Design of
Database Security Policy
In
Enterprise Systems

by Krishna R Singitam
Database Architect

Table of Contents

1. Abstract 3
2. Introduction 3
   2.1. Understanding the Necessity of Security Policy 3
3. Design of Database Security Policy 4
   3.1. Requirements from Business owners 4
   3.2. Regulatory Requirements 4
      3.2.1. Sarbanes-Oxley 4
      3.2.2. PCI DSS 5
      3.2.3. CA SB1386 5
      3.2.4. HIPAA 5
      3.2.5. SAS 70 6
      3.2.6. Business Domain vs Industry Regulatory Requirements 6
   3.3. Requirements with upstream data source and feeding systems 7
   3.4. Security Requirements form Database Support services 7
   3.5. OS and database Server level Policies 7
   3.6. Security Variations 7
   3.7. Database and Data Encryption policy 8
   3.8. Secure database from Network, Virus Attacks 8
   3.9. Evaluate Security Requirements 8
   3.10. Choose Policies and Exceptions 8
4. Process Chart – 1: Database Security Design Process 9
5. Conclusions 10
6. References 10

1. Abstract

For an enterprise to acquire better market share its products and services should reach out global customers. To achieve this, in a quickest way all the major enterprise systems tend to expose their products and offerings through World Wide Web. Although this puts the enterprise name in the world market, but its battle has just began. Any such product or offering(s) should gain the customer(s) confidence not only in running their business efficiently with superior quality and reducing cost but also should secure the integrity of its customers or end users. Such data integrity means the product or the service should secure the customer or its clients data and their processes for any un-authorized access. Secondly it also should comply to the local government regulations and as per the geographic/cultural laws. Thus along with product or offering's functional features, its ability in securing the data and the processes of the customer is the key element for it to be accepted in the global Market. To secure the data and processes adopted by client a strong security standards to de formulated, which are abstracted from the customer's & end user's security policy. Here is an attempt to derive such a security policy at an enterprise level, so that it can be further refined and tailored as per the specific business problem the product or offering addresses.

2. Introduction

This white paper highlights the benefits of following enterprise database security policy, and dives deep in design principles to arrive at an "Enterprise database security policy". Finally also talks about the process flow to design the Security Policy. This is an attempt to guide the enterprise architect(s) to design a database security policy. But they should tailor it, by considering their specific functional requirements to meet business needs and also local regulations as per the nature of their business problem they are addressing.

2.1. Understanding the Necessity of Security Policy

Following are some of the benefits of designing and implementing Database Security Policy

- Enforce uniform security policies in a consistent manner through out the organization.
- It will help reduce legal liability by enforcing appropriate security standards for customers or business partners.
- It serves as a remainder to various stake holders for their commitment to information security.
- To define the roles and responsibilities of various employees in an organization.
- To track as well as audit the database security violations.
- Gain confidence of customers by keeping their & their clients data and process safe and secure.
- It serves as set of rules to create simplified instructions or checklists for security practices.
- Simplify the security policy implementation process across organization for various business needs.

3. Design of Database Security Policy

A security policy is a document or set of documents that contains the general rules that define the security framework of an organization. Once these rules are formulated across an organization, these can be tailored for any process or product to meet the specific business needs. In a product development environment such a security policy will bind the product or its process with a unified and controlled access to the data to all the user's, interfaces and tools that communicates with it. In order to design a security policy for the database of a product in an organization, special considerations are to be made during requirements gathering. These are termed as Security Requirements which are to be captured and evaluated to formulate security policies. Best suitable methods are to be chosen to implement the mandatory, regulatory and optional policies evaluated. Although the nature of the business processes drives most of the security requirements, below section explains the process outline to capture the database security requirements in order to arrive at database security policies.

