

On: 11 May 2008
Access Details: Free Access
Publisher: Taylor & Francis
Informa Ltd Registered in England and Wales Registered Number: 1072954
Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



EDPACS

The EDP Audit, Control, and Security Newsletter

Publication details, including instructions for authors and subscription information:
<http://www.informaworld.com/smpp/title~content=t768221793>

Database Access, Security, and Auditing for PCI Compliance

Charles Le Grand; Dan Sarel

Online Publication Date: 01 April 2008

To cite this Article: Le Grand, Charles and Sarel, Dan (2008) 'Database Access, Security, and Auditing for PCI Compliance', EDPACS, 37:4, 6 — 32

To link to this article: DOI: 10.1080/07366980802063582
URL: <http://dx.doi.org/10.1080/07366980802063582>

PLEASE SCROLL DOWN FOR ARTICLE

Full terms and conditions of use: <http://www.informaworld.com/terms-and-conditions-of-access.pdf>

This article maybe used for research, teaching and private study purposes. Any substantial or systematic reproduction, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The accuracy of any instructions, formulae and drug doses should be independently verified with primary sources. The publisher shall not be liable for any loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.

DATABASE ACCESS, SECURITY, AND AUDITING FOR PCI COMPLIANCE

CHARLES LE GRAND AND DAN SAREL

A CALL TO ACTION FOR DATABASE CONTROL AND AUDIT

Now eight years into the aught decade, we ought to be proficient with the controls, monitoring, risk management, and governance needed to prevent and detect the debacles that ushered in the Sarbanes Oxley act of 2002. And we should have a pretty good idea how to protect against Internet attacks and identity theft. But while you are considering that, remember the “Billion Dollar Bubble” or Equity Funding scandal (the first major so-called computer fraud) was started in 1964 and brought the company down in 1973. And the first major electronic privacy legislation was the Privacy Act of 1974 following revelations of privacy abuse during the Nixon administration.

We are in a seemingly endless race to protect our information, systems, and communications before the bad guys can bring us down—and preferably before onerous legislation forces us into rigid requirements about how to solve problems. We have built some spectacular information infrastructures, and left enough holes in them to present an inviting target to those who would hijack systems and data for fun or profit. Now, while the technology capabilities continue to expand, we are trying to plug the holes in our existing systems while hoping the new systems we implement will not create the next wave of vulnerabilities and attacks.

Audit must address a lot more than SOX and PCI

Database management affects a lot more than SOX and PCI compliance. Depending on whether your industry or company must comply with FFIEC, GLBA, HIPPA, ISO, CA SB 1386, or other requirements, the auditor may choose to perform a limited scope compliance audit for a specific set of requirements. The audit scope may be coordinated with risk and compliance management and may focus on known areas of greatest risk.

IN THIS ISSUE

- Database Access, Security, and Auditing for PCI Compliance

The auditor must develop or modify the scope of plans, internal control questionnaires, testing, and reporting based on the requirements to be addressed in a given audit. This article addresses only a relatively narrow example of such audits.

Control requirements vary depending on the industry and type of business, but some of the most prevalent compliance requirements today are the Sarbanes Oxley act (SOX) and the Payment Card Industry's Data Security Standard (PCI DSS). In the past 5 or 6 years we have seen heavy emphasis on financial reporting "controls" and improving the quality and reliability of financial reporting. And it looks like the next 5 or 6 years will continue to add emphasis on "protecting" our data (and not just financial data). So while we are assessing and improving financial application controls, we will see increasing emphasis on access controls, general IT controls, controls over how we manage and audit changes to systems and infrastructure, and the controls for how we authorize and authenticate changes to sensitive data and database systems.

Data controls are spread over large portions of the enterprise information architecture. They include perimeter protection, user and operator identity and privilege assignment, application systems controls, identification of sensitive database objects, database access protection and monitoring, encryption of sensitive information at rest and in transit, monitoring network traffic and patterns, malware protection, data protection for PCs and mobile devices, and more. The complexity makes it difficult to determine which controls are the most significant. Yet management and auditors must identify which controls they rely on within the organization's system of internal controls. And management and auditors must evaluate and test the key controls in the scope of assurance and compliance practices.

Willie Sutton robbed banks "because that's where the money is." So, "Where's the data?" It's in the database. Many organizations have dozens or even hundreds of databases. And if an insider or attacker can bypass general and application controls by directly accessing the database, then the only thing we have is a false sense of security about the integrity, confidentiality, or even availability of the data.

We really need to protect our databases and the data in them. The process is effective database administration. Yes we need effective control of data flowing into, through, and out of our networks. And we need controls over data in the unstructured environments of data in transit and in personal computers, portable storage devices, and personal digital assistants. But the central repository is the database, and until we can provide positive assurance about control for the data in the database we have no basis for assuring the reliability of data or controls in the other environments.

This article is a "call to action" for protecting the database. It proposes an approach to data controls focused primarily on the database as a central repository and control point for sensitive and

valuable information. It recommends taking advantage of available technology to centralize controls for database protection and monitoring. It recommends audit steps to ensure the key data access controls are reliable. It explains why management should establish an ongoing objective to establish, validate, and maintain effective database controls. Recommendations are based largely on the PCI DSS, but are also applicable or adaptable to SOX and other requirements.

INFORMATION SECURITY AND DATABASE ACCESS CONTROL

“Information Security” means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

