


The Business Leader's Primer for Incorporating Privacy and Security into the SDLC Process

by *Rebecca Herold, CISSP, CISM, CISA, FLMI*

July 2006

It is important for business leaders throughout the enterprise to understand the system development life cycle (SDLC) and how decisions made can impact, negatively or positively, the entire business. First and foremost, systems and applications must be built to support the business in the most efficient and effective manner possible. Business leaders must be involved with the process to ensure systems and applications are being developed to meet this goal; the information technology (IT) areas cannot create applications and systems on their own and reach this goal. Second, applications and systems must be created to reduce risk to the level acceptable by the business as well as to meet compliance with applicable laws, regulations, and contractual requirements.

 Business leaders are key components of the SDLC and must understand the basic phases as well as the information security and privacy issues that must be addressed within each phase.

 The information for the rest of this paper is built around the SDLC topic discussion within a portion of the 2-day workshop "Effectively Partnering Information Security and Privacy For Business Success" by Christopher Grillo and Rebecca Herold

What Is the SDLC?

Smart organizations follow an SDLC to ensure applications and systems are created and updated in the most efficient and consistent manner possible to support the business need. Over the years, there have been a variety of SDLC methodologies created and used. They are typically very similar, as demonstrated in Table 1.

NIST 800-30	U.S. Department of Health and Human Services	ISO/IEC 12207
Initiation	System Concept Development Planning Requirements Design	Investment Analysis Acquisition Requirements Analysis Design & Engineering
Development or Acquisition	Development	Development
Implementation	Integration, Test & Implementation	Testing & Implementation
Operation or Maintenance	Operations and Maintenance	Operations and Maintenance
Disposal	Disposition	Retirement

Table 1: Comparison and mapping of SDLC phases.

Very generally, SDLC processes include the phases as labeled by NIST 800-30:

Initiation—The need for a new system, application, or process and its scope are documented. Security categorization standards are identified to help select the appropriate security controls. A preliminary risk assessment reveals the type of threat environment for the planned system.

Development—A large number of activities occur during this phase, most of which need to consider information security and privacy impacts. Such activities include a formal risk assessment, analysis of the necessary security requirements, determination of how much of the development cost should be allotted to information security and privacy, plan for security to ensure all security and privacy controls are fully documented, security controls development, security and privacy test and evaluation plans, and other related planning components. The system or process is designed and requirements are gathered and documented.

Implementation—This phase includes assurance-testing activities to validate and verify the information security and privacy specifications are within the deliverables and to ensure integration of security controls, security certification, and accreditation. The system is implemented in production.

Operation or Maintenance—This phase includes activities to ensure appropriate security and privacy configuration management and control as well as continuous monitoring to ensure the controls continue to be appropriate and effective.

Disposal—This phase is when the system is retired and no longer used. It is critical but often overlooked with regard to information security and privacy considerations. It includes activities for information preservation to meet data retention requirements, media sanitization as necessary, and appropriate hardware and software disposal.



Incorporating information security and privacy considerations and activities from the very start of the SDLC will not only result in more secure and compliant applications and systems but also help the business by being less expensive and more effective than trying to band-aid information security and privacy onto the final application or system.

Organizations must ensure that information security and privacy are constructed throughout the SDLC:

To ensure systems and applications support corporate policies and procedures

To protect data throughout the entire information life cycle

To meet data protection laws and regulations requiring information protection, such as access controls, access logging, availability, and so on

People in the SDLC


There are many key players who must participate in SDLC projects involving personally identifiable information (PII) and other sensitive information to ensure information security and privacy are appropriately addressed. The key players to involve within an SDLC include:

- Business unit leaders
- Project sponsors
- Marketing and sales
- Project managers
- Business analysts
- Business managers and users
- Technical IT administrators
- Information security
- Consultants and vendors
- Privacy
- Legal and compliance
- Auditors
- Human Resources

Organizations need to include other areas as appropriate to their own unique situations and environments. For example, healthcare providers will likely need to include physicians and nursing staff; manufacturing will likely need to include their standards and quality control staff; and so on.