3.1. Requirements from Business owners

Securing the enterprise data is one of the key design elements for any product which captures, processes and reports on critical data of its customers. All databases which store such data should be secured for any unauthorized access. The database architect should clearly understand the data and its criticality to the business and design the security policy for the database. To do this task effectively, inputs should be taken from all the business stake holder groups which impact and interact with the data at various stages. These security requirements should address organizations needs for sensitive data protection as well as the needs of user who access the data at various levels.

3.2. Regulatory Requirements

Depending on the nature of the data and the geographic location the business targets, enacted legislation might require securing the data in a specific way. In order to adhere to such legal regulations, consultation with organizations legal counsel is required to understand the regulatory acts that affect the security policy. There are several regulatory acts which are audited at organization level to certify for compliance of the organizations data security policy. These are to be understood clearly and documented as they affect the organizations database security policy. Below are some of well accepted and followed security regulations with which business and so the technical implementation needs to comply.

3.2.1. Sarbanes-Oxley

The Sarbanes-Oxley legislation of 2002 (SOX) forced publicly traded companies to be more transparent about their financial data. This talks about the process to adhere "effective

controls" in place. As per SOX in a nut shell on the financial data security is highlighted below.

- § SOX Section-302: - require executives to certify the accuracy of financial reports. This is to control the data flow that used to generate the reports and to make sure that data cannot be seen or accessed by unauthorized personnel, altered without authorization, or otherwise tampered with.
- § SOX Section-404: - require executives and auditors to confirm the "effectiveness of internal controls". Auditors put particular emphasis on:

  - Ensuring the integrity of sensitive data
  - Activity of privileged insiders
  - Traceability of data (audit trail)
  - Separation of duties (audit independence)

3.2.2. PCI DSS

The Payment Card Industry's Data Security Standard (PCI DSS) is the result of the joint efforts of the major credit card companies. It is not legislation nor regulation but a standard, and periodically gets updated (so far – once a year). The standard compels merchants and companies who process and store credit card data to comply with a set of technical and procedural requirements, and pass audits. PCI gets specific about what measures need to be put in place for protecting credit card data.

- Card holder data encryption
- Securing the network for the credit card transactions

Along with some of the above methods, real-time monitoring of user activity is also recommended.

3.2.3. CA SB1386

These laws compel organizations to notify the authorities and affected individuals whenever a breach of personal identifiable information (PII) is exposed, such as Social Security numbers, etc. Privacy breach notification laws do not require a specific set of controls, but rather specify what a company must do when a breach is suspected to have occurred. Since notification is expensive both in direct costs as well as indirect damage to reputation, loss of customer trust etc., it is in the company's interest to take measures to protect PII.

3.2.4. HIPAA

The Health Information Portability and Accountability Act is a federal law that was put in place to ensure that the freedom of patients to choose healthcare insurers and providers will not come at the expense of the privacy of their medical records.
The articles relevant to securing database are mainly the following:

- § 164.312(a)(1): Access Control, which requires organizations to "Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights"
- § 164.312(b): Audit Controls, which requires organizations to "Implement hardware, Software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."
- § 164.312(c)(2): Integrity, which requires organizations to "Implement electronic Mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner"

3.2.5. SAS 70

SAS 70 is an auditing standard for the service industry that allows auditors to certify that a service company has the appropriate controls in place to safeguard customer data. This is not a regulation but a standard, and one that gives organizations who adhere to it a badge of quality, which is important in the service industry. Like SOX, SAS 70 does not specify what measures need to be in place, but tools and procedures that facilitate the job of the auditors, and can demonstrate who was doing what in the database can automate this process and save costs.

Below table details the industry regulatory requirements as per its business domain.

3.2.6. Business Domain vs Industry Regulatory Requirements

Compliance / Domain	SOX	FAS	PCI DSS	HIPAA	SB1386	FAD & EPA
Finance	✓	✓	✓			
Billing	✓	✓	✓		✓	
Marketing	✓				✓	✓
Retail	✓			✓	✓	
CRM	✓			✓	✓	
HR				✓	✓	
Health Care				✓	✓	
Manufacturing	✓					✓

Table – 1: Business Domain Verses Compliance Regulatory Practice

3.3. Requirements with upstream data source and feeding systems

As the data flows from various applications and processes, it is required to understand the security requirements during the data movement at various stages. There may be several scenarios where data comes from various data sources and processed in a data warehouse and required data is send another database for reporting etc. So the database architect should gather and outline the requirements of the data and database security from data sources as well as data feeding systems. By implementing these security policies at all the interface layers the data is secured through out its life cycle.

