Best Practices for Ensuring Data Privacy in Nonproduction Systems with Data Masking
## Table of Contents

Executive Summary ................................................. 2

Data Privacy Best Practices Are Sound Business Practice ............... 3

Protection of Sensitive Information .................................. 4

- Best Practices for Data Classification ................................ 5
- Structured and Unstructured Data .................................. 5
- Data Leakage ..................................................... 6
- Best Practices for Data Leakage Prevention ......................... 6
- Sensitive Data and Data Masking .................................. 6
- Best Practices for Data Masking .................................. 7

Special Regulatory and Industry Requirements .......................... 7

- Best Practices for Regulatory and Industry Requirements ......... 7
- Regulatory Requirements ......................................... 8
- Best Practices for HIPAA ........................................ 9

Risk Assessment ...................................................... 10

- Ongoing Compliance Assessment ................................ 11

Securing Applications and Data in Development ....................... 11

- Software Development Life Cycle ................................ 12
- Best Practices for SDLC Application Design ....................... 12
- Best Practices for Programming .................................. 13
- Best Practices for Sensitive Data in Development .................. 14
- Documentation ................................................... 14
- Best Practices for Documentation ................................ 14
- System Administrators and Developers ............................. 15
- Best Practices for Developers and Administrators ................. 15
Executive Summary

There is a growing need to protect sensitive employee, customer, and business data across the enterprise wherever such data may reside. Until recently, most data theft occurred from malicious individuals hacking into production databases that were made available across the Internet. With a number of well-publicized and costly thefts creating both tremendous legal liability and bad publicity for the affected organizations, business has quickly grown more and more sophisticated in protecting against such schemes.

While the industry deals with the most egregious aspects of data theft, many computer systems still remain vulnerable to attack at some level. An important tier of computer data remains practically untouched and unprotected by today’s new data security procedures: nonproduction systems used for in-house development, testing, and training purposes are generally open systems and leave a large hole in the data privacy practices at companies of all sizes. These environments leverage real data to test applications, housing some of the most confidential or sensitive information in an organization, such as Social Security numbers, bank records, and financial documents.

This white paper discusses best practices for creating data privacy procedures in nonproduction environments. These procedures include creating a comprehensive set of policies to classify datatypes that need to be protected, integrating these policies into day-to-day business processes, providing ongoing compliance reviews, using a proven commercial solution for masking sensitive data in all nonproduction environments, and integrating these privacy processes and technology across the enterprise.
Data Privacy Best Practices Are Sound Business Practice

Confidentiality, integrity, and availability are the cornerstones of information privacy, as well as a sound business practice. They are essential to the following:

• Compliance with existing regulations and industry standards
• Reliable, accurate, high-performance services
• Competitive positioning
• Reputation of the firm
• Customer trust

“Best practice” is a term we need to be careful with. The truth is that what is “best” varies widely from one situation to another, even for a specific kind of control such as passwords. That’s why regulations afford the latitude they do for control definition by each company. “Best” is not used here in a literal way. Rather, it is used to wrap together such notions as “good,” “commonly used,” “prudent,” “industry standard,” or “generally accepted.” Although there is no official framework for best practices that you can simply adopt, a variety of information protection controls have come to be widely accepted as sensible, baseline, and sound practice. In the end, the true authority for what is right for your company is your company management, your regulatory examiners, and industry validators.
Protection of Sensitive Information

Every company has sensitive data, whether it is trade secrets, intellectual property, critical business information, business partners’ information, or its customers’ information. All of this data must be protected based on company policy, regulatory requirements, and industry standards. This section will cover a number of important elements of protecting this data.

Data classification policy organizations that collect, use, and store sensitive information should establish an information classification policy and standard. This classification policy and standard should contain a small number of classification levels that will meet the business needs of the firm. Most organizations have at least three categories such as public, internal use only, and confidential.

