Розділ 2.
Управління, обробка та захист інформації

UDC 004.056

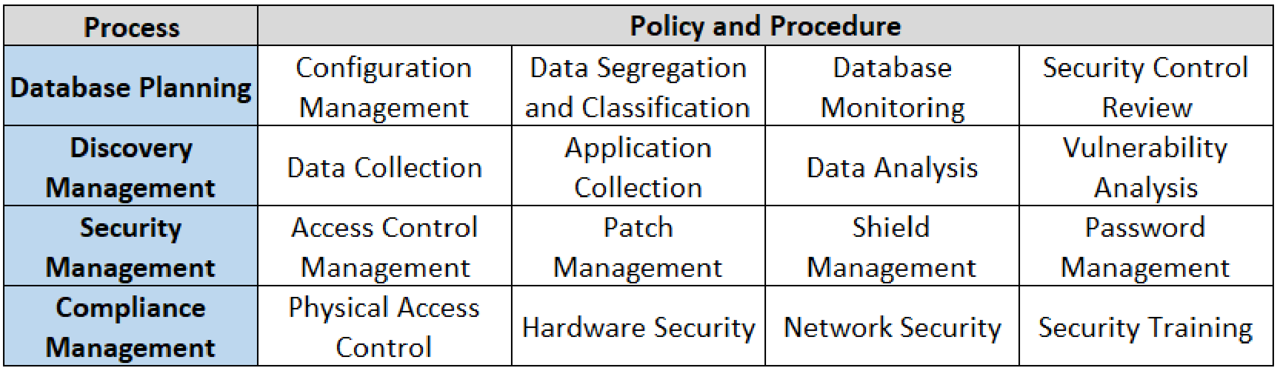
TOWARDS THE ALIGNMENT BETWEEN DATABASE SECURITY FRAMEWORK AND BUSINESS PROCESS MATURITY MODEL

Kopp A.M., Orlovskyi D.L. (kopp93@gmail.com, orlovskyi.dm@gmail.com)
National Technical University “Kharkiv Polytechnic Institute” (Ukraine)

Abstract. *This paper considers the extension and improvement of database security framework by means of its alignment with business process maturity model in order to provide the holistic tool for organizations that are planning to establish a database security system, as well as to assess and ensure its quality using the well-known scale of maturity levels.*

Introduction. Modern applications tend to process large volumes of data, which makes their operations barely impossible without databases as structured collections of related data records, and database management systems (DBMS) as special software used to access and manage such data collections. Just 10-15 years ago databases were used only as components of enterprise information systems and enterprise-level web applications (e.g. e-commerce sites, corporate portals, early social networks etc.). However, these days databases are used in almost any software – from dating or activity tracking applications for smartphones and wearable devices (e.g. smart watches, activity trackers etc.) to e-government services and online healthcare services. It means, today either open public data or private vulnerable data about any person that has at least an e-mail address is kept somewhere in database systems deployed on web hosting servers or cloud services. Therefore, all organizations must ensure database security in order to avoid or at least to minimize the chance of intentional or accidental events occurrence that may threat their or their customers’ data.

Surprisingly the “database security framework” key phrase seems extremely unpopular both in academia resources or just in a Google search results. However, such framework exists and it was proposed by Sharma P. [1] on July 2019. This framework is intended to be adapted by organizations in order to assure the quality of database security system. Moreover, a database security framework is process-centric, since it defines four main processes requires to establish database security system within an organization. Each of considered processes consists of four policies and procedures [1]. In details all of process areas within the Database Security Framework (DSF) are given in [1], whereas below (see Fig. 1) are outlined its four main processes, respective policies and procedures.



Process	Policy and Procedure			
Database Planning	Configuration Management	Data Segregation and Classification	Database Monitoring	Security Control Review
Discovery Management	Data Collection	Application Collection	Data Analysis	Vulnerability Analysis
Security Management	Access Control Management	Patch Management	Shield Management	Password Management
Compliance Management	Physical Access Control	Hardware Security	Network Security	Security Training

Figure 1 – Essential structure of DSF [1]

Considered Database Security Framework [1] is focused on processes that ensure the database security system. The DSF itself does not provide any scale to assess the database security system in a quantitative measurable manner. However, the process management area has the Business Process Maturity Model (BPMM) that can be traced back from the Process Maturity Framework (PMF) and its successor Capability Maturity Model (CMM) [2]. Similarly to the CMM, the BPMM considers five maturity levels (1–5) that represent states of organizational transformation and improvement of its processes [2] (see Table 1).