Where Do Information Security and Privacy Fit In?

Information security and privacy must be addressed throughout the entire SDLC process. Historically, organizations tried to patch on security in the last week or two before systems or application deployment to production, or even following production deployment. This did not work, and it still will not work!

 Addressing information security and privacy for the first time during the production phase puts your business at significant risk of security incidents, privacy breaches, and noncompliance with laws and contractual requirements.

Organizations must follow a well-defined SDLC process to address information security and privacy every step of the way through the use of policies, procedures, standards, privacy impact assessments (PIAs), and information security risk assessments.

PIAs will determine:

- Where PII will be obtained, stored, transmitted, and retired

- Applicable data protection laws and regulations

- Who should have access to PII

- The PII data flow map

- Risks throughout the data flow

Information security risk assessments will identify:

- Technical, administrative, and physical risks within the planned system

- Cost-effective controls to reduce the identified risks to an acceptable level

Initiation Phase

The objectives and goals of the initiation phase are to:

- Describe the envisioned project

- Identify the project sponsor and budget

- Identify project resources

- Establish the preliminary project plan estimates

- Obtain management review and approval

- Engage the business requirements team

- Determine business requirements

During this phase, your information security and privacy goals are to:

- Integrate privacy and security into the project initiation phase to communicate any initial security and privacy requirements and risks upfront

- Determine privacy and security requirements

- Plan and perform preliminary privacy and security training

- Collect applicable infrastructure policies and standards that apply to the project

- Perform a preliminary information risk assessment and security categorization

- Conduct a PIA to identify PII, regulations, laws, contractual requirements, threats, and so on

It is important to identify applicable laws and regulations during this very first phase to ensure all issues and compliance requirements are then successfully addressed throughout the development of the application or system. The regulations that have information security and privacy requirements must be identified. Responsibility for ensuring requirements are met should be formally assigned to someone on the development team.



Examples of regulations that have information security and privacy requirements include, but are not limited to:

- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley Act
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)
- European Union Data Protection Directive
- State-level laws

It is also critical to ensure you have identified all the contractual requirements with business partners, vendors, and others related to systems and applications development. For example, many service and product agreements include clauses that have stipulations for notification for applications or systems changes, updates, or implementations.

During this phase, the policies, procedures, and standards associated with the project should be identified. This identification includes not only your internal information security policies but also all the information security and privacy policies your organization has on Web sites. You also need to check whether are obligated to follow any of your business partners' information security and/or privacy policies.

PIAs and Security Risk Assessments

PIAs should be performed during the initiation stage to determine:

Whether PII will be used within the system or application

Where PII will be obtained, stored, transmitted, accessed, and retired

Applicable data protection laws and regulations

Who will have access to PII

The planned PII data flow

Where are the risks throughout the flow

Information security risk assessments should be performed during the initiation stage to identify:

If risks involved could be mitigated to an acceptable level to pursue the project

Technical, administrative, and physical risks within the proposed system

Development Phase

The objectives and the goals of the development phase are to:

Finalize business requirements

Develop business use cases and finalize process flows



Use cases describe the functional view of what the system or application should do. They describe the sequence of actions the application or system performs with regard to interaction with the end users. In many SDLC use case procedures, the end users are referenced as “actors.”

Obtain business owner approval of the plans

Engage the development team in coding, documentation, testing, and other activities

Determine technical specification and design requirements

Develop code using secure coding techniques and standardized security and privacy coding procedures

Create and review the proposed development and testing strategy

Create and review the quality assurance (QA) testing plan

Develop and document the application or systems operating and training manuals and accompanying plans

Develop and document the deployment plan

During this phase, your information security and privacy goals are to:

Review the requirements specifications to verify privacy and security requirements are documented, understood, and responsibilities assigned

Approve the information security and privacy standards and design requirements

Create the documentation for the project—such as the security plan, privacy laws requirements, technical configuration standards, business continuity and disaster recovery plan, and so on