Many companies have long-established data classification guidelines. However, with all of the new regulations and industry standards, they have discovered that the mere presence of a corporate policy is no longer sufficient. Some of these organizations have spent the last couple of years “operationalizing” their data protection policy into the information technology (IT) infrastructure. Digital data classification is an emerging technology that is not yet standardized. In the interim, organizations have been deploying various controls and tools to minimize the risk of noncompliance. Data leakage detection, prevention, and protection technologies have emerged during the past two years and are now being implemented within the infrastructure (see the Data Leakage section below).

Business requirements should drive the number and definition of each category of data as well as the requirements for labeling, storage, distribution, disclosure, retention periods, and destruction. Regulatory and industry rules and standards will clearly play a significant role in this process. Other knowledge, information, and data will require protection, including trade secrets, research, formulas, prepatent discovery, and various forms of customer and employee information.

Another important aspect in the protection of knowledge, information, and data is how they are used within the operations of the firm and in what form the data resides (hard copy, electronic, or human). In addition, protection requirements will also vary by type of operational environment, such as production, preproduction test, development, quality assurance (QA), or third party. In this document, we will focus on best practices for protecting the data used for internal or external development and QA environments.

The requirements for protecting this knowledge, information, and data must be clearly defined and reflect the specific requirements within the appropriate regulatory and industry rules and standards. Specific data elements must be labeled as sensitive and should never be used within their factual state in development, QA, or other nonproduction environments. The data classification policy should clearly identify the requirements for data masking. Note that knowledge and information can be broken down into specific data elements.

Finally, the organization must implement a compliance process that will provide periodic independent review of the development and QA environments to ensure that best practices are followed.

1 Frameworks such as ISO27001, COSO, CoBiT, and ITIL do not provide specific information protection controls or the effectiveness of controls; they provide a broad range of control objects.
Best Practices for Data Classification

Companies must create a comprehensive set of policies and procedures for the classification of all data to adequately protect their information and defend their intellectual property. In addition, companies should implement these three steps:

- Provide awareness training for employees, contractors, and third-party service providers periodically
- Integrate procedures into the day-to-day business processes and automate as much of the policy as feasible
- Obtain ongoing independent compliance review and report the results to senior and executive management

Structured and Unstructured Data

Sensitive data occurs in two forms: structured and unstructured. Structured sensitive data is easier to find because it typically resides within business applications, databases, enterprise resource planning (ERP) systems, storage devices, third-party service providers, back-up media, and off-site storage. Unstructured sensitive data is much more difficult to find because it is usually dispersed throughout the firm’s infrastructure (desktops), employees’ portable devices (laptops and handhelds), and external business partners. That dissemination is not the problem; what increases the level of difficulty substantially is that this sensitive data is typically contained within the messaging infrastructure (email, instant messaging, voice-over-IP), personal production tools (Excel spreadsheets), unmanaged portable devices, and portable media. So if these various unstructured environments are “unmanaged,” then the sensitive data can propagate in an uncontrolled manner. For example, if users are permitted to archive local data and/or move it to a personal (home computer) or portable storage device (USB memory stick), it becomes uncontrolled and at risk.

Organizations must define, implement, and enforce their data classification policy and provide procedures and standards to protect both structured and unstructured sensitive data. For example, they can use end-point security tools to control the use of portable devices and media, content analysis tools to detect the presence of sensitive data, and encryption tools to protect unauthorized access to these devices.
Data Leakage

So what is data leakage? Simply put, data leakage is when sensitive data leaves the protection of the custodian who has been authorized by the owner to have access to this data. The owners’ authorization requires that the custodian (your company) take reasonable measures to protect the confidentiality and integrity of the sensitive data, and that it foresees and prevents intentional or unintentional misuse, breach, or theft of the sensitive data.