3.4. Security Requirements form Database Support services

There are several database support services which are run in parallel to the database engine, to enhance and simplify the database activities as well as to minimize the database server downtime. These support services such as database mail service, automation of database maintenance activities, data analytical services, High-Availability services, Database Replication etc need to function in sync with the data server. These are either provided by the database vendor or a third party; require certain permissions to access database and its data. Thus the database architect should design the security policy in such a way that these services acquire just the minimum required privileges to function without leaving gaps in the data/database security.

3.5. OS and database Server level Policies

Database architect should understand the organizations security policy in the existing products at the various access layers like Operating System or Database. These may vary as per the nature of the business, so a tailored security policy should be formulated to the current business needs at Operating System and Database layers. These securities requirements at OS and DB layers are to be documented and approvals to be obtained from business and technical stake holders.

3.6. Security Variations

In any organization, the roles and responsibilities of various departments and the duties of its employee's demand variations in security requirements to data and the database. These variations should be captured and well documented so that they can be implemented across the organization uniformly. This gives clear accountability and responsibility to the user who access the data and so the database.

3.7. Database and Data Encryption policy

In a situation where, nature of the business demands data encryption, its data/database and processes encryption policy or methodology should be documented. This data encryption policy can be applied at the server-level or database-level or data-level as per the organization security policy. Such data encryption relies on server certificate which should be obtained from a trusted certificate authority (CA). A certificate authority can be chosen as per the business needs and organizations policy with the approval of the business stake holders and senior management.

3.8. Secure database from Network, Virus Attacks

Any product, which works with critical data, should have protection from various attacks from network or Viruses. This becomes more critical in case of a web based product where the users or attacks can come from any place at any time. So the product should be designed in such a way that it is secured from any possible network or viruses attacks. The possible security breaches or the week links should be identified and a security policy should be formulated to counter any such attacks to secure the data.