Use secure coding techniques, including adequate controls to the source code library, version control procedures, and so on

Ensure security coding and the development of test cases with appropriate security and privacy tests

Conduct and document privacy and security tests

Ensure security and privacy functionality and protection

Perform system security and privacy tests and vulnerability and penetration tests


Address regulatory compliance and customer access issues

Plan for system security and/or privacy certification and accreditation as appropriate

PIAs and Security Risk Assessments

PIAs should be performed during the development phase to:

- Ensure use cases address all OECD principles, applicable laws and regulations, contractual requirements, and international data flow issues
- Identify privacy changes from the initiation phase
- Identify and document privacy risks, controls, planning, and responsibilities
- Ensure there are no gaps with contractual, legal, or regulatory requirements
- Ensure PII database checks are made as appropriate within the system or application
- Determine whether programming tools such as P3P should be used

 The definition of P3P is provided by the World Wide Web Consortium Web site (<http://www.w3.org/>): *The Platform for Privacy Preferences Project (P3P) enables Websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents will allow users to be informed of site practices (in both machine- and human-readable formats) and to automate decision-making based on these practices when appropriate. Thus users need not read the privacy policies at every site they visit.*

Information security risk assessments should be performed during the development stage to ensure:

- Use cases address technical, physical, and administrative security
- Appropriate access controls are created
- Security policies, procedures, and standards are followed
- Security procedures are created as necessary for the application or system
- Security specifications are followed
- Appropriate technologies are used, such as encryption, digital signatures, and so on
- A documented system security code review occurs


Version Control

Most systems and applications consist of literally millions of lines of code and potentially thousands of programs, modules, screens, and forms. Version control is vital to the successful and productive use. Examples of version control considerations include:


- Is a version control system in place?
- What is the backup strategy?
- Does the source code contain sensitive or confidential business rules?
- Is the version control process secure?

Privacy and Security Testing Plan

A thoughtful, well-documented testing plan must be used during systems and applications development not only to ensure all information security and privacy issues have been thoroughly tested and resolved but also to provide demonstrated due diligence that security and privacy were appropriately addressed during development.

 Organizations that do not carefully document and execute security and privacy plans for new and updated systems and applications might find themselves in legal jeopardy if a security breach subsequently occurs using the system or application.

Government oversight agencies have specifically indicated within their judgments and consent decrees that lack of or insufficient design and implementation of reasonable safeguards to control risks—and then lack of or insufficient regular testing of those controls—was of significance in determining the fines, penalties, or otherwise resulting actions the organization had to take.

 For example, the FTC consent decree against CardSystems Solutions, Inc. required many activities including the design, documentation, and implementation of reasonable safeguards to control the risks identified through risk assessment as well as regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.

Many types of tests need to be performed during the development phase. Two types of significance are functional tests and code tests.

Functional Tests

Functional testing can be used to confirm the correct behavior of the system's or application's security controls. Examples of functional security and privacy tests include:

- Ensuring only specific user groups can access certain databases or data fields

- Ensuring data is successfully encrypted within specified situations

Code Tests

Code testing reviews the control structure, the data flow structure, decision control, and modularity of the program code to ensure the application is constructed appropriately, comprehensively, and completely. Code testing can be manual through visual inspection or automated. Examples of security and privacy code tests include:


- Reviewing access control code and modules

- Testing and validating the successful execution of encryption code

- Ensuring backdoors are not built into the code that allow access that would create risks or be in noncompliance with applicable laws and contractual requirements

Use of PII During Testing

Real PII should not be used for test or development purposes if at all possible. Not only is it a good idea and leading system development practice, it is against the law in some countries.

 A 2006 Compuware survey of U.K. IT directors found that 44 percent of companies use live data for testing even though the 1998 U.K. Data Protection Act states organizations should not use actual sensitive personal data for such purposes.