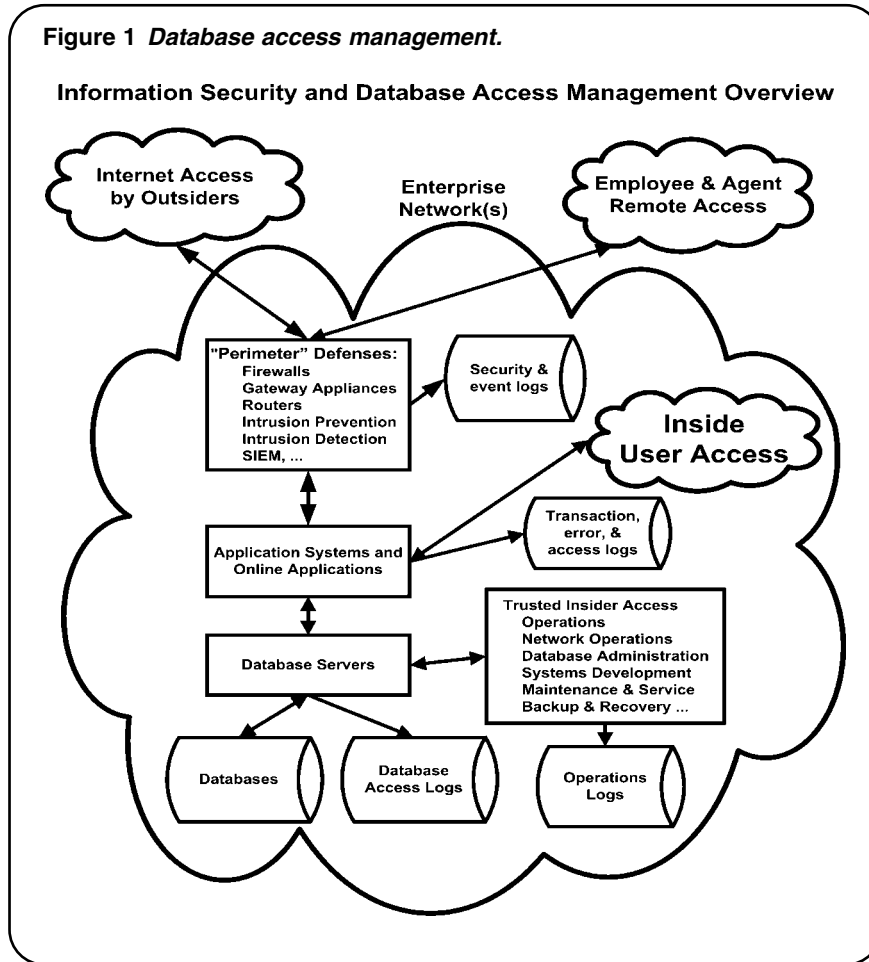
- Integrity—guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
- Confidentiality—preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- Availability—ensuring timely and reliable access to and use of information.¹

Data access control is a key element of information security (see Figure 1). When considered in the context of enterprise information access management, it is an immense and complex subject. It encompasses the structured as well as unstructured repositories of sensitive and other valuable information throughout the enterprise as well as across relationships with customers, stakeholders, business partners, governance and regulatory bodies, and auditors. It encompasses virtually every term and concept used to describe information throughout its life cycle. While this article is relevant to all of those concepts, it does not attempt to “boil the ocean.” Instead, it focuses on the tools to manage and secure information in its primary repository—the database. And it focuses providing guidance on management and auditing of database security in a way that will promote assurance and compliance.

SECURING THE DATABASE

In a simplified (one may say idealized) view, information is collected from a variety of sources, each with appropriate controls to ensure data integrity and protection. Data elements from multiple sources are organized and combined in a database. The database security is usually managed by a commercial Database Management System (DBMS) with a set of rules based on security policy. Records are maintained for every database access to note new information added, changes and deletions, as well as the providing of views and copies of information. Depending on the sensitivity of information, it may be encrypted and complete and unimpeachable records of all accesses may be kept and made available for assurance, compliance, audit, discovery, and forensics.

Figure 1 Database access management.



If you find the environment subject to audit in your organization does not quite match the idealized view, it may be because alternative control approaches are in place, or perhaps enterprise risk management has not yet reached a level of maturity capable of defining or maintaining information security at an acceptable risk level. Perhaps other issues have priority, or maybe management is just not aware of the sensitivity of data in communications, processing, or storage.

From a technical viewpoint the tools for database protection and monitoring have evolved over many years and new developments continue to effect what can and cannot be done effectively to provide complete and efficient database protection. While commercial DBMS typically include some capability to monitor database access and provide audit records, native DBMS features are often not used because of the burden on processing, response time, and storage space. Instead, access controls have tended to migrate into application systems wherein the "trusted application" is granted permission to access and modify the database and the application determines and verifies "authorized" users and what they are allowed to do.

With the advent of remote access, much emphasis for access protection shifted to the "perimeter" and an array of preventive and detective tools were created to keep the bad guys out

and allow only trusted parties inside the network. But this “hard shell” and soft interior model soon fell victim to insider abuses and to the heightened capabilities of desktop and portable computers and storage devices to create and move copies of data. Access protection weaknesses were further exacerbated by the ability to transfer files and individual records indiscriminately across the Internet, and by malware and attacks designed to exploit software vulnerabilities in Internet-facing systems.

Because of the emphasis on perimeter and other network access controls, and reliance on application-based protection, information security practitioners have tended to view the database itself as a relatively safe and protected entity within the systems and network infrastructure, and additional security has not been perceived as a priority. But this view is changing with the increasing incidence and costs of data disclosure and the related penalties.

The insider threat is serious, and the harm that can be caused by insiders is becoming more evident. Security regulations, legislation, and proposed legislation are focusing specific attention on controlling insider access. The category of “privileged users” (from supervisory override to database administrators, system developers, and other technical roles) is now a key focus of tightened requirements. Although a certain element of trust is necessary among key employees, the ability to verify all accesses is essential for protecting not only the data but also the rights, responsibilities, and interests of trusted insiders.

Further, “insider” activities such as customer service, technical product support, systems development and maintenance, security services, and other sensitive functions are now frequently outsourced, perhaps offshore, and this trend is growing. This blurs the lines between outsiders and trusted insiders, and heightens the need for reliable database access protection and monitoring.

SECURING SENSITIVE DATA

The database remains the primary trusted repository, but copies of sensitive, private, and volatile records are now widely dispersed across most organizations and across organizational boundaries. Availability of wireless communications and inexpensive, high volume storage devices increases the direct risks to exposure or theft of sensitive data. To ensure effective control of sensitive data, controls must recognize and record not only who accesses the data, and when, but also what they do with it.

The genie is out of the bottle. By dispersing access controls across a tremendously broad and frequently changing infrastructure of networks, hardware, software, and user interfaces, organizations have created a control problem of immense proportions and complexity. In large global networks the requirements for protection, detection, assurance, and compliance are beyond human comprehension and will only be resolved by applying new developments in technology to detect all existing instances of sensitive data, discover and protect all access and egress methods and practices, and return a semblance of

order and auditability to transactions, processing, storage, and communications.

The way to start solving a set of problems this large and complex is to establish priorities and begin solving the most significant problems first—one at a time—within an overall plan to provide and maintain a reasonable level of risk and substantial compliance with security requirements. In the interest of providing targeted and useful information we will now focus on perhaps the most significant control point—information protection and monitoring of the database itself.

WHAT ARE THE COMPLIANCE REQUIREMENTS FOR DATA PROTECTION?

Compliance requirements vary by industry, company, and activity, and there is no silver bullet to ensure compliance. Compliance is accomplished by meeting requirements and ensuring the ways requirements are met actually provide effective security and accountability. Compliance alone is merely meeting a baseline set of minimum requirements, and the minimum is rarely sufficient. An organization can be in compliance with a lot of requirements and still not have effective security. The goal is to provide both.

Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) is a good example of information security requirements with broad applicability. PCI requirements have gained stature in recent years and they apply to any organization that processes, stores, and transmits cardholder account data. (Michigan and other states have even proposed writing PCI compliance into law with criminal penalties, imprisonment, and fines.) PCI compliance must be demonstrated and documented through automated and manual systems audits.

The 12 major PCI DSS requirements are structured to promote: effective information security policies, secure networks, protected cardholder data, vulnerability management, strong access controls, and regular monitoring and testing.

Central to all the PCI requirements is the need to protect data access, ensuring accountability, privacy, and data integrity. *The simple goal is to ensure only authorized individuals have access and to ensure all access is monitored.* To limit access to only people whose jobs require it, access protection must apply to identifying the sensitive data elements, the methods for managing user credentials and access rights, and the records of who accessed what, when, and what they did with it.

PCI DSS Requirements in a Nutshell

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data

2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security (https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf)

Please note the requirements listed here are only a brief summary of the 17 pages of the PCI DSS available at the indicated Web address. For example, Requirement #3 goes into significant detail about encryption as a critical component of cardholder data protection. The intent is to ensure unauthorized access will yield only unreadable data. Specific control requirements include keeping cardholder data storage to a minimum, not storing sensitive authentication data, masking personal account numbers (PAN) when displayed, and more.

Compensating controls are an important part of these requirements. For example, Requirement 3.4 specifically requires rendering the PAN unreadable anywhere it is stored “(including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks.)” But recognizing that some companies may be unable to encrypt cardholder data, for whatever reasons, the standard allows for “*Compensating Controls for Encryption of Stored Data.*”

Compensating Controls

Compensating controls are those considered when the preferred controls are inadequate or not applied.² PCI DSS requirements allow compensating controls to be considered “... when an entity

cannot meet a technical specification of a requirement, but has sufficiently mitigated the associated risk.” To be allowed to rely on compensating controls, companies must first undertake a risk analysis and document legitimate technological or business constraints for not being able to meet the specific PCI requirement(s).

Compensating controls have varying degrees of effectiveness, and management’s assurance of controls effectiveness must identify why and how compensating controls are reliable in a given environment. The compensating controls must be in addition to PCI-required controls, and must satisfy the PCI’s glossary definition of compensating controls (see References and Resources at the end of this article). Auditors must also consider management’s assertion of effectiveness of the compensating controls.

PCI DSS requirements spell out the conditions for reliance on compensating controls for Requirement 3.4—Render the Primary Account Number (PAN) Unreadable. The company must understand the risks to the data posed by maintaining it in readable form, and show how the compensating controls meet the specified conditions. For PCI Requirement 3.4, the compensating controls for protecting access to readable PANs must accommodate a broad range of avenues of possible access to the data. Each of the compensating control requirements must be demonstrated and tested both for management’s assertions of control and for the auditor’s assessment and attestation.

More About Compensating Controls, Testing, and Audit

Auditors assess key controls for their ability to consistently and reliably meet specific control objectives. In cases where a control is only partially effective, compensating controls will be assessed for their ability to supplement the weaknesses of the primary control. Information systems auditors have for many years referred to the controls in a hierarchy such as the PCI requirements as complementary and compensating controls. Today they are also called layered controls.

PCI DSS Compensating Controls for Requirement 3.4

...Compensating controls may consist of either a device or combination of devices, applications, and controls that meet **all of the** following conditions:

1. Provide additional segmentation/abstraction (for example, at the network-layer)
2. Provide ability to restrict access to cardholder data or databases based on the following criteria:
 - IP address/Mac address
 - Application/service
 - User accounts/groups
 - Data type (packet filtering)
3. Restrict logical access to the database

- Control logical access to the database independent of Active Directory or Lightweight Directory Access Protocol (LDAP)

4 Prevent/detect common application or database attacks (for example, SQL injection).

A solid control foundation specified in a policy statement reduces ambiguity when it is enacted in technical control elements. In a solid hierarchy of controls, those threats that evade preventive controls such as intrusion protection will be detected—even if after the fact—by the monitoring controls. Regular testing helps ensure ongoing reliability of the controls infrastructure. So although no control is the fabled “silver bullet,” the right combination of controls provides an acceptable level of risk as well as assurance that the risk tolerance level is not breached.

If user access rights are poorly assigned, policies are not regularly checked and enforced, and/or the organization is not able to keep pace with changes to users’ roles, then individuals may have too much access to data not pertinent to their jobs. If sensitive stored data are not encrypted, then the vulnerability of the data to disclosure is greatly increased. In such cases, compensating controls may be employed to restrict and monitor data access. Such controls may look for suspicious or anomalous patterns in data access (e.g., accessing large volumes for a function that normally deals in individual transactions), or may actually serve as a check on user access rights assignment and detect individuals accessing data not relevant to their position descriptions. However, if a control is only effective for monitoring access by 90% of the individuals allowed to access the database, then compensating or complementary controls must manage and monitor the other 10%.

Database access protection and/or monitoring should serve as a primary point of control, and should provide a double check for the reliability of other controls. If only monitoring is applied at the database level, then risk indicators (reports and alarms) should alert management when actual data accesses exceed authorized levels. The detective monitoring controls must be supplemented by corrective controls that apply to assignment of user access privileges.

When protective controls are applied to database access, then invalid user access attempts will be rebuffed. However, monitoring is still necessary because supervisors may use their authority to override access policy requirements, and even authorized users may show signs of abusing their privileges.

Strong access protection controls applied at the database level can be considered a primary control for PCI DSS compliance if they protect and monitor access rights of all users, including privileged users. However, if controls at the database are weak and/or subject to override or modification by privileged users, or do not include encryption of the PAN, then they must be supplemented with compensating controls. The auditor must assess and determine

the reliability of database access controls when determining which controls are significant and when designing the audit test plans.

WHO ACCESSES THE DATABASE AND WHY?

Lots of people need access to the database and the database owner or custodian has the responsibility for knowing who they are and what their access privileges should be. The “effective practice” control concept is the principle of “least privilege” or allowing user access to only the data needed for the job. The organization has a responsibility to ensure data protection policies are well defined, appropriate to the levels of protection required, and effectively implemented. Companies in certain industries must meet regulatory requirements to ensure personal information privacy is protected. People at all levels of the organization have a role in defining data access privileges and ensuring they are enforced with effective controls.