3.9. Evaluate Security Requirements

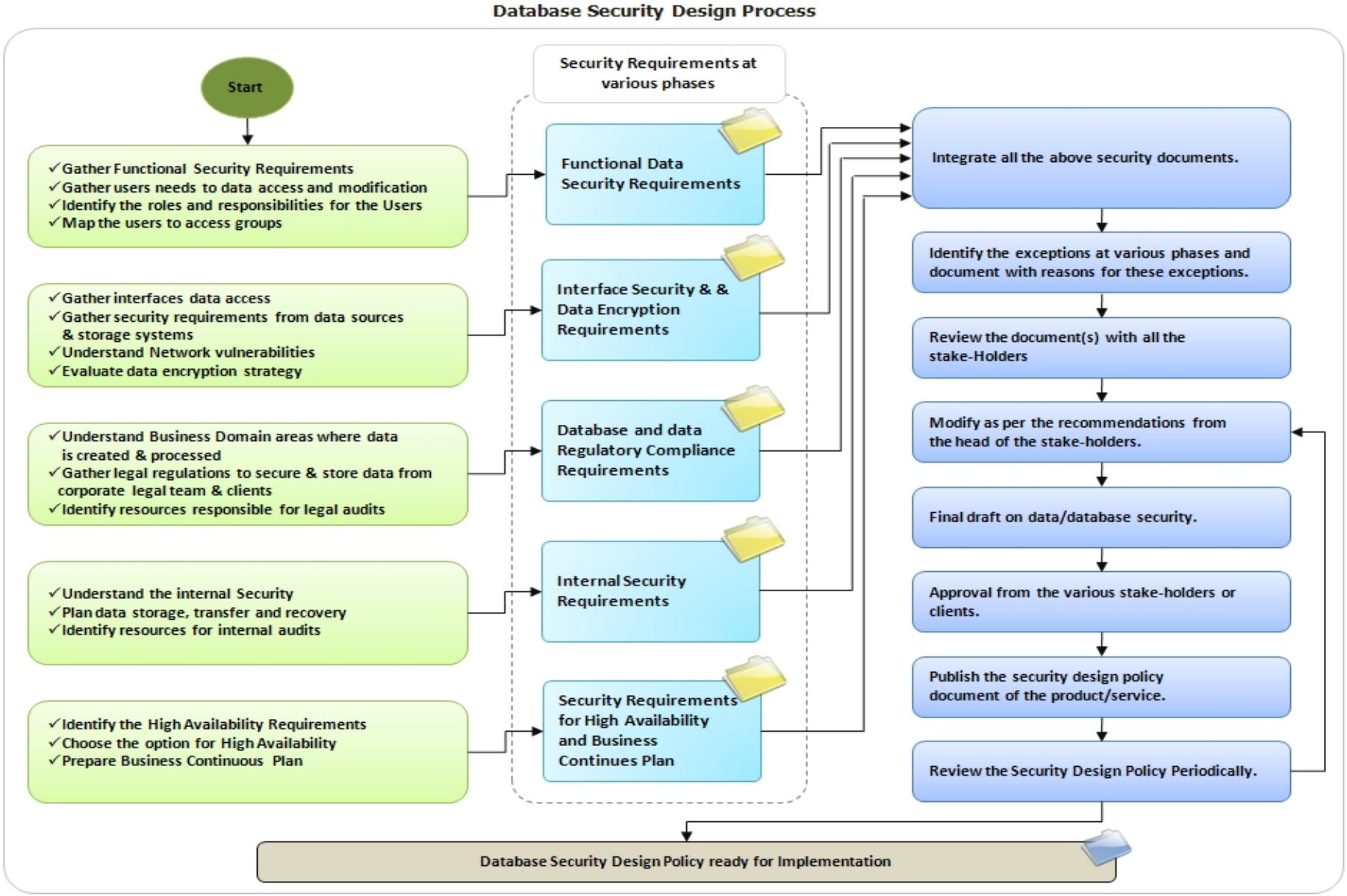
After gathering all the security requirements from various sources, processes and stake holders evaluate these requirements, considering the possible options to meet them. Evaluate the risks associated by implementing the security requirements, keeping in mind the organizations (your & clients) administrative resources.

3.10. Choose Policies and Exceptions

Once the security requirements gathered and evaluated select the security policies and formalize them in a security document. These security policies should include all the consideration to satisfy the security requirements. This document should also specify the security policy exceptions. General guidelines to formalize exceptions:

a) Keep the security exceptions to a minimum.
b) Consider the ramifications of security exceptions.
c) Document all security exceptions
d) Review security policies and exceptions periodically & update as per current situation.

4. Process Chart – 1: Database Security Design Process



5. Conclusions

Design of Database security policy in an enterprise should be documented and is required to be published as an enterprise level standard security practice document. As it is generic document on database security at an enterprise level, it is required to be tailored for any specific database solution which addresses a business problem. Generally these documents are prepared with the coordination of several groups in the enterprise. In general, major stake holders consist of Database Architects, Functional/ Technical Design Architects, Senior Management, Legal Advisers and Business Portfolio Heads and other supporting groups. Also there is a need for the enterprise to make sure these policies are in practice by having regular internal audits and organizing periodic external security audits. These security policies are also to be reviewed on a periodic basis and required to be updated as recommended by the stakeholders as per the business/regulation changes.

6. References

- *Risk Management - Information security: The route to compliance – by Arif Mohamed*
- *Practical Guide to database Security and Compliance from Sentrigo.*
- *Database Security and monitoring tools – DBAudit.*