COBIT 5: Information Security to the Enterprise Environment...

Dr.Mundhe S.D.
Director-MCA
Sinhgad Institute of Management and Computer Application(SIMCA),
drshivaji.mundhe@gmail.com

Prof.Hiremath C.M.
Assitant Professor
Sinhgad Institute of Business Management, kamlapur
Chandrashekhar67@gmail.com

ABSTRACT- ***This paper is an review of COBIT 5`s Introduction, Benefits, COBIT 5 Principles, Policies and Frameworks. The research paper provides guidance to help IT and Security professionals to understand, utilize, implement and direct important information security related activities and make more informed decisions. The paper begins by describing a set of Mechanisms and policies for computing, and examining the impact of these threats on the Information system.***
Next, it summarizes the key Policies that the organization has to adopt for the better performance. Finally, it describes the research opportunities in improving the information security.

In 21st century the world is moving towards the vision 20-20.Every area is growing with rapid speed. Every organization is improving its quality by making computerization in every department. But Today's businesses are facing the biggest threats from many introducers by number of unethical things that they do in. So plenty of Security models, developed for many organizations, differ in many aspects because they focus on different features of the Information security problem or because they make different assumptions about what constitutes a secure data security. This leads to disjointed and incomplete understanding of the organizational security strategy. This makes it difficult to reconcile different security requirements

Keywords: introducers, TOGAF [The Open Group Architecture Framework (TOGAF) is a framework for enterprise architecture which provides an approach for designing, planning, implementing, and governing an enterprise information technology architecture], ITIL Information Technology Infrastructure Library (ITIL) , Information Systems Audit and Control Association (ISACA)access, corporate, legislation, security, malevolent.

I. INTRODUCTION

The Information Systems Audit and Control Association first released COBIT in 1996; ISACA published the current version, COBIT 5, in 2012.COBIT aims "to research, develop, publish and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers, IT professionals and assurance professionals".[1]

COBIT, initially an acronym for "Control objectives for information and related technology" (though before the release of the framework people talked of "CobiT" as "Control Objectives for IT"), defines a set of generic processes for the management of IT. The framework defines each process together with process inputs and outputs, key process-activities, process objectives, performance measures and an elementary maturity model.

The framework supports governance of IT by defining and aligning business goals with IT goals and IT processes.COBIT provides a set of recommended best practices for governance and control process of information systems and technology with the essence of aligning IT with business. COBIT 5 consolidates COBIT4.1, Val IT and Risk IT into a single framework acting as an enterprise framework aligned and interoperable with TOGAF and ITIL

COBIT 5 for Information Security is a major strategic evolution of COBIT 5—the only business framework for the governance and management of enterprise IT. This evolutionary version incorporates the latest thinking in enterprise governance and management techniques, and provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems. Information is a key resource for all enterprises and, from the time information is created to the moment it is destroyed ,technology plays a significant role. Technology is increasingly advanced and has become pervasive in enterprises and the social, public and business environments. COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT. Simply stated, it helps enterprises create optimal value from information technology (IT) by maintaining a balance between realising benefits and optimising risk levels and resource use. COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking into account the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders.[2]

For those that are new to IT management and compliance, COBIT is the business framework for enterprise IT management and governance created by the standards body ISACA. Just about everyone in the group said COBIT was extremely important. But there's recently been a new release of COBIT (COBIT 5), and most of the people I asked didn't seem to know what it means for their organizations. I believe COBIT is going to be increasingly important to IT organizations in the future – we already see it playing an important role in European financial institutions trying weather what has been called financial contagion. For them and you with COBIT 5 you can:

- Mitigate organizational risk for IT and business as a whole
- Strengthen security
- Ease your auditing and compliance burden
- Reduce cost while improving the consistency of IT delivery

For these reasons, I've decided to write a blog series to discuss what COBIT 5 asks for in terms of IT measurement and management. My goal is to provide an overview and then over successive weeks to dig into specifics. Please feel free to ask questions during our collective journey.

II. WHY YOU SHOULD CARE ABOUT COBIT 5

COBIT 5 is on its way to becoming an overarching IT standard even though it had its origins nearly 20 years ago as basis for auditing IT management. With the passage of Sarbanes-Oxley in 2002, COBIT

got some teeth, especially for financial institutions. And if you were going to be compliant with SOX, you needed to have COBIT ingrained in your organizational DNA.

With COBIT 5, the standard takes a major leap. This isn't just a refresh. COBIT 5 adds a governance layer. This means that COBIT 5 organizations aren't just compliant – they're reaping the benefits of good IT governance, like running more efficiently and effectively. So IT now has a comprehensive framework that assists it in achieving the business's objectives for the governance and management of enterprise IT. What's more, it puts enterprise and IT scorecards front and center.

