Proceedings of the 2014 Federated Conference on
Computer Science and Information Systems pp. 901–910

DOI: 10.15439/2014F77
ACSIS, Vol. 2

A Comparison between Business Process Management and Information Security Management

Gaute Wangen
Norwegian Information Security Laboratory
Gjovik University College
Teknologiveien 22, 2802 Gjovik, Norway
Email: gaute.wangen2@hig.no

Einar Arthur Snekkenes
Norwegian Information Security Laboratory
Gjovik University College
Teknologiveien 22, 2802 Gjovik, Norway
Email: einar.snekkenes@hig.no

***Abstract*—Information Security Standards such as NIST SP 800-39 and ISO/IEC 27005:2011 are turning their scope towards business process security. And rightly so, as introducing an information security control into a business-processing environment is likely to affect business process flow, while redesigning a business process will most certainly have security implications. Hence, in this paper, we investigate the similarities and differences between Business Process Management (BPM) and Information Security Management (ISM), and explore the obstacles and opportunities for integrating the two concepts. We compare three levels of abstraction common for both approaches; top-level implementation strategies, organizational risk views & associated tasks, and domains. With some minor differences, the comparisons shows that there is a strong similarity in the implementation strategies, organizational views and tasks of both methods. The domain comparison shows that ISM maps to the BPM domains; however, some of the BPM domains have only limited support in ISM.**

Keywords: Information Security, Information Security Risk Management, Business Process Management, BPM Methodology Framework, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, NIST SP 800-39

I. Introduction

INFORMATION technology and systems play a crucial role by supporting the organization in achieving its goals and objectives. The main goal of information security (IS) is to secure the business against threats and ensure success in daily operations, and aid the businesses in reaching the desired level of reliability and productivity through ensuring integrity, availability and confidentiality [1]. We define the main profit of IS risk management (ISRM) as maximizing long term profit in the prescence of faults, conflicting incentives and active adversaries.

Business Process management (BPM) is a discipline that combines knowledge from information technology and management sciences and centers on business processes [2]. It is used to represent business processes (BP) for analysis and improvement purposes [3], [4]. The main goals of BPM is to align the organization's business processes to the organization's mission, goals and objectives and improve efficiency to create a competitive advantage [3], [5].

Some of the existing information security frameworks mention risk management (RM) of business processes in some form, e.g. ISO/IEC 27005:2011 defines BPs as a primary asset [6], and NIST SP 800-39 suggests RM of Mission/Business Process as tier 2 in the multi tier organization-wide risk management model [7]. While the purpose of both IS management (ISM) and BPM is similar, to map and improve organizational performance in their own way, they remain two different disciplines that require two different sets of skill.

In this paper, we investigate the similarities and differences between BPM and ISM, and explore the obstacles and opportunities for integrating the concepts of ISM and BPM. The BPM methodology framework [8] by BPTrends as described by Harmon [5] and Mahal [3] represents the main sources used to describe BPM, and we use the ISO/IEC 27000-series [6], [9], [10] and NIST SP 800-39 [7] to describe ISM.

A. Problem Description

While it can be said that the scope of ISM is turning towards BPs security, BPM and ISM remain two different disciplines and are most of the time regarded as separate activities [11]. However, the disciplines mutually affect each other's objectives, e.g. re-engineering a BP will often have security implications, and introducing an information security control is likely to affect the BP flow. In addition, the impact of a materialized security risk will usually affect the business. A different set of skills is required to risk manage a BP than an IT-system; one requires knowledge of BPM methods, and the other technical insight in information security. In addition, there exists several types of BPs, ranging in abstraction level, from value chain at the very top of the organization, to work instruction & procedures [3], [5], see Fig. 1. People employed at different levels of the organization, perceive and worry about different risks [12], and focus on a variety of different goals in their work efforts [5]. The difference in abstraction makes it likely that one ISRM approach designed for a low level BP is not likely to be applicable for risk managing the higher abstractions, such as value chain or core processes. Hence, there is a need to make sure that IS and BPM activities are aligned. Very little has been published in terms of investigations regarding to what extent IS and BPM guidelines and methods are well aligned, overlapping or in conflict. The aim of this paper is to contribute towards the filling this gap.