For publicly traded companies, the CEO and CFO are responsible for reporting on the effectiveness of internal controls, assuring the protection of sensitive assets, and assuring the reliability of financial reporting. The Board of Directors has the governance role in this responsibility. Auditors must perform analyses and testing so they can report on the reliability of access controls as well as attest to management’s control assertions.

Database access protection is perhaps the most significant control for ensuring the protection of data assets and the reliability of data managed and provided for financial reporting. Essential to providing access protection are the elements of knowing who is allowed to access data and what they do with it: the rights and circumstances for allowing data to be changed, and keeping records of all accesses and changes. Continuous monitoring of access is essential for ensuring the data protection controls remain in place and are effective.

If you think of an access policy management agent sitting at the access point for the database, checking the credentials of every individual attempting access, reviewing the access for consistency with specified privileges and policies, allowing or disallowing access, and then keeping a record of each and every access or attempted access, its purpose, the function performed, and the before and after state of the data elements accessed, you begin to understand this responsibility.

Auditors might like to see a complete and consistent set of data protection controls in place, but such a state is rare. Auditors must audit what they find rather than what they would like to find, and couch their reports and recommendations within the realm of what is reasonable and achievable. The auditor should be able to work with management and agree to plans for improving controls as needed to attain a reasonable level of protection and a “substantial” level of compliance. The costs of control are always a consideration, and it may not be possible to show financial benefits of the improvements. Further, management may be willing to live with the stated risks rather than implement potentially costly changes (which they do not understand) with no guarantees of improvements in efficiency or reliability. Estimated costs may also

be weighed against the threat probability and the potential costs of non-compliance penalties.

When you consider the complexities of different roles, responsibilities, and circumstances involved in security decisions, and when you multiply database accesses by potentially billions of times in a given period, you can see the task of protecting the data is not simple and the resources needed to make it work properly are not trivial. Fortunately database protection encompasses a combination of human and technology issues and concerns that can be answered almost entirely with a technology solution. The word “almost” is used because any such solution requires human monitoring and ongoing assessment to ensure its continuous reliability.

Now let’s look a little closer at who accesses data and why, and at how access privilege controls are managed and monitored.

Customers

Customers are a primary user of their own data. For example, use of a credit card initiates an access to customer data on behalf of the customer to allow access to credit, cash, or even just information such as available account balance. The controls over access to data and transactions that change the data proceed through a structured path designed to provide reasonable assurance the customer is legitimate, the transaction is within acceptable limits, and the cumulative effects of multiple transactions do not exceed prescribed limitations such as maximum daily withdrawals or credit limits, and other important protections. These controls, although not perfect and occasionally breached, generally provide the acceptable level of risk needed for the customers, merchants, and financial institutions involved to trust and be protected by the processing system.

At the database level, access to the data is frequently recognized as an application-level control function such that access is provided to the trusted application rather than to the combination of the application and the individual initiating the activity. In many cases the database access by a trusted application is not even logged at the database level. Transaction and error history is maintained by the application. In other cases database logs may be required for each access regardless of the trusted status of the application. And in highly sensitive circumstances the authorized individual as well as the trusted application and the individual data elements accessed and/or changed must be logged.

Business Partners

Access to sensitive data by agreement between business partners is managed similarly to customer access. But in this case each business party to a transaction or inquiry will bear their own responsibility for protecting the data and for reasonable assurance that reliable protection will be provided by the other business party/parties to the transactions.

In the audit world, the reliability of business partners is frequently attested through the provision of a SAS 70³ audit. A SAS 70 is provided so multiple business partners can rely on the

controls in a given business entity without each one having to conduct their own assessment of the entity's controls.

Employees

With employees we begin to get to the heart of requirements for authorization, authentication, and monitoring of access to sensitive data. Put simply, employees are provided a certain level of trust to allow them to do their jobs. Generally, the more sensitive the job, the higher the level of trust placed in the employee. Many are the examples of trusted employees betraying their trust, sometimes for personal gain, sometimes for retaliation or revenge, sometimes just to make things look a little better than they really are, and sometimes even millions or billions better than reality.

It is unfortunately all too common to find employees with far greater access privileges than they need to accomplish their responsibilities. There are many reasons for excess privileges (but that is a subject in its own right). The solution is to adopt and apply the principle of "least privilege." It is far better to tightly restrict access on an as-needed basis and then make exceptions only as needed for special cases. This approach also ensures these "special cases" are noted and can be monitored.

WHAT EMPLOYEES CAN DO WRONG

Auditors say, "Trust but verify." And it is often more of a goal than a reality. Because trusts are betrayed we have financial debacles that destroy companies and financially injure millions of stakeholders with an interest in the reliability of the company's financial reporting. And we have trusted employees willing to take sensitive data entrusted to their custody and sell it for personal gain.

Customer Service and Business Operations Employees

Customer service often involves repairing mistakes made by people or errors in systems. Whether routine customer transactions or more complicated tasks like error correction, it is important to know exactly what each employee is and is not allowed to do. It is also important to maintain records of exactly what each person did, when they did it, and the results. And it is important to be able to establish innocence as well as guilt.

When access to data is controlled via application systems, it is still important to view data protection from the database level. Not all applications are created with equal security, and applications can be modified intentionally, accidentally, or as the result of an attack. An auditor performing a database access control audit must determine all application systems with access to the database and establish the reliability of controls for each one. If the applications have been audited, the auditor can review the results to determine whether they can be relied on for the purposes of the database audit and adjust scope accordingly.

Application Systems, Database Administration, Technical Support, and Maintenance

Some companies say they rely on the access protection and monitoring provided by commercial application systems (such as the ERPs), and do not see a need for access protection at the database level. Part of the logic is that the ERPs tend to be so complex that any alteration of data at the database level would be detected because of problems it would cause within the application. This theory also presumes all application errors and issues are traced to their source and corrected, and it does not address the disclosure risk resulting from users and technical personnel with access to databases and database servers. And inappropriate changes and disclosure are not the only risks. Even the ability to read data represents risks such as inappropriate access to inside information about financial results and personal information subject to privacy regulations.

The development and maintenance of application systems requires access to databases and their data. In some cases this access is protected by maintaining development and testing environments separate from production. In other cases a company may decide such controls are too complex or expensive and will opt for managing production data access within the scope of the development and change management cycle. Regardless of the approach used, the result is significant potential for programmers to have access to production data or copies of it. In either case sensitive data must be protected and monitored wherever it is located, and such protection is outside the scope of application systems controls.

Data administration and database administration may or may not be separate functions. Here collectively called DA, they include the responsibility to understand and manage the sharing of data and databases by all users and application systems. DA may be responsible for ensuring consistency in assignment of access rights, the application of edits and validation, and limitation of access to the database. If the access protection role resides with the application(s), that responsibility must be clearly understood and closely coordinated with DA.