How COBIT 5 ties to the Balanced Scorecard

The new release gives sample scorecards – one for the enterprise and one for IT – and shows the linkages between them. Not only that, it shows how to translate high-level enterprise goals into manageable, specific IT-related goals and then map these to specific processes and practices.

COBIT 5 defines a set of enterprise-related goals in balanced scorecard format and then cascades them in turn to IT-related goals also in balanced scorecard format. Each scorecard has 4 goal quadrants—financial, customer, internal, and learn and grow. This includes what they call a goal cascade allowing for defining priorities and responsibilities for improvement. They use a similar methodology to the HP Executive Scorecard although with slightly differently naming. Regardless of what performance system you use, you'll want to have a way to relate KPIs and metrics to the COBIT scorecards.

Over the next few weeks, I'll look at COBIT 5's enterprise scorecard and where IT fits. Next, I'll do the same for the IT goals scorecard. This includes the specific metrics that relate to each. I'll then relate these to data that existing systems produce and HP Executive Scorecard uses to create KPIs and metrics. If you walk away with anything today, let it be that COBIT 5 is going to affect how manage your organization and show your progress at control and improvement. It is here to stay, and this is the time to learn how it will affect you.

COBIT 5 for Information Security, highlighted in figure 1, builds on the COBIT 5 framework in that it focusses on
information security and provides more detailed and more practical guidance for information security professionals and
other interested parties at all levels of the enterprise.

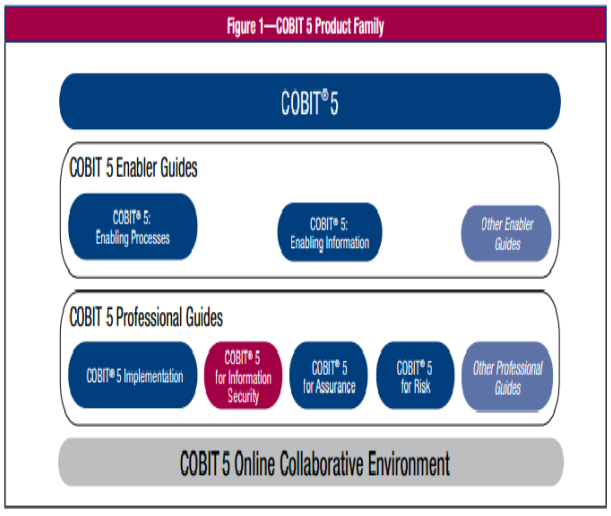


Figure 1—COBIT 5 Product Family

III. MOST VALUABLE DRIVERS FOR COBIT5

In COBIT 5, the processes APO13 Manage security, DSS04 Manage continuity and DSS05 Manage security services provide basic guidance on how to define, operate and monitor a system for general security management. However, the assumption made in this publication is that information security is pervasive throughout the entire enterprise, with information security aspects in every activity and process performed. Therefore, COBIT 5 for Information Security
provides the next generation of ISACA's guidance on the enterprise governance and management of information security[3].

COBIT 5 is based on five key principles for governance and management of enterprise IT:

Principle 1: Meeting Stakeholder Needs
Principle 2: Covering the Enterprise End-to-End
Principle 3: Applying a Single, Integrated Framework
Principle 4: Enabling a Holistic Approach
Principle 5: Separating Governance From Management

The COBIT framework classifies IT activities and risks into four domains:[4]

- Plan and Organize (PO)-Provides direction to solution delivery (AI) and service delivery (DS)
- Acquire and Implement (AI)-Provides the solutions and passes them to be turned into services
- Deliver and Support (DS)-Receives the solutions and makes them usable for end users
- Monitor and Evaluate (ME)- Monitors all processes to ensure that the direction provided is followed

COBIT identifies 34 processes within these four domains. It defines activities and control objectives for all 34 processes, as well as overarching process and application controls. Controls are designed to support seven information criteria:

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

COBIT also includes an IT Governance Maturity Model

IV. BENEFITS COBIT5

Using COBIT 5 for Information Security brings a number of information security-related capabilities to the enterprise, which can result in a number of enterprise benefits such as:

- Reduced complexity and increased cost-effectiveness due to improved and easier integration of information security standards, good practices and/or sector-specific guidelines
- Increased user satisfaction with information security arrangements and outcomes
- Improved integration of information security in the enterprise
- Informed risk decisions and risk awareness
- Improved prevention, detection and recovery
- Reduced (impact of) information security incidents
- Enhanced support for innovation and competitiveness
- Improved management of costs related to the information security function

- Better understanding of information security

COBIT 5 for Information Security helps enterprises:

Bring Order to Complex Standards and Frameworks:-COBIT 5 for Information Security leverages the COBIT 5 framework—the globally accepted information and technology management and governance framework— through a security lens. It is the only security framework that integrates other major frameworks and standards.