The remainder of this paper is structured as follows; In Sect. II, we present related work. In Sections III & IV we

978-83-60810-58-3/$25.00 © 2014, IEEE

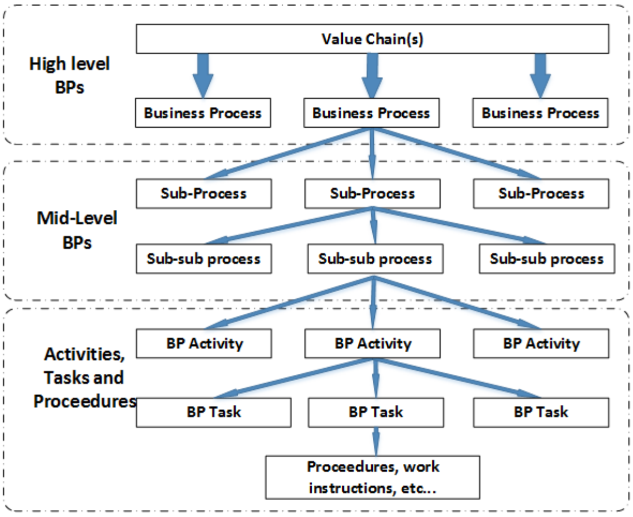

Fig. 1. Example of a Business Process Hierarchy.

introduce relevant IS and BPM concepts used in this article. Sect. V introduces the research method. Sections VI, VII & VIII presents comparisons of ISM and BPM and discussions of findings. The three areas of comparisons are Lifecycles, Organizational Views & corresponding tasks, and Domains. Conclusion and Future Work are given in Sect. IX.

II. Related Work

Much of the published research within combination of BPM and ISM focus on risk analysis of BPs; Milanovic et. al. [13] presents a framework for modeling BP availability. The framework takes into account services, the underlying ICT-infrastructure and people, and has a special focus on dependencies between these layers. Jallow et.al. [14] present a framework for risk analyzing BPs, using modeling activities and Monte Carlo analysis for calculating risks and forecasts. Asnar and Massacci [15] takes the GRC management approach to information security, and presents a method for analyzing and designing security controls in an organizational setting using BPs. Zoet et.al. [16] introduces the different kinds of risk that affect a BP and establishes the relationship between operational risk, compliance risk, internal controls and business processes. Zoet et.al. also present an integrated framework for dealing with RM and compliance from a BP perspective. Taubenberger and Jurens [17] suggest to improve security processes by using BP models to move away from probabilities.

There also exists approaches for risk managing BPs; In 2000, Kokolakis et.al. [18] presented a paper discussing the use of BPM for IS. The authors argue that the asset-based approach of ISRM treats IS as an add-on feature aiming to minimize the overhead cost. The authors suggests that the combination of BPM and IS-SAD (information security analysis and design) techniques can be used for security re-engineering of a BP, and integration of IS. The authors presents an overview of existing BPM approaches and requirements they should support to be used in ISRM.

Jakoubi and Tjoa [11] introduce a reference model for considering information within the BPM and RM domains. The authors argue for a stronger interweaving between RM and BPM, and present an approach for reengineering business processes as risk-aware. Herrmann and Herrmann [19] introduces the MoSS BP (Modeling Security Semantics of Business Processes) frame, based on object-oriented process models. The authors introduce several security properties and correlations between security requirements and BP elements, together with the following general approach to risk managing business processes, the three first steps focus on identificaiton of: (i) Business Processes and their actors. (ii) And valuation of assets and their security levels. (iii) Security requirements - and responding vulnerabilities and threats. While the two last steps address risk analysis and treatment: (iv) Assessment of risk. (v) Proposal, design and implementation of countermeasures.

AURUM [20] supports the NIST SP 800-30 standard [21], and is a framework for addressing IT risks which utilizes business processes for RM. AURUM prioritizes BPs based on importance, and derives the important assets from the BP. The method then continues to determine asset importance and conducts risk analysis based on Bayesian threat networks.