Table 1 – Maturity levels of BPMM

evel	Name	Description	How to achieve?	Goals
	Initial	Individual efforts with no explicit process or organizational support	Motivate people to overcome problems and just “get the job done”	Planned innovations Change management Capable processes
	Managed	Managers establish a stable work environment in their work unit	Build disciplined work unit management to stabilize work and control commitments	Stable processes Reuse/knowledge management Predictable results
	Standardized	Organization establishes standard processes and assets for performing the product and service work	Develop standard processes, measures, and training for product & service offerings	Productivity growth Effective automation Economy of scale
	Predictable	Work processes are managed quantitatively to establish predictable results	Manage process and results quantitatively and exploit benefits of standardization	Repeatable practices Reduced rework Satisfied commitments
	Innovating	Organization’s processes are continually improved	Implement continuous proactive improvements to achieve business goals	Productivity growth Effective automation Economy of scale

The BPMM scale could be used to quantitatively assess the quality of database security system based on the DSF processes. Thus, this study aims at extension and improvement of the Database Security Framework using its alignment with the Business Process Maturity Model. Research object includes the database security system quality assessment procedure. Research subject includes the alignment between the DSF and BPMM.

Materials and Methods. Quantitative assessment of the database security system is proposed to be based on the BPMM levels 1–5, given to each policy and procedure of each DSF process. This means as the result of quantitative assessment by database security experts we will obtain the 4 × 4 matrix of values in the range 1–5 according to the DSF essential structure shown in Fig. 1. Having $n = 4$ processes and procedures respectively, the quantitative DSF could be represented as a matrix:

$$DSF^{BPMM} = \left(DSF_{ij}^{BPMM}\right)_{i=1,j=1}^{n,n}, DSF_{ij}^{BPMM} \in BPMM_{levles}, i = \overline{1,n}, j = \overline{1,n},$$

where:

– DSF_{ij}^{BPMM} is the maturity level of j-th policy or practice that belongs to i-th process;

– $BPMM_{levles}$ is the set of business process maturity levels, $BPMM_{levles} = \{1,2,3,4,5\}$.

However, there could be a problem when comparing database security systems or evaluations of the same database security system given by different cybersecurity experts. Therefore, in order to compare maturity levels of two or multiple DSF^{BPMM} matrices we can apply multi-criteria decision making methods, such as:

1. Weighted sum model (WSM):

$$DSF_{level}^{BPMM} = \sum_{i=1}^{n} p_i \cdot \left(\sum_{j=1}^{n} w_{ij} \cdot DSF_{ij}^{BPMM}\right),$$

where:

– DSF_{level}^{BPMM} is the maturity level of database security system described by DSF^{BPMM} matrix;

– p_i is the weight of i-th process:

$$\sum_{i=1}^{n} p_i = 1;$$

– w_{ij} is the weight of j-th policy or practice that belongs to i-th process:

$$\sum_{j=1}^{n} w_{ij} = 1, i = \overline{1, n}.$$

When having equal weights (i.e. $w_{11} = w_{12} = \ldots = w_{nn}$ and $p_1 = p_2 = \ldots = p_n$), the WSM is transformed into the average value:

$$DSF_{level}^{BPMM} = \frac{1}{n \cdot n} \cdot \sum_{i=1}^{n} \sum_{j=1}^{n} DSF_{ij}^{BPMM}.$$

2. Weighted product model (WPM):

$$DSF_{level}^{BPMM} = \prod_{i=1}^{n} \left(\prod_{j=1}^{n} \left(DSF_{ij}^{BPMM} \right)^{w_{ij}} \right)^{p_i}.$$

These multi-criteria decision making models (WSM and WPM) can be used to quantitatively assess maturity of database security systems with respect to both DSF and BPMM.

Results and Discussion. As the result of this paper, we would like to suggest an extension of original DSF – Quantitative Database Security Framework (QDSF) based on both DSF and BPMM, as well as on considered multi-criteria decision making models (WSM when compensation of weak values by strong ones is acceptable or WPM otherwise). The calculation model is shown in Fig. 2.