Available technologies vary from simple blocking devices, paths, ports, other forms of egress and access, mass encryption of devices, media, and connections to more complex or selective blocking. Technology now exists to monitor content in real time to identify selected information, conditions, people, entitlements, and actions to block, quarantine, encrypt, log, alert, or sanitize data. There are currently two methodologies: scanning information at rest and analyzing information in motion. These technologies can be deployed in many parts of the infrastructure, but are more commonly found at end-point devices and external gateways. End-point devices typically contain removable digital storage devices, hard-copy devices, and various forms of network connectivity that provide access to many internal network resources and in some cases could by-pass internal managed network gateways to get outside the organization. These often become conduits for data leakage.

Some of the major drivers to prevent data leakage come from regulations primarily focused on privacy and confidentiality of information (data)—for example, the Gramm-Leach-Billey Act, Health Insurance Portability and Accountability Act (HIPAA), State Breech Laws (37); industry requirements—for example, Payment Card Industry; national security—for example, NERC Cyber Security Standard (CIP), DHS, NIST; and corporate policy.

Best Practices for Data Leakage Prevention

Deploy and integrate technology and processes throughout the infrastructure to detect and/or protect sensitive data from leaking out of your enterprise. These steps will require physical and logical controls and technology, changes in routine business and operational processes, and ongoing monitoring and assessment of personnel who have access to sensitive information.

Sensitive Data and Data Masking

It is important to have a common definition of “real data” and what we will refer to as “nonfactual but real data” or “masked data.”

So for example in SAP ERP, data elements within a domain, a built-in data type, or an object field within data objects is real data and must comply with the data definition of the data element. However, this information can be factual—an actual Social Security number—or it can be nonfactual—a random collection of numbers conforming to the data definition for that particular data element.

As we know, data elements, such as “customer” or “order,” are often related to each other through the use of a keyfield. When there is an association with many data elements, protecting individual data elements becomes complex. Some data elements alone may not contain sensitive data; however, once an association with other data elements occurs, they all become sensitive data. So data masking must quickly become very sophisticated to ensure that all the sensitive data is protected (masked), the data is still “real,” and a record of the association is retained.

Not long ago, organizations developed their own data masking tools, which were effective to varying degrees. Today, with all of the regulations and risk of fines, the negative impact on reputation, and the possibility of criminal convictions, organizations have moved toward third-party masking technology that is regularly updated according to evolving standards and regulations. This technology is used to mask sensitive data in the general open development and QA environments.
Best Practices for Data Masking

Use a proven commercial solution for data masking of sensitive data in all development and QA environments internal or external. Never provide third parties with sensitive data that is not masked.

Special Regulatory and Industry Requirements

Depending on the countries that your organization does business in, there will be some unique requirements for the protection of sensitive data. Nearly every country in the world has a data privacy law, so you should always do a comprehensive review of each of the pertinent laws and their supporting requirements. You will find that there is substantial commonality among these regulations—at least in their spirit or intent. This white paper will focus on some of the more common regulations in North America.

Best Practices for Regulatory and Industry Requirements

Although there are unique aspects to each regulatory item, complying with one may help you comply with (or minimize your exposure) to another. In general, information security techniques are broadly applicable across these regulations and also across a wide variety of industries. What one industry devises has a good chance of being useful to others.

Many financial services firms have been taking information security seriously for a long time. The majority of controls called for by the new regulations have simply been considered sound business practices for earning customer trust. The latest regulations only add a few “new” concepts, so many firms will find themselves well down the road toward compliance. Testing and monitoring of controls should be done by parties not directly involved in the design or operation of those controls, so you should expect to see security specialists and/or IT auditors more often. This had led to a substantial increase of a new business function called IT risk management or IT governance as a new best practice. The financial services industry has taken the lead, but we have seen other industries adopt this new function as well.

Many of the regulations and industry standards have special requirements for third-party service providers. These third-party service providers include IT outsource and/or in-source vendors as well as providers that fulfill elements of certain business processes—for example, a third party that provides contract programming services and needs full access to a test system, a business that does promotional mailings for the company and must receive names and addresses, or a third party that processes bills and transactions.

Your company (the primary contracting institution) is not relieved of its responsibility to protect sensitive information just because the covered information moves into someone else’s hands.