Ozkan and Karabacak [22] suggests that process modeling can be used to ease the use of risk analysis methods and move the IS focus from hardware and software over to IT processes. The authors suggests using process modeling to model the activities of the information processing and to determine the scope of the risk analysis. The CERT Resilience Management Model v 1.0 [23] (CERT RMM) is an approach for handling the challenge of operational resilience in day to day operations. The notion is that organizations deliver services that are supported by BPs' which are further supported by assets.

III. IT Governance, Information Security Risk & Management

Gregory [24] state that *"The purpose of IT governance is to align the IT-organization with the needs of the business"*. IT governance involves a series of activities to achieve this goal such as creating IT-policy, internal prioritizing between e.g. mission, objectives and goals, program and project management [24]. It also includes the responsibility for managing risks appropriately, and verifying that resources are used responsibly [7].

A. Information Security Management (ISM)

Generally, the main goal of information security is to secure the business against threats and ensure success in daily operations by ensuring confidentiality, integrity, availability (CIA) and non-repudiation [1]. Information can be present in many forms within the organization, it may be stored on a physical medium, be in the form of paper, or it can be an employee's knowledge and experience. Common for all these is that they are all valuable assets to an organization and their security needs assurance. One of the main components of ISM is to establish a security program, often referred to as an information security management system (ISMS). The ISMS is a collection of security related documents often with the company wide security policy as the main document. The purpose of the ISMS is to ensure CIA through management of the organization; by choosing and implementing the appropriate security measures and controls. These measures can be chosen from e.g. the ISO/IEC 27002 [10], which is a standard consisting of security measures and how to implement them. The ISMS can be implemented following a Plan-Do-Check-Act (PDCA) cycle of continuous improvement [1], [6], see Fig. 2.

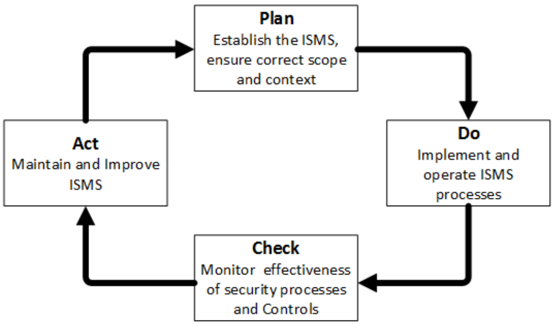
Plan
Establish the ISMS, ensure correct scope and context
Do
Implement and operate ISMS processes
Check
Monitor effectiveness of security processes and Controls
Act
Maintain and Improve ISMS

Fig. 2. Plan Do Check Act-phases of ISMS implementation as described in ISO/IEC 27000:2009 [1].

The security documentation of the ISMS is represented by a top-level security policy, generally founded in the organization's mission, vision, goals, values and objectives. Further represented by topic/issue-specific policies, standards, procedures and routines.

B. Information Security Risk Management (ISRM)

There exists several definitions of risk, ISO/IEC 31000:2009 [25] standard explains risk as *the effect of uncertainty on objectives*, and *Risk management* as a set of activities and methods applied in an organization to manage and control the many risks that can affect achievement of business goals. Hence, the main goal of ISRM is to maximize the long term profit, and optimally manage risks presented by potential failures, conflicting incentives and active adversaries.

A risk assessment is the *overall process of risk analysis and risk evaluation* [1], and risk analysis (RA) is the *systematic use of information to identify sources to estimate the risk* [1]. Risk evaluation is the *"process of comparing the estimated risk against given risk criteria to determine the significance of the risk"* [1].

ISO/IEC 27005:2011 [6] is a standard specialized for ISRM and defines the formal process of managing risks as an iterative process of reviewing and monitoring risks, including: context establishment, risk assessment, communication and treatment to obtain risk acceptance [6]. Risks for information systems are generally analyzed by using a probabilistic risk analysis (PRA) [6], [21], where impact to the organization (e.g. loss if a risk occurred) and the probability of the risk occurring is calculated. Probability calculation in ISRM has previously recieved critisism for relying too much on subjective estimates, and being too much like guesswork [24], [26], [27]. Risk evaluation uses the results from the analysis, and if the risk is found unacceptable, risk treatments are implemented, which consists of choosing a strategy and measures for controlling undesirable events.