Database technical and operational controls such as backup/recovery, checkpoint/restart, maintaining pointer integrity, optimizing physical data storage and performance, and so on take place outside the access constraints of application systems, but must also be closely coordinated with application and user requirements.

Systems and network administration, DA, security operations, systems development and maintenance, systems programming, and other technical functions all have legitimate needs for access to databases. They need the freedom to correct problems and restore or continue operations. Some believe the people in these functions cannot be controlled or monitored. Although that is not true, such control may be difficult and you can count on those people to resist control changes they may see as making their jobs more difficult or “impossible.” Physical and logical controls within and outside their sphere of operational control must provide evidence of their

actions. These controls are important and necessary, and must be sufficient to clearly establish fault or innocence.

Separation of duties is a key control in technical environments. In the case of personnel with physical or root access to computers, it is important to ensure system and network monitoring will provide evidence of their actions. For example, if a technical support person can access and modify log records, it is important for a system outside of their control to monitor their activities. If no one else in the organization is capable of monitoring a person providing technical support, then such monitoring can be provided by a third party.

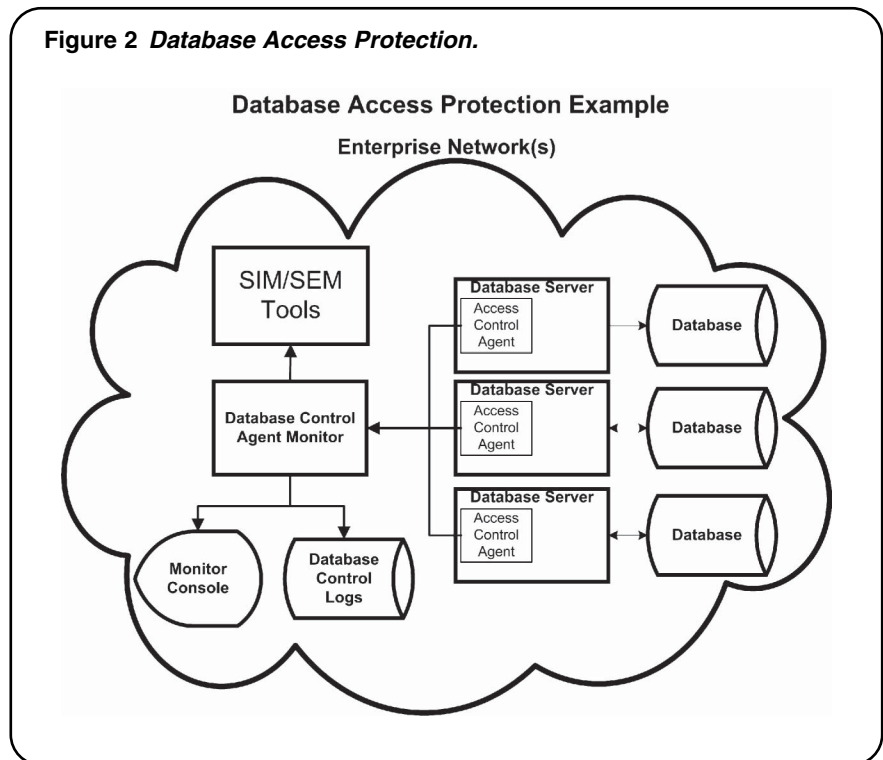
This section illustrates the importance of understanding who has access to data and databases, what their access rights are, and how they are controlled. It is important to understand that anyone with physical access to computer hardware or root access to systems may be able to bypass all controls and monitoring associated with systems or data on such hardware—depending on their technical competence and level of supervision. The risks of unauthorized access, modification, destruction, or disclosure of data must be considered in the light of all personnel with access rights.

RECOMMENDED APPROACH: CONCENTRATE DATABASE ACCESS CONTROL AT THE SOURCE

If you place database access protection and monitoring as close as possible to the database, you gain the advantages of simplifying the access protection model while also supporting separation of duties, forensics, and audit requirements. Placing policy management and monitoring controls as close as possible to the object of the controls, in this case the database server, can make it difficult for anyone to avoid or bypass those controls.

The PCI DSS provides a good list of control requirements specifically applicable to database access control. This section illustrates how selected examples of those requirements can be met with access protection and monitoring implemented at the level of the database server. Such controls may be implemented through monitoring at the network traffic level, but would not apply to activities performed within or upon the database server itself. The controls can also be provided via a security appliance or with an agent on the database server communicating with a separate monitoring and control system. For this description, we will address the controls as implemented via the agent and monitoring system.

This simple solution employs a software agent that runs on the database server enabling policy-based data access protection and monitoring. By communicating with a separate system the agent can ensure it has not been modified by persons with root access to the server. Note the agent should be capable of operating in a monitoring-only mode for analysis, discovery, or audit purposes, or in full-protect mode to enforce security policy at the database level.



How this Solution Compares to PCI DSS Requirements

Requirement 2.1—Always Change the Vendor Supplied Defaults Before you Install a System on the Network

Caveat: System upgrades and patches may reinstate vendor defaults.

Solution: *Provide policy-based access protection on the database server.* Use a tool that can apply security policy at the database server level. Access to specified data types can be denied to unauthorized users and/or unauthorized computers. Access attempts using a default user name or password, unauthorized users, or unauthorized computers can be denied (terminate session) and/or generate an alert.

Ideally, policy enforcement can be tuned for such details as whether a person can access simultaneously from two or more machines, and can recognize anomalies like a user ID logged in locally also attempting a remote login.

Requirement 2.2—Develop Configuration Standards for all System Components

Address all known security vulnerabilities, consistent with industry accepted system hardening standards, prevent misuse, remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems.

Caveat: An organization not already committed to configuration security standards (such as those by the Center for Internet Secu-

rity, CIS, www.cisecurity.org) may find it impractical to harden and continuously maintain all databases in a hardened mode.

Hardening? Can you make “soft”ware “hard”er?

Wikipedia (www.wikipedia.org) says hardening is the process of securing a system—especially to protect systems against attackers. This would typically include removal of unnecessary usernames or logins and disabling or removing unnecessary services.

Database security may require hardening of the security settings of the database management software upon installation, and once a specific database (often referred to as an instance) is established and configured. Additionally, many database utilities have their own enhanced security that can be enabled, but is disabled by default. An example is establishing the password on the Oracle listener process, to ensure unauthorized users cannot change configurations related to the database management software.