There are effective tools available to create dummy data for testing. If, for some reason, PII must be used for test data, you need to know what your privacy policy is regarding the use of PII and if such testing would be in noncompliance with your policy. You must also determine how the PII will be protected during all phases of the testing process.

Implementation Phase

The objectives and the goals of the implementation phase are to:

- Successfully deploy the system or application

- Provide end user training

- Transition to operational support

During this phase, your information security and privacy goals are to:

- Re-certify and re-accredit the system or application

- Perform a vulnerability assessment

- Implement the information security and privacy assessment and monitoring plan

- Implement compliance monitoring

Post-Implementation Review

Soon following the move to production, perform a post-implementation review to document lessons learned from the team while they are still fresh in everyone's minds and to ensure the documentation actually is accomplished. Oftentimes, team members are already starting on other projects and this valuable documentation is never created.

Another objective of performing a post-implementation review is to obtain end-user feedback regarding how the new or updated system or application is working in the production environment and then tweak the system as necessary to get rid of any identified bugs or issues. The information security and privacy goals for performing a post-implementation review are to analyze the information security and privacy lessons learned throughout the project and improve the security and privacy SDLC processes accordingly.

PIAs and Security Risk Assessments

PIAs should be performed during the implementation phase to:

- Ensure there is still compliance with all privacy laws and contractual commitments

- Ensure support personnel successfully follow privacy-related activities, such as appropriately responding to customer requests for access to their PII

- Ensure links with other production systems and applications have not created inappropriate access capabilities to PII

Information security risk assessments should be performed during the implementation phase to:

- Verify that the security monitoring plan is adequate and effective

- Ensure that integration with other production systems has not introduced new risks or vulnerabilities

- Verify that backup and recovery plans will work

Maintenance Phase

The primary objectives and goals of the maintenance phase are to ensure the transition from development personnel to operations personnel is successfully completed, and that ongoing support of the system or application is achieved. During this phase, your information security and privacy goals are to:

- Follow proper configuration management procedures to ensure all security settings are where they should be

- Ensure adequate consideration of the potential security and privacy impacts due to specific changes to an information system or applications within the surrounding environment

- Follow secure change-control procedures

- Ensure security and privacy considerations are addressed for each change to the application or system

- Continuously follow the information security and privacy monitoring and assessment plan, being particularly vigilant during personnel changes for this responsibility

Disposal Phase

The primary objectives and goals of the disposition phase are to ensure the successful sunset, or retirement, of the application or system with as little impact to the business as possible. During this phase, your information security and privacy goals are to:

- Preserve information as necessary for applicable data retention legal and business requirements

- Ensure that data is irreversibly deleted, erased, and written over on all storage media when retention periods end

- Ensure secure and appropriate hardware and software disposal

Closing Thoughts

The objective of incorporating information security and privacy is not to totally overhaul an existing SDLC project management process but to add well-defined security and privacy checkpoints and security and privacy deliverables. The ultimate goal is to make the applications and systems as secure as reasonable based upon risk and to ensure compliance with applicable data protection laws.

Some lessons learned about incorporating information security and privacy into the SDLC (Source: “Effectively Partnering Information Security and Privacy for Business Success” two-day workshop by Christopher Grillo and Rebecca Herold):

- If you wait until an application or system is already in production to make it secure and address privacy, you’re too late to ensure effective security and privacy. Such a band-aid approach is dangerous to your business.

- Effective security and privacy practices need to be incorporated into all the applications and systems layers involved, such as the network, host, application, storage, end-points, and so on.

- Ensure clearly written and easily accessible information security and privacy policies, standards, and guidelines are used as frameworks for the security and privacy being constructed within the application or system.

- Implement, or follow the existing, policy deviation-exception process.

- Create checklists that include step-by-step instructions within every SDLC phase for information security and privacy.

- Personnel education is crucial to the success of incorporating security and privacy into the application or system; make sure it occurs, not just once but on an ongoing basis during the life of the application or system.

- Information security and privacy are ongoing and always changing processes; make someone responsible for addressing these issues during the lifetime of the application or system.