C. Context Establishment for ISRM

The term "Context Establishment" is from the ISO/IEC Risk Management standard 27005 [6], and defines both the external and the internal parameters that must be considered when managing risks. The internal context for ISRM will usually be a product of different factors, such as IT systems, stakeholders, governance, contractual relationships, culture, capabilities, business objectives, and others. Examples of relevant external factors for establishing context are external stakeholders, external environment, laws and regulations, and other factors that can affect the organizations objectives.

Many established ISRM methods center around assets, the *NIST Specification for Asset identification* [28] uses three main classes of information system related assets; (i) Persons, (ii) Organization, and (iii) Information Technology. In addition, it provides nine sub-classes of assets of Information technology. In contrast to this, ISO/IEC 27005:2011 uses two primary asset classes; (i)Business processes & activities" and (ii)Information, with supporting assets: (i) Hardware, (ii) Software, (iii) Network, (iv) Personell, (v) site, and (vi) organization's structure.

A control can exist as automatic or manual, an automatic control performs its function with little or no human interaction, and a manual control requires a human to operate it, and generally fall within three major categories [24]: (i) Physical - represents controls that are found in the physical world, such as fences, doors with locks, and laptop wires. (ii) Technical - represents controls that are implemented in the form of information systems, they are usually in a logical form, such as a firewall, antimalware, and computer access control. (iii) Administrative - represents controls in form of e.g. policies and procedures that forbid certain activities, such as the IS policy.

The 14 Control Clauses and security domains from ISO/IEC 27002:2011 [10] and ISO/IEC 27001:2013 [9] are:

1) Information Security Policy - Top level documented security objectives for the whole organization, determined by management.
2) Organization of Information Security - IS Roles and Responsibilities, and IS management in general.
3) Human Resources Security - IS requirements and controls for recruitment of staff, terms of employment, security awareness training and process for termination.
4) Asset Management - The management and application of hardware and software assets, and classifying and handling of information.

5) Access Control - Effective password, privilege and user management on operating systems, applications and within networks.
6) Cryptography - Controls for securing CIA of information using encryption.
7) Physical and Environmental Security - Securing the human and system environment, including entry controls, power and cabling security.
8) Operations Security - Ensure CIA of operations and facilities.
9) Communications Security - Key security aspects of managing systems securely, such as backups, antivirus, media and laptop security
10) System Acquisition, Development and Maintenance - Secure development of software and maintenance of systems to maintain ongoing security
11) Supplier Relationships - Protect the organization from security breaches caused by third parties.
12) Information Security Incident Management - The reporting, recording, management and review of security incidents.
13) Information security Aspects of Business Continuity Management - Determine requirements, plan and training for response in the event of disasters.
14) Compliance - Ensuring compliance with legal requirements, including IPR, computer misuse and privacy legislation.

IV. Business Process Modelling and Management

A business process (BP) is a set of activities within an organization whose objective is to produce a desired result [29]. A process is, in short, "How work gets done" [3], and work is the *"exertion of effort directed to produce or accomplish something"* [4]. The purpose of modeling a BP is to describe the logical order and dependence, such that the practitioners can achieve a comprehensive understanding of the process [29]. A process generally has some sort input and transforms this into an output, e.g. a manufacturing process will take raw material as input, process this material, and output a product. We borrow the explanation from Mahal [3]:"a process is triggered by an event, governed by some rules using relevant knowledge, and executed through people using enabling technology and supporting infrastructure, such as facilities". A common abbreviation used to describe the components of a BP is IGOE - Inputs, guides, outputs and enablers [3], [5].

Besides from documenting processes, BPM can be used to facilitate large scale software developments to support BPs, BP analysis and improvement re-engineering [29]. The top-level representation of the BPM approach seen in Fig. 3.