The Center for Internet Security is the best resource for guidance and tools to “harden” systems. CIS is a non-profit enterprise whose mission is to help organizations reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls.

CIS members develop and encourage the widespread use of security configuration benchmarks through a global consensus process involving participants from the public and private sectors.

The practical CIS Benchmarks support available high-level standards that deal with the “Why, Who, When, and Where” aspects of IT security by detailing “How” to secure an ever widening array of workstations, servers, network devices, and software applications in terms of technology specific controls.

CIS Scoring Tools analyze and report system compliance with the technical control settings in the Benchmarks.

The CIS Benchmarks and Scoring Tools are available for download free of charge to the Internet community from the CIS website.

Solution: Ensure access controls provide protection for known vulnerabilities. Employ a strict security policy relevant to your organization. Configure access protection policies on the database server to prevent any user attempt to exploit vulnerabilities for any databases whether or not they are hardened. Ensure the system vendor maintains the protection tool to compensate for all known vulnerabilities.

Requirement 3: Protect Stored Cardholder Data

Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic

keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.

Caveat: Database encryption is effective as a prevention measure for non DBMS data access, such as copying raw data files from the database (provided data access does not also provide access to the encryption key). But data encryption can impact overall database functionality, performance, and management. Encryption is also ineffective for authorized users (or for unauthorized users with authorized IDs and passwords) as data is decrypted once extracted from the database using the DBMS.

PCI standards permit compensating controls for some of the data encryption requirements. This is especially relevant for section 3.4.

Encryption and Audit Trails

Encryption and Audit Trails are touchy subjects for organizations housing vast quantities of data and for the DBAs that manage the data. Both techniques have definite pros and cons. For example, encryption can be applied on a selected set of rows, one or more columns, or the entire database. Encryption also can be either disabled by default, or enabled at the DBA's request for the database authentication that occurs when a user connects.

Without the proper controls, a user's authentication credentials (i.e., username and password) can flow across the network in the clear even though the social security numbers in the database may be properly protected. If the connecting user is the DBA, security can be severely compromised or rendered useless. Audit trails are wonderful tools, but must be cautiously enabled for specific events, rather than for all database object activity.

Solution: Implement encryption or compensating controls as specified for section 3.4 in Appendix B. *Encrypted:* Ensure security policy protection covers improper access of sensitive data and monitoring controls are set to detect unusual patterns in data access such as users accessing data in unusually large quantities or in patterns different from the usual transaction processing.

Protect stored encryption keys by monitoring and auditing all access to the encryption keys. This can be achieved by configuring the security policy to prevent unauthorized access to encryption keys (terminate the session, send an alert).

Not Encrypted: Ensure security policy enforcement tools define a level of granularity that adequately identifies all accesses of sensitive data (source IP address, source application, user account, OS/MS domain account, application user ID, target data object, DB activities [DML, DDL, stored procedures, triggers, etc.] and any other evidential information needed).

Requirement 6: Develop and Maintain Secure Systems and Applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses. Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations.

Caveat: Security patches may be impractical for database systems. Security patches may appear frequently and often require down time for the patched systems. In many cases, the patches may change the behavior of the patched system to the extent that it interferes with its previous functioning. To avoid risks of interference with business continuity, patching complex systems may require a multi-stage, time-consuming process of testing and planning before the implementation of each patch. It is common practice to aggregate multiple patches before applying them to save effort and avoid system downtime. The result is that systems can remain unpatched (i.e., vulnerable) for some time before the next patch cycle. PCI requires you to maintain your systems soon after any security patch is issued by the vendor.

Solution: Ensure policy-based access protection on the database server includes known but not yet patched vulnerabilities. Configure access protection policies on the database server to prevent any attempt to exploit system vulnerabilities that are not patched. Ensure the system vendor maintains the protection tool to compensate for all known vulnerabilities. In some cases the security vendor may upgrade protection even before the DBMS vendor patches are available or when they are available but installing them poses a major risk to the system. When the source of the attack is the application itself, the software should also be able to provide visibility into the application user ID, which both deters and enables forensics if an attacker manages to execute an attack.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

This requirement ensures critical data can only be accessed by authorized personnel.

7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.

7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.

Caveat: Databases may have a built-in granular access control policy, but an inherent issue with role separation is that in many cases DBAs end-up owning a large set of entitlements over the databases, including aspects of the security policy itself. The enforcement mechanism should eliminate this issue.

Solution: Ensure access protection on the database server extends to all privileged users. Role separation is an important

control—particularly for privileged users. Fine grained access policy enforcement includes deterrence as well as preventive controls. Protective controls should include prevention as well as alerting of privileged users (such as DBAs) for attempts to access sensitive areas of the database.

General controls for limiting access include:

- Limit unprivileged users by denying all user access to sensitive (card holder) data with the exclusion of specific (need to know) users.
- Translate security definitions into a set of specific rules for individual sensitive data elements where the only solution is to define what each user is entitled to access.
- Be realistic about the role of privileged users such as DBAs or developers.

One cannot avoid granting DBAs, developers, and others high enough privileges to pose a substantial risk to the organization. Ways to control privileged users include building monitoring and alert rules over privileged user accounts, alerting about suspicious/risky actions, and preventing actions that can be identified as malicious.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.

Caveat: Current solutions (either database inherent or network-based solutions) do not track and monitor all access to card holder data. Solutions may fall short for several reasons:

- Role separation: Relying on inherent database audit mechanisms only, enables privileged users to disable system or audit logs.
- Performance implications: Fine grained auditing significantly impacts the performance of the database system, and often results in not using these mechanisms at all.
- Network-based enforcement is insufficient: Trying to control database access using network devices leaves local activities and/or remote-shell access uncontrolled.
- Using local access to the system enables savvy privileged users to modify system files for their own (possibly malicious) purposes.
- Database logs, monitoring, and auditing are useless if DBAs can turn them off when they want to.

Solution: *Ensure access protection on the database server addresses all transactions, provides preventive measures, full monitoring, and audit capability.* Agent-based database security software avoids the operational overhead of using the inherent DBMS

controls and imposes no substantial burden on the database server. This enables efficient implementation of security as well as collection and analysis of evidence for forensics and auditing.

Requirement 10.2: Implement Automated Audit Trails for all System Components to Reconstruct Key Events

- 10.2.1 All individual user accesses to cardholder data.
- 10.2.2 All actions taken by any individual with root or administrative privileges.
- 10.2.3 Access to all audit trails.
- 10.2.4 Invalid logical access attempts.
- 10.2.5 Use of identification and authentication mechanisms.
- 10.2.6 Initialization of the audit logs.
- 10.2.7 Creation and deletion of system-level objects.