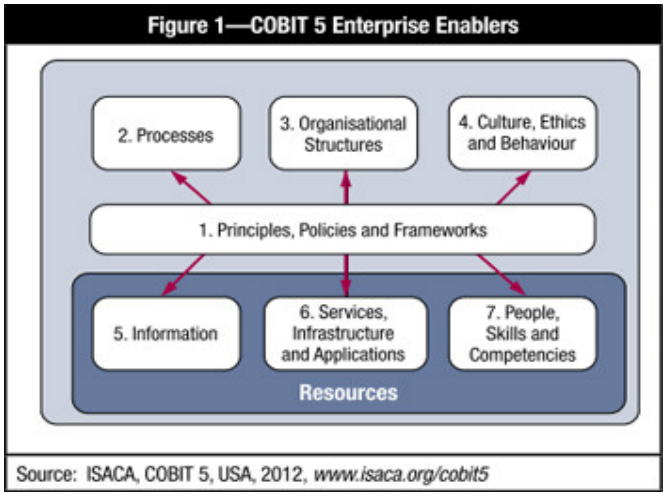
Extract Value from Information Chaos:-COBIT 5 for Information Security provides the most complete, up-to-date guidance on information security that incorporates COBIT 5 as well as aspects of globally accepted standards and practices. It provides users the knowledge and guidance to increase trust in, and value from, information systems throughout your enterprise.

Address all Stakeholders Needs and Maximize Value of Corporate Information:-COBIT 5 for Information Security has a complete, consistent and easily navigable structure that promotes access to information, functionality and user satisfaction. Regardless of geographical location, it provides users with the foundational tools to protect information.

Protect and Drive Enterprise Value:-COBIT 5 for Information Security provides guidance and an end-to-end security view of COBIT 5 to help enterprises manage risk and ensure compliance, continuity, availability, security and privacy. This framework supports IT assets and business goals to help ensure that information systems comply with necessary risk controls.

IT Policy Framework Based on COBIT 5

Creating IT policies in a changing environment is not a straightforward task but often a necessary one. Organizations might not fully appreciate advantages, limitations and risk factors of emerging technologies; for instance, choosing a cloud computing solution requires management of the associated risk and empowerment for a route to create business value in an environment full of uncertainties.[6]
IT policies are not an IT-only activity. Incorporating IT principles with end-to-end business processes ensures better coverage and cooperation across the enterprise (i.e., responsibilities and authorities are clearly defined), reduces duplication of controls across different teams, and provides a consistent approach to address business requirements.



Policies as Enablers

COBIT 5 introduces seven enablers (see **figure 1**) as support tools for the implementation of GEIT.5 The four dimensions (stakeholders, goals, life cycle and best practices) of the enabler Principles, Policies and Frameworks are discussed in the following sections and suggestions for a systematic method of designing and implementing a policy framework are provided.

COBIT 5 ensures that a policy framework meets stakeholders' needs, covers the end-to-end process (and not only the IT function), and establishes the additional documentation required to ensure that governance and management goals and activities are achieved.

Stakeholders Dimension
There are stakeholders who define and set policy principles, and there are others who follow, adhere to or implement such principles.

The first group of stakeholders defines and sets policy principles, taking into consideration general organizational governance principles and analyzing and identifying internal and external factors (e.g. regulation), business direction, and organizational culture. The organization's board of directors and executive management belong to this group. They are, in addition, accountable for giving direction about, communicating on and implementing governance objectives, and for defining the core components of a policy framework.

The core components of a policy framework are:

- Appointment of individuals who have the authority to approve policies and their associated responsibilities
- Determination of the consequences for failing to comply with given policies
- Definition of a process for handling exceptions to policies
- Definition of a method for measuring and monitoring compliance with policies
- Definition of the scope of the policy and the group of stakeholders that has to follow the policy

V. CONCLUSION

As far as today`s world concern the Computer security is a serious and ongoing issue which requires your constant observation. Don't let your guard down or you could end up being a victim. Continuous innovation and research in the field of computer security can make success.
It is difficult to secure of the information technology without innovations and powerful secure interference. The COBIT 5 will be one of the solution for your organization.

VI. REFERENCES:

1 http://en.wikipedia.org/wiki/COBIT
2.http://www.enterprisecioforum.com/en/blogs/mylessuer/4-reasons-cobit-5-should-be-part-your-it
3. http://searchsecurity.techtarget.com/definition/COBIT]
4. http://www.sox-online.com/cobit.html
5.http://www.isaca.org/Journal/Past-Issues/2013/Volume-1/Pages/IT-Policy-Framework-Based-on-COBIT-5.aspx]