A. The BPM Lifecycle

The BPM lifecycle represent the key activities in BPM. There is no uniform view of the number of BPM-LC phases [30]. Ko [31] state that there are many views of what steps the BPM life cycle actually consists of, and presents van der Aalst et.al.'s (2003) [32] view due to succinctness and relevance. Van der Aalst (2013) [2] has also published a newer review of the key activities in BPM after [31] was published. Wetzstein et.al. [30] present a general version of the BPM-LC. An analysis of the different lifecycle steps from [2], [30], [32], [33] show that they have the following steps in common:

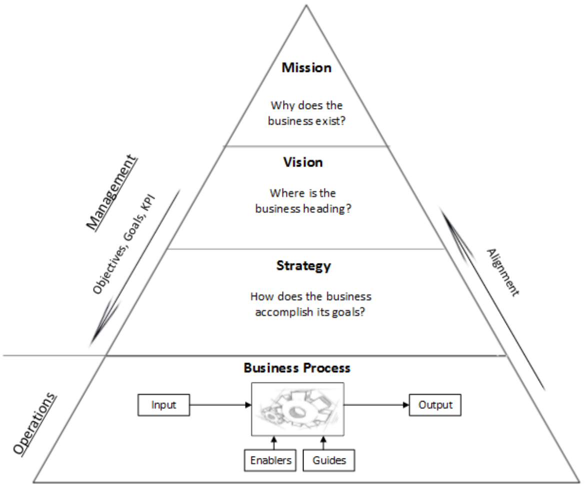

Fig. 3. Connection between Mission, Vision, Strategy and Business Processes. *Based on Mahal [3]*

1) Modeling and Design - Map/re-design or create a process model for analysis and/or enactment.
2) System Configuration & Implementation - Configure the system and implement the process model for enactment.
3) Enact/Execution - Deploy and execute the BP model using set configuration control and support concrete cases.
4) Monitor/Analyze - Analyze a process model studying the BP and/or event logs.
5) Manage/Diagnosis - Adjust/improve process, reallocate resources, manage large collections of BP models.

B. BPTrends Associates' BPM Methodology

The BPM Methodology Framework [8] is a best practices framework that provides a view of BPM sorted into three levels with associated steps. The framework recognizes the variety of goals at the different levels of the organization. The framework sorts the different levels into enterprise, process and implementation levels. The *Enterprise* level centers on corporate strategy, and focus on understanding and modeling BP architecture, definig performance measures, governance systems, aligning enterprise capabilities and prioritizing efforts. The main ongoing task consist of managing enterprise processes.

The *Process* level runs process improvement projects, where modeling, redesign and improvement of existing processes is in focus, taking processes from AS-IS to TO-BE. The main day-to-day tasks are BP execution and management.

The *Implementation* level focuses on designing human, software and information systems to implement BPs. It consists of various IT and HR methodologies that are used for maintaining resources and continuous improvement.

C. BP Domains

Fig. 4 illustrates the BP domains, and shows how the different aspects of business support the BP, which ultimately determines enterprise performance. The general purpose of a BP is to transform an input to a desired output. The enterprise delivers value to its stakeholders and customers, and enterprise performance can be described using a set of measurable goals and objectives. KPIs provide the mechanisms for measuring performance. Information, knowledge and insight is what fuels the BP. The BP execution transforms the information into knowledge which is applied to create solutions. The "Guides" manages and controls the input/output transformation [3]. Put in the information security language; Guides are generally about governance and controls. The "Enablers" are the reusable resources of an organization that support the BP in transformation of input to output [3]. We leave inputs and outputs out of scope in this comparison. An explanation of the BP domains in the hexagon is as follows [3]: *Guides* provide governance, stakeholder expectations, direction, funding, rules and compliance restraints to the business process.