Caveat: Referring to database systems, this section requires the ability to associate each access to a data object in the database to a specific user ID, which in many cases goes beyond the database user account information. For instance—cases where multiple users regularly use the same database account (shared accounts) or when a client application is accessing the database on behalf of a user, using a single database account for all users.

Solution: *Ensure audit trail features of the database protection tool enable complete reconstruction of key events.* The tool must prevent unauthorized access to the database audit log, and fully monitor legitimate access by authorized users. The logs and audit trails must be inherently secure and separate from the database.

Requirement 10.3: Record Key Audit Trail Entries for all System Components for Each Event

- 10.3.1 User identification
- 10.3.2 Type of event
- 10.3.3 Date and time
- 10.3.4 Success or failure indication
- 10.3.5 Origination of event
- 10.3.6 Identity or name of affected data, system component, or resource

Caveat: Inherent DBMS auditing mechanisms may not provide actual (application) user identity information. Managing the required level of granularity is also a challenge as the auditing system must enable effective analysis. Relying solely on database inherent audit mechanisms does not adequately restrict privileged users from turning-off, deleting, or modifying audit logs, which deems the whole process ineffective.

Solution: *Ensure audit trail features of the database protection tool capture all required data.* The database protection and monitoring tool must create audit trails containing all the details required by sections 10.3, including the actual user identity provided by the application. The system should also make it easy to review access on an ongoing basis while enabling users to view only the relevant audit information without requiring them

DATABASE CONTROLS AND AUDITS MUST ADDRESS:

- USER INTERFACES*
- OPERATION OF THE DBMS*
- DATABASE ADMINISTRATION*
- DATA DEFINITION AND DOCUMENTATION*
- SECURITY AND ACCESS*
- ORGANIZATIONAL POLICIES AND PRIORITIES*
- BACKUP AND RECOVERY*
- BUSINESS CONTINUITY*
- COMPLIANCE WITH STANDARDS AND REQUIREMENTS*

to sift through millions of records. Features for using the built-in database auditing mechanisms should include user-friendly sorting and query rules for audit trails.

How the Database Access Protection Control Solution Improves Efficiency

Having a single source for recording all access to the database reduces the level of effort required for controls analysis and auditing. Controls analysis can be significantly less demanding than that required when controls are based in multiple applications, operations logs, network traffic monitors, data scans, and so on. When controls are centralized in a single source, it facilitates the ability to verify compatibility across multiple operational areas. The existence of similar controls in application systems may include redundant data, but the organization benefits from complementary controls and with controlled redundancy.

Auditing Database Access

Conceptually, database auditing focuses on answering some fairly basic questions: “Who accessed and/or changed the data, when, and how was the content changed?” The difficult part lies in assessing the full scope of controls to determine their effectiveness in: fully recording all accesses, ensuring only authorized access, and maintaining unimpeachable evidence for assurance and forensics purposes.

The attached “Example Database Access Control Audit Program Elements” is a list of audit issues selected for their relevance to security and access control. A broader scope audit program may be required for audits with a different purpose or objectives.

To review and summarize material covered thus far, the database environment is complex and controls must address: User Interfaces, Operation of the DBMS, Database Administration, Data Definition and Documentation, Security and Access, Organizational Policies and Priorities, Backup and Recovery, Business Continuity, and Compliance with Standards and Requirements. Access protection begins with understanding who accesses the data, for what purposes, and with what permission.

CONCLUSION

Remember, the way to start solving a set of problems as large and complex as information access protection is to establish priorities and begin solving the most significant problems first—one at a time— within an overall plan to provide and maintain a reasonable level of risk and substantial compliance with security requirements.

At the core of business controls over information, as well as PCI DSS requirements, is the need to protect data access ensuring accountability, privacy, and data integrity. *The simple goal is to ensure only authorized individuals have access and all access is monitored.* To limit access to only people whose jobs require it, access protection must apply to identifying the sensitive data elements,

the methods for managing user credentials and access rights, and the records of who accessed what when and what they did with it.

A single source for recording all access to the database is an efficient approach to controls, assurance, and auditing, and can be significantly less demanding than the effort needed to manage controls based in multiple locations. When controls are centralized in a single source, it facilitates the ability to verify compatibility across multiple operational areas.

If you place database access protection and monitoring as close as possible to the database, you gain the advantages of simplifying the access protection model while also supporting separation of duties, forensics, and audit requirements. Placing policy management and monitoring controls as close as possible to the object of the controls can make it difficult for anyone to avoid or bypass those controls.

Auditors must audit, evaluate, and test the controls they find in place for database protection and monitoring, but audit recommendations can focus on moving the organization to a more reliable and efficient approach to information protection and access control.

EXAMPLE DATABASE ACCESS CONTROL AUDIT PROGRAM ELEMENTS

Database controls include the hardware and software of the database system, interfaces with other systems, database personnel, and the policies, procedures, and activities supporting the data and its uses. The data dictionary typically contains an index and descriptions of all items in a database, and shows the data location and the access method. Data dictionary controls are important for database security.

Some controls may not seem relevant to security, but are worth considering for their potential to impact or be impacted by security. For example, user service level may be impacted if security tools employed impact system performance. Quantity, type, and sensitivity of records stored and transactions processed and the number and types of system users are also indicators of the need for capacity, performance, and security.

Risk Management

A key audit component is the risk associated with the data maintained in the database and the potential impacts if risks materialize. For each control objective the auditor must assess the specific controls in place and consider the risks and consequences if the objectives are not consistently and continuously met.

Control Objectives

- Appropriate assignment of responsibilities including separation of duties
- Access allowed only as appropriate (no unauthorized access)
- Completeness and accuracy of data in the database
- Evidence that each transaction or update is accurately applied and recorded

- Appropriate management of data sharing
- Adequate transaction/access audit trail
- Adequate service level for database users
- Data recorded in the appropriate calendar period
- Ability to detect and recover any failure of the DBMS
- Sufficient evidence and analysis to detect and recover from attack, fraud, and embezzlement
- Current and adequate documentation, to include,

For database structure:

- how security is achieved
- recovery actions
- reorganization changes

For each data element:

- precise and unambiguous definition
- source
- frequency of change
- individual accountable for correctness
- relationship to other data items
- program(s) and individuals authorized access and the type of access
- physical devices authorized to access (example, payroll department only)

- Continuity of processing
- Compliance with internal and external policies, standards, and requirements
- Effective management of systems development, maintenance, and changes/patches
- Periodic independent database audits

