovery issues
- Documenting IT records retention requirements

Coding

Once the technical specifications and plans are finalized, it is time to start coding. A different team than the one that created the technical specifications typically does the coding, so it is critical that the IT information security and privacy specifications are comprehensive and clearly documented in the previous phase. The typical objectives for this phase include:

- Develop code using secure development techniques and standardized security and privacy coding procedures
- Create and review the testing strategy
- Establish code version controls
- Perform code reviews

Key IT data protection activities include:

- Ensuring IT security and privacy coding techniques and procedures are followed
- Developing IT security and privacy code test cases
- Incorporating IT security and privacy checks within the code review

Testing

Testing is critical for information security and privacy due diligence in the IT areas. Comprehensive tests, as identified and documented in the previous phase, must occur. Typically, a different team does the testing than those who created the code and the test cases. It is important that those testing have a good understanding of information security and privacy concepts so that they know problems when they see them, so ongoing training and awareness for this group is essential. The typical objectives for this phase include:

- Establish developer and QA testing
- Create an operating and training manual plan
- Create a deployment plan
- Produce a test summary report

Key IT data protection activities include:

- Conducting IT privacy and security tests
- Performing IT security and privacy penetration and vulnerability tests as are appropriate
- Performing applications and/or systems security and privacy certification
- Establishing the first draft of the operating and training manual, including security and privacy features.

Data protection cannot be effective unless information security and privacy testing is an integral part of the software testing process. Comprehensive information security and privacy testing during development enables IT to identify functional issues early, when they are easier and less expensive to fix.

Delivery and Deployment

After thorough testing, it is time to plan for a smooth deployment. This critical point often reveals significant security and privacy problems that were not properly addressed during development. Such oversights have often resulted in significant security incidents and privacy breaches. The typical objectives for this phase include:

- Deploy application
- Provide end-user training
- Publish the operating and user manuals
- Transition to operational support

Key IT data protection activities include:

- Ensuring security and privacy re-certification and re-accreditation once the system and/or application are deployed
- Implementing an IT security and privacy assessment and monitoring plan after the application and/or system is in production
- Ongoing security and privacy compliance monitoring

Post-Implementation Review

After the application and/or system has been put into production, and ongoing support and maintenance has been passed on to a different team, the development team needs to review the project and determine the things that worked well, as well as the things that need improvement. The typical objectives for this phase include:

- Document lessons learned from team
- Obtain end-user feedback
- Document necessary improvements for the systems and applications development process

Key IT data protection activities include:

- Performing an information security and privacy process lessons learned analysis
- Documenting key security and privacy issues that proved to be the biggest challenges, and how to make them work easier in the next project

Maintenance

The day-to-day IT maintenance and operations teams now must work to ensure the applications and systems continue to work smoothly as intended as well as be on the alert for any potential problems. The typical objectives for this phase include:

- Transition to operations completed
- Change control management
- Incident and problem management
- System disposal (also commonly called disposition) plan (where applicable)

Key IT data protection activities include:

- Performing information security and privacy configuration management and maintenance
- Ensuring adequate consideration of the potential security and privacy impacts due to specific changes to an information system or its surrounding environment
- Following secure change control procedures and ensuring security and privacy considerations are addressed for each change
- Following a documented information security and privacy monitoring and assessment plan

Retirement

Retirement is another of the commonly overlooked phases when it comes to information security and privacy due diligence. Don't slack off and just throw away security and privacy when a system, application, or storage devices is retired and no longer used! The typical objectives for this phase include:

- Backup and archive data to meet retention requirements
- Update the data, systems, applications, and hardware inventories
- Retire the system, application, and applicable computers and storage devices
- Dispose of data, code, and hardware

Key IT data protection activities include:

- Security and privacy information preservation to meet legal, business, and compliance requirements
- Thorough media sanitization, ensuring that data is irreversibly deleted, erased, and written over when retention periods end
- Secure hardware and software disposal

IT Data Protection Compliance Commonalities

Increasing numbers of laws, regulations, industry standards, contractual obligations, and organizational policies require information security and privacy practitioners to view their job responsibilities as including compliance enforcement activities. Growing fines, penalties, and other types of sanctions make it increasingly important to implement comprehensive enterprise-wide information security and privacy practices.

When IT uses a unified approach to information security and privacy compliance, organizations can more effectively manage the growing number of compliance requirements. A unified IT approach to information security and privacy compliance allows organizations to not only address identified risks but also comply with legal requirements.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.