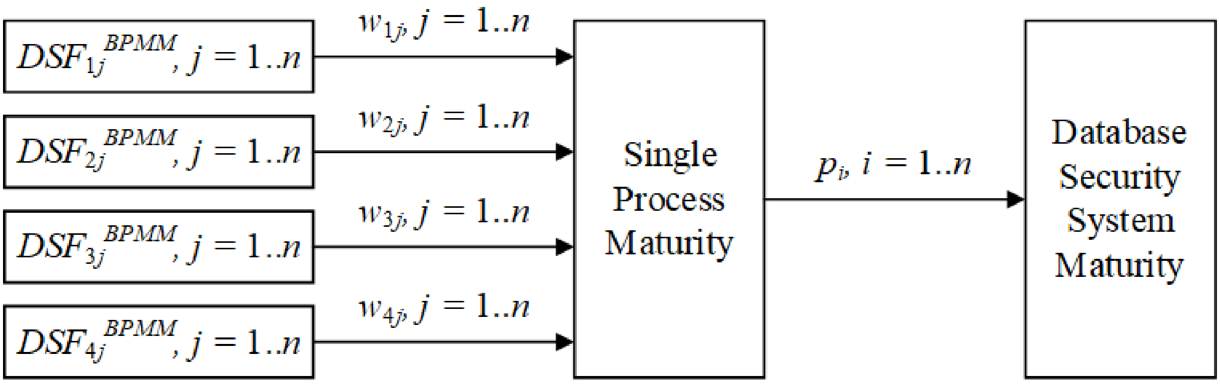

$DSF_{1j}^{BPMM}, j = 1..n$
$DSF_{2j}^{BPMM}, j = 1..n$
$DSF_{3j}^{BPMM}, j = 1..n$
$DSF_{4j}^{BPMM}, j = 1..n$
$w_{1j}, j = 1..n$
$w_{2j}, j = 1..n$
$w_{3j}, j = 1..n$
$w_{4j}, j = 1..n$
Single Process Maturity
$p_i, i = 1..n$
Database Security System Maturity

Figure 2 – QDSF calculation model

On practice each policy and procedure could be given with the required rank in the 1–5 range, so the weights w_{ij} then will be calculated as:

$$w_{ij} = r_{ij} \Big/ \sum_{j=1}^{n} r_{ij}, i = \overline{1, n}, p_i = r_i^p \Big/ \sum_{i=1}^{n} r_i^p,$$

where:

– r_{ij} is the rank of j-th policy and procedure that belongs to i-th process (given in 1–5 range);

– r_i^p is the rank of i-th process (given in 1–5 range).

Conclusion. In this study we considered the extension and improvement of database security framework, the QDSF. It was proposed as the result of alignment between DSF and BPMM in order to provide the holistic tool for organizations willing to establish a database security system, as well as to assess and ensure its quality using the well-known scale of maturity levels. Now assessment is implemented by the quantitative model (Fig. 2) and respective decision making approaches (WSM or WPM). Further study should consider usage of WPM to support rigorous cybersecurity policies.

References.

[1] Database Security Framework & Best Practices, https://www.cisoplatform.com/profiles/ blogs/database-security-framework-best-practices-for-cisos [Accessed: September 8, 2021]

[2] Business Process Maturity Model (BPMM), https://www.omg.org/spec/BPMM/1.0/PDF [Accessed: September 8, 2021]

UDC 021:004.9

MANAGEMENT, PROCESSING AND PROTECTION OF INFORMATION IN DIGITAL LIBRARIES

Ruzieva M.B. (maftu0425gmail.com)
Tashkent University of Information Technologies (Uzbekistan)

Technological advances have led to a proliferation of digital libraries over the past decade or so. These offer valuable opportunities for convenient access to information and data, regardless of an individual's location. For librarians though, the transition from physical to digital library collections brings many new challenges, not least in the areas of security and privacy. The purpose of this article is to examine the nature of these challenges and the opportunities available for overcoming them, so that libraries can continue to fulfill their important role of providing accurate, secure and timely information to users, while protecting their privacy and the confidentiality of their personal information. The article addresses in particular the following issues: protecting the information infrastructure; identification and authentication in security and privacy; standards and policies;access and control of digital information; ethical decision-making in design, implementation and evaluation of digital libraries; and privacy, anonymity and identity.

There has been a vast increase globally over the past decade or so in digital libraries, facilitated by technological advances and driven by consumer demand for easy and convenient access to knowledge and information from any location. According to Ershova and Hohlov the digital library as ”a distributed information systems ensuring reliable storage and effective use of heterogeneous collections of electronic documents- text, graphics, audio, video,etc. In brief, digital libraries are organizations that hold information resources in digital format. However, while bringing benefits to patrons and new opportunities for library

Professionals to expand their roles, the developments have also brought about new problems and challenges, especially relating to information security and user privacy. Society has been increasingly dependent on information technology (IT) for several years now. In this Information Age, millions of users (or participants) access and exchange billions of objects of information content in complex work flow processes (e.g., commerce, learning, health care). The research community uses computer systems to perform research and to disseminate findings.

Information sharing has been made easier and less expensive by Internet technologies and global networking infrastructures, but availability of such information systems comes at the expenses of higher risks. In the long run, information is not preserved, websites tend to disappear frequently and digital media become obsolete easily and there can be an abuse in the privacy of information. Moreover, the integrity of the systems could be compromised. Access control is often described as rules regulating how participants are allowed to access object and could also be viewed as information flow control because every access results in flow of information between entities.

Emerging digital technology has paved the way for the creation of digital libraries, which have made it easier for users to access information through digital systems and networks. The digital library is generally designed to perform and serve the same primary functions and tasks as a traditional library. libraries include developing and producing information records in print and non-print formats, managing these information records, and distributing information for the use of