The regulations and industry standards either imply or specify that you must adapt to change and could result in a situation of “You snooze ... you lose.” You really have to keep up with changes in the business risk profile, outdated processes, your human resources (employees), all forms of threats, the technologies, software bugs, the never-ending flow of patches, and so on.
Regulatory Requirements

The following are three examples of government regulation and industry standards that govern how confidential data should be handled.

Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act (GLBA) applies to financial institutions that offer financial products or services such as loans, financial or investment advice, or insurance to individuals. Compliance is mandatory for all nonbank mortgage lenders, loan brokers, financial or investment advisers, tax preparers, debt collectors, and providers of real estate settlements. The law requires that financial institutions protect information that is collected about individuals; it does not apply to information that is collected in business or commercial activities.

Best Practices for GLBA

There are three basic rules to understand to ensure compliance with GLBA:

1. Ensure the security and confidentiality of customer records and information
2. Protect against any anticipated threats or hazards to the security or integrity of such records
3. Protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer

So let's look into these three simple rules further. First, what does “ensure the security and confidentiality of customer records and information” mean?

In general terms, you should take all reasonable measures to guarantee that the privacy of nonpublic personal information in all forms (electronic, hard copy, verbal) is protected from unauthorized access and disclosure.

Second, what does “protect against any anticipated threats or hazards to the security or integrity of such records” mean? Let us dissect this and put the definition into layperson terms:

- “Protect against anticipated threats or hazards”—this requires the application of a risk assessment process to foresee the possible known or unknown threats and vulnerabilities in any form (physical, logical, human, or act of God) that may compromise the security and integrity of nonpublic personal information.

- “to the security or integrity of such records”—in this case, security can be defined as anything that would compromise the confidentiality of nonpublic personal information; integrity can be defined as anything that could compromise the trustworthiness, reliability, accuracy, or soundness of nonpublic personal information.

Finally, what does “protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer” mean?

The term “unauthorized access” is very familiar to us, but who authorizes access? We as consumers and customers play a role in defining who has access to our “nonpublic personal information” and under what conditions they can use this information. We sign and click on agreements every day that define the terms and conditions of granting access to and use of our nonpublic personal information. However, the service providers we grant these privileges to are required to follow security practices to ensure that “need-to-know” concepts are followed and all unauthorized parties are denied access to our nonpublic personal information.

Some other very important best practices are to keep up to date with agency guidance on GLBA; it’s just like keeping up with operating system patches, but with less frequency. You must protect PFI in all environments and including development, QA, and test environments; the regulations do not differentiate among these environments. Remember: masking is the safest way to protect sensitive information in development and QA environments.
Health Insurance Portability and Accountability Act (HIPAA)

The HIPAA Security and Privacy Standard defines administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (PHI), sometimes referred to as personal health information. HIPAA has three major purposes:

- To protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information
- To improve the quality of health care in the United States by restoring trust in the health care system among consumers, health care professionals, and the multitude of organizations and individuals that are committed to the delivery of care
- To increase the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals

Best Practices for HIPAA

Understanding the HIPAA Security and Privacy Standard requirements is the key to interpreting what the covered entities must do:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information that the covered entity creates, receives, maintains, or transmits
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part
4. Ensure compliance with this subpart by its workforce

One of the most important aspects of this process is to use a risk management approach. If your organization deals with health, financial, or other personal information, then your risk model should be risk adverse and therefore, your interpretation of these requirements should lean toward a higher bar for your controls.

Privacy is a subset of confidentiality and, in the spirit of these regulations and industry standards, must be protected from unauthorized access by using the latest industry security technology products and solutions.

Some best-practice technologies are content extrusion at the host and network gateways, encryption or masking of data at rest in all environments internal and external, network segmentation of sensitive data storage, and logging all access attempts to sensitive data (successful and unsuccessful) at infrastructure and application levels. Data at rest must be encrypted and hashed or masked in all environments. Use of tamper-proof technologies in data storage environments is one of the new methods of best practice.