Audit Evidence

Each database environment may have slightly different forms of evidence. The following items are typical forms of evidence to be evaluated in verifying the integrity of a database system:

- Database management system*—software that manages the database, and its controls
- Data dictionary system*—automated documentation tool for metadata
- DBMS logs*—history of all transactions occurring during database operations
- Security logs*—log of accesses and potential or actual security violations
- Database utilities*—variety of utilities in the DBMS to perform day-to-day maintenance
- Database structure map*—pictorial representation of the database structure, produced by a utility program
- Database verifier reports*—listing of integrity problems in the database structure produced each time the database verifier utility program is executed
- DBMS reports*—periodic status reports produced by the DBMS providing statistics about the content and operation of the DBMS
- Security profiles*—listing of the resources accessible to individual users

- Organization charts and job descriptions*—assignment of responsibility, segregation of duties, and accountability for actions
- User complaints and requests*—documentation of the problems and needs of users
- Master operation procedures*—process for performing privileged maintenance on the DBMS
- Database operating procedures*—instructions provided operators for day-to-day operation
- Database recovery procedures*—instructions provided operators on how to prepare for and conduct recovery after a database failure
- Database reorganization procedures*—instructions on when and how to reorganize the database
- Database integrity procedures*—methods used by database administration, operations, and user personnel to verify the proper functioning and content of the database

Internal Control Assessment

The auditor should look for key controls over specific activities:

End-User Interface to DBMS

- Program modification and maintenance control*—management ensures the proper change is tested and installed in the proper version
- Adequacy of programmed input validation check*—routines to verify the accuracy, completeness, and authorization of input

Operation of the DBMS

- Access authorization control*—ensures only authorized individuals gain access to database resources appropriate for them
- Data error handling*—procedures and timeliness in examining and correcting errors
- Concurrent data control*—ensures data elements are not misprocessed because of two or more users concurrently processing the same data element
- Deadlock detection and resolution*—breaks a stalemate in processing between two users of the same data record

Data (Base) Administration Controls

- Assignment of responsibilities*—making individuals accountable for their functions
- Segregation of duties*—splitting functions so an individual with responsibility for performing a function does not also have responsibility for using or approving the results of that function
- Processing performance standards*—establishment of criteria to measure economy, effectiveness, and efficiency of the database system
- Reorganization utilities*—tools and techniques for restructuring and expanding the database
- Database verifier*—tool to ensure all data in the database are properly structured and can be located
- Maintenance plan*—predetermined maintenance schedule to correct problems before they occur

Data Definition Controls

- Data element responsibility*—making individuals accountable for each data element in a database
- Conceptual data independence*—database administration establishes data definitions as opposed to individual user groups
- Data dictionary system*—automated documentation for metadata that should be fed automatically into the operating environment

Security/Access Controls

- Database malfunction reporting*—reports to management identifying the type and severity of problems occurring with the database
- Security officer function*—appointing specific accountability for security of the database
- Security profile*—matching user needs to the database functions
- Passwords*—and appropriate password management

Organizational Controls

- Database standards*—methods and procedures to be followed in establishing and operating a database
- Personnel training*—providing courses and materials to teach appropriate skills for personnel using the database
- Review board*—group of managers, users, and database personnel who oversee priorities and projects using the database
- Regulatory reporting requirements*—formal methods to ensure database users comply with regulations
- Personal privacy requirements*—methods and procedures to ensure individual privacy is not compromised through the use of a database

Backup and Recovery Controls

- System documentation*—formal written explanation of the database environment so its continuity and maintenance can be ensured
- Audit trail*—ability to trace transactions from source to control totals and back to source, reconstruct processing if problems occur, and provide unimpeachable evidence for forensics or litigation
- Recovery procedures*—complete and proven tools and techniques for recovering the database
- Application system failure*—procedures for business continuity if applications are not operational
- Backup databases*—database copies made at specific points in time for recovery purposes
- Natural disaster and environmental protection*—measures to protect the database from acts of God and man such as fire, earthquake, and so on
- Business continuity*—ensuring technical database recovery activities are effectively coordinated with the recovery of system user activities and the overall business processing environment

REFERENCES AND RESOURCES

PCI Requirements, www.pcisecuritystandards.org

Payment Card Industry (PCI) Data Security Standard—Glossary, Abbreviations, and Acronyms Compensating Controls

Description: Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must:

1. meet the intent and rigor of the original stated PCI DSS requirement;
2. repel a compromise attempt with similar force;
3. be “above and beyond” other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and
4. be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

Sentriago Hedgehog and PCI DSS Compliance, www.sentriago.com

A document published by Sentriago to assist organizations required to comply with the PCI DSS (e.g., Internet vendors and retail merchants). The document asserts that organizations facing security standard compliance challenges should not merely do the minimum it takes to comply with the standard, but rather understand the implications and use the compliance effort as an opportunity to tighten their security considerably beyond the minimum requirements.

Handbook for Internal Auditors by Lexis/Nexis, www.lexisnexis.com

LexisNexis publishes a complete subscription-based handbook for the internal audit function. Much of the material in the database audit program section is used with the permission of LexisNexis.

NOTES

1. See: 44 U.S.C § 3542 (b)(1) (2006).
2. See Mair, W.C, Wood, D.R & Davis, K.W (1972), *Computer Control & Audit*. Alamonte Springs, FL: The Institute of Internal Auditors, Inc.
3. See www.aicpa.org, and search for SAS 70. For further information, send an e-mail to: info@sas70.com

Charles H. Le Grand, CIA, CISA, Principal, TechPar Group; CEO, CHL Global Associates is an information security, audit, and assurance practitioner and consultant, author, and public speaker. Le Grand addresses critical technology

issues in management, security, control, risk, auditing, assurance, compliance, and governance. He has authored works in *IT Controls*, *Audit Guidance*, *Software Security Assurance*, *Risk and Compliance Management*, *Policy*, *Metrics*, and more. Le Grand served many years at The Institute of Internal Auditors (IIA) headquarters addressing IT issues for the profession. He is a seminar author and instructor, researcher, IT manager, project manager, systems analyst, and IT auditor. www.chlglobalassociates.com

Dan Sarel, Vice President, Product, Sentrigo, Inc., is responsible for directing Sentrigo's product definition and design, and brings over a decade of security software and hardware experience. Dan joined Sentrigo after serving as Check Point Software Technologies' Director of Product Management. At Check Point Dan led the VPN product line and went on to manage an international team that leads all of Check Point's enterprise product lines. Dan led several new product launches and served as a member of the product council, which determines the company's product strategy. Prior to Check Point Dan held a number of product management, marketing, and consulting positions in the hardware and software security product market.