Encryption of portable devices is now an industry standard best practice, and failure to encrypt portable devices containing sensitive data can be seen as being negligent by the regulatory agencies, the courts, and the general public.

Finally, while real and frequent testing of your security infrastructure and IT control environment is not a common best practice, the lack of frequent testing of these protection mechanisms (compliance) can be looked at as negligence. Disaster recovery and business continuity plans should be tested (really tested = you actually switch over to the respective sites) at least annually. Some organizations test their disaster recovery plan every quarter.
Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS originally began as five different programs: VISA Card Information Security Program, MasterCard Site Data Protection, American Express Data Security Operating Policy, Discover Information and Compliance, and JCB Data Security Program. Each company’s intentions were roughly similar: to create an additional level of protection for customers by ensuring that merchants meet minimum levels of security when they store, process, and transmit cardholder data. In December 2004, these five companies aligned their individual policies and created the Payment Card Industry Data Security Standard.

The first PCI DSS was introduced in January 2005. The standard is intended to allow merchants, card issuers, card processing companies, and other third-party service providers to demonstrate compliance with a common agreement for information security due care, rather than requiring them to comply with differing requirements from each payment processing company.

All of the five founding members have agreed to incorporate the PCI DSS as the technical requirements of each of their data security compliance programs. Each founding member also recognizes the Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs) certified by the PCI Security Standards Council as being qualified to validate compliance to the PCI DSS. The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection.

The PCI DSS is considered one of the more comprehensive data security standards in a cluster of regulations that have emerged over the past decade, and it is regarded as being relatively more prescriptive than other laws and regulations. PCI covers six overall areas and 12 requirements, each supported by lower-level requirements.

Risk Assessment

Any risk is assumable so long as the risk assumption decision is made by the right person(s) and so long as they are adequately informed.

Risks pose potential consequences that can increase the cost of doing business. The same is true for controls, which can add obvious costs (such as new processes, IT equipment, or software licenses) and can also introduce qualitative costs (such as inconvenience to customers or employees or processing overhead). A control is only cost-justified if the cost of control is less than the avoided costs of compromise.

No control is perfect, no matter how much you spend; it’s just another balancing act. Strong controls are usually more costly and almost always much more intrusive into processes and people’s experiences. Least privilege and need to know are very well-accepted best practice that is not always easy to implement. If you limit a person’s privileges to the minimum he or she needs to do his or her job, you will have done what you can to minimize the risks associated with that person working in your environment. Some companies believe that every employee should be empowered to serve the customer in any way. This business choice makes limitation of privileges somewhat moot. People make or break security; no amount of technology can make up for poor practices and behaviors.

Every technical control ultimately relies on some form of fallible human process: to build it, configure it, administer it, and use it.
Ongoing Compliance Assessment

Compliance assessment is not a one-time task. It requires a repetitive process to be reasonably effective. Ideally, compliance is fully integrated into daily operations. Our definition of best-practice compliance assessment is fairly broad. It starts with understanding the controls:

1. First, you need a clear understanding of the purpose of the control (what risk or risks it is mitigating), the specific attributes of the control (settings, parameters), the significance of the control (from a risk perspective), whether there are secondary controls (back-up control that will perform the same level of risk mitigation), and the type of control (technology, process, people). Of course this must all be documented.

2. There must be specific documented test criteria to ensure that the control, as defined in the first step, has been implemented correctly. The control must, most importantly, be tested to determine its effectiveness in mitigating the risk as defined in step 1.

3. The test results must be recorded (a permanent record of the test results must be retained based on your regulatory requirements). There should be an accountability process for this step. In some cases, the recording may be technological. If you are using a software tool to test your controls, then the recording should be protected to ensure the integrity of the results.

4. The test results must then be collected into a central repository for correlation and reporting.

5. Periodic reporting of the state of controls should be focused at three primary levels.

Securing Applications and Data in Development

The information processed by and/or housed in applications and databases must be protected. Therefore, applications and databases must be secured. Infrastructure security is necessary for application and database security, but in itself is not sufficient. Applications and databases have to contribute to the overall security model. Some security elements can only be performed within the application or database code. Operation of the applications and databases is also critical to the security model. If we are going to protect certain information, then application-level security controls related to operation of the application are essential.

Some might think that it is enough to strongly secure the infrastructure that hosts the application, but this is simply not true. The applications are at the top of the IT food chain—they are the heart of the business lifeline, they are the channels to the consumers, business clients, and business partners—so the controls start here. For example, the application is the logical place to handle user entitlements to the application and to the data managed by the application, to incorporate segregation of duty controls, to audit critical activities and transactions, and to protect sensitive information.
Software Development Life Cycle

Best practices assume that you have adopted a software development life-cycle (SDLC) methodology that you use when you develop and purchase application software and that it has clear steps and guidelines for defining controls and security requirements early in the process. Having security controls established from the start is important for several reasons, but one good one is that security controls often have an architectural impact on an application or database.

Access controls are a good example of getting something designed in early. If the appropriate combinations of application functions (from a risk and security perspective) are not defined in the requirements or logical design phase, then it is likely that the resulting application will not be able to separate risky functions via user entitlements profiles. The same idea can easily apply to data. If the need to separate access to certain data elements or aggregates is not anticipated in the design, then it will be costly or perhaps impossible to process and present data in appropriate ways. The underlying file structure may simply be inadequate.

Questions about how users will be identified and authenticated need to be carefully discussed early in the development life cycle. If each application addresses these issues in its own way, the aggregate corporate result is a tangled mess. If standard, shared services can be adopted, the resulting simplicity can be elegant and cost-effective.

If the application is not specifically designed to run on a securely configured platform, then conflicts with secure O/S configuration are likely. Think how often we can’t install patches because of conflicts with production applications.

Best Practices for SDLC Application Design

A best-practice software development life-cycle methodology must consider this list of controls at a minimum for the design phase:

- Access controls (entitlements)
- Record counts
- Control totals
- Balancing controls
- Reconciliation reports
- Field-level edits
- Limits on user authority (trans. type, value)
- Audit trails and journals
- Change history
- Report integrity controls
- File integrity controls
- Process execution controls
- Authentication levels commensurate with the sensitivity of the information
- Ability to measure the controls and their effectiveness

What good are security and control features in the application if tools are not available to manage and administer these features properly? Access reports, audit trails, and the like are just as important as any business functionality in the eyes of examiners and the auditors if nobody else.
Best Practices for Software Development

Control and security requirements must be defined early and included from the start. Security controls are often architectural and retrofit is costly. Some selected best practices:

- Life-cycle process requires definition of security controls
- Business owners must participate and own security controls
- Security control standards simplify control development
- Shared security services simplify development, increase security effectiveness, and reduce cost
- Life cycle covers concept to retirement

Malicious code, bugs, or poor programming practices can introduce significant risks to your company in various forms. Select best practices whether you build or buy:

- Adopt and enforce good programming standards
- Adopt and apply a code review using tools and/or independent experts
- Test rigorously and independently with tools and/or independent experts
- Ensure accountability for developers’ work - part of performance criteria
- Build it right once and reuse modular code

Best Practices for Programming

Here is a top-ten list of good programming practices:

- No buffer overflow conditions and no malicious code often written into applications to assist developers with test and debug but never removed
- Applications are captive with no keystroke sequences that abort execution and leave the user with an operating system shell, usually in a privileged account
- Protocols are faithfully followed
- Good memory management, including clearing cache and memory buffers of sensitive data ASAP
- No sensitive data is stored permanently on risky servers unless it is masked
- No dormant code
- No undocumented features
- Proper use of http, html, and cookies, and avoidance of risky Web application coding techniques, such as poorly written Perl scripts
- One process knows how to trust a call from another
- Input strings from untrusted devices are rigorously checked before processing

Developer accountability is nicely supported by some of today’s disciplined source code management (library) systems. We suggest using modular, reusable code especially for functions that must be supported with very high reliability.
Best Practices for Sensitive Data in Development

Developing and testing applications demands access to data—lots of it and as “real” as possible. Copies of real databases usually contain sensitive or confidential data that must be protected. Here are some selected best practices:

• Minimize points where real data is required
• Mask real data to remove personal identification
• Apply very strict controls—similar to production controls—when real data must be used (this applies to physical, logical, and people controls)
• Never send sensitive “personal identifiable” data offshore without masking the sensitive data. U.S. regulations are typically unenforceable outside the United States

Except under rare circumstances, developers and administrators have no defensible reason to view sensitive or confidential personal information. This applies to structured data and unstructured data. If they do, then it is probably a clear violation of regulations, maybe even the firm’s privacy policy. Corporate policy should state that even if they can, they must not. Severe penalties should accompany violations of this principle. “Poking around” in the data must be stricken from the IT culture.

Documentation

Let’s be honest, documentation is not free. It takes legwork upfront and maintenance: time, effort, and an investment.

However, it is undoubtedly a regulatory requirement. The Auditing Standards Board (on which the Public Company Accounting Oversight Board (PCAOB) and SEC are likely to rely) has said that the “lack of documentation” is a clear regulatory deficiency in the context of the Sarbanes-Oxley Act. Whether the controls are effective or not, documentation is required. If not documented, then how can management assert that they know the state of control versus the intended state?

Best Practices for Documentation

Good documentation is a valuable business/technical resource and best practice. Here are some examples of what to document:

• Document procedures and processes, both business and IT
• Keep records of controls and the decision processes behind them
• Furnish support for IT and security architectures and strategies
• Document monitoring and oversight activities and control status
System Administrators and Developers

System administrators who can also administer security components (e.g., add, change, and delete users and give them rights/privileges) can do anything on that platform and/or the applications it supports. If they can also alter the logs, then they can be totally stealthy.

Developers who also test their own code may be tempted to overlook certain faults or avoid certain tests that might make their work look bad or cause them to miss deadlines. Or they could abuse this combined role to move malicious code through the test phase and possibly into production.

Some development organizations like to test in the production environments. Such testing has a high risk of breaking things or launching bogus transactions (there are actual cases of this practice). Testing in production would be a good way to introduce malicious code. The same principle applies for testing against live networks (intranet or Internet). Best practice: run the final test of your applications in a segregated preproduction environment that is a replica of your production environment (network, computing, database, and application) infrastructure, and also ensure that your sensitive data is masked.

Developers who are also operators (have access to production) have the power to unilaterally cause harm perhaps without an audit trail and can make mistakes with extremely serious consequences. There are rare situations when developers really do have to patch production code. Best practice: a fire call ("break glass") is the accepted way to manage this. The problem/change ticket must be completed ASAP following fire call access. Fire call passwords are changed after use.

Developers who are also administrators may not only be able to create malicious code but could also use their admin rights to alter logs that might hold clues to the attack. The broader the powers and rights you have, the more likely that an error or mistake will have serious consequences. Small organizations may be forced to combine roles due to the limited number of qualified staff. This is a great example of why “best practice” is hard to define.

Best Practices for Developers and Administrators

Developers and administrators must often have root access to many systems (trusted by other systems) just to do their job. They possess the technical skill to use and abuse privileges. Some selected best practices:

- Isolate development environments and monitor them closely
- Limit (tightly control) test Internet connections
- Configure development platforms securely
- Motivate developers to use good security practices
- Find alternatives to shared accounts for administrators and support functions
ABOUT INFORMATICA

Informatica enables organizations to operate more efficiently in today’s global information economy by empowering them to access, integrate, and trust all their information assets. As the independent data integration leader, Informatica has a proven track record of success helping the world’s leading companies leverage all their information assets to grow revenues, improve profitability, and increase customer loyalty.