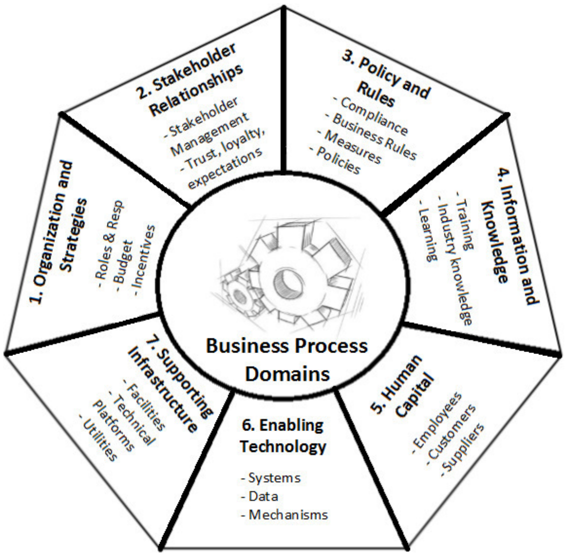

Fig. 4. Illustration of Guides and Enablers that contribute to the BP. *Based on [3], [34]*

1) Organization and Strategies - Constitutes the organization's governance and its support structure. This domain covers consistent management, cohesive policies, processes, roles and responsibilities. It also includes organizational alignment and strategy development to achieve vision and deliver results.
2) Stakeholder Relationships - This domain constitutes both the external and internal stakeholders of the organization. It covers stakeholder management of expectations, trust and loyalty. The stakeholders are people who have vested in the success of the organization and can benefit from its performance.
3) Policy & Rules - Constitutes the business policies and rules of the organization, and are established to ensure compliance and mitigate risks through appropriate controls. The policies provide a decision-making framework at all levels of the organization.
4) Information and Knowledge - Encompasses training, learning and industry knowledge.*Defined as a guide in [3], [5].*

   Enabler are the reusable resources of an organization that support the BP in transformation of input to output. Enablers provide execution capabilities for the BP.
5) Human Capital - Constitutes of the people who enables the process, namely employees, customers, and suppliers. For the employee it is about their competence, which encompasses of a combination of knowledge, skills and behavior. Capable people are essential to optimally executing a process.
6) Enabling Technology - Constitutes of the technology that enables the BP. Includes information technologies such as business applications, data stores, and mechanisms such as production lines, robots, and engineering equipment.
7) Supporting Infrastructure - Constitutes of production facilities, technical platforms, communications, utilities and energy, and other infrastructure. Can also be considered as the capital asset of the organization.

V. Method

The primary research method adopted in this work is analytical. This article uses theoretical comparisons and mapping of BPM and ISM, for each BP activity we look for a corresponding IS activitiy. Similarly, for each IS activity, we look for a corresponding BP activity. This process will identify the intersection of BP and IS as well as what activities that are missing if BP and IS "compliance" is desired.

Following Ko et.al. [33] we start at the very top of the abstraction levels, comparing the generic lifecycles of BPM and ISM. Staying at a high level of abstraction, we compare organization/risk views and corresponding tasks. Lastly, we do a domain comparison of the BPM and ISM.

VI. A Comparison of ISM and BPM Lifecycles

The purpose of this section is to look for similarities and possibilities of integration between the top-level implementation strategies of the ISMS and BPM. We compare the high level steps of the plan-do-check-act (PDCA) lifecycle of the ISMS [9] and BPM lifecycle (BPM-LC) and look for common ground. Both cycles represent high-level views of the general activities of each approach. As there is no uniform view on the BPM-LC, we use the steps summarized in this article. We make the assumption that the ISMS lifecycle is compliant with the original PDCA-cycle, and compare the BPM-LC with the PDCA cycle as described by Moen and Norman [35].

TABLE I
A COMPARISON OF THE GENERIC PDCA STEPS AND THE BPM LIFECYCLE

PDCA steps/ BPM Lifecycle	**Plan**	**Do**	**Check**	**Act**
1. Modeling	X			
2. Implement/ Sys Config		X		
3. Enact/ Execution		X		
4. Analyze/ Monitor			X	
5. Manage/ Diagnosis				X

Table I shows that the generic BPM-lifecycle is loosely related to a PDCA notion of continuous improvement. A further comparison of the ISMS and BPM lifecycle approaches shows:

1) *Plan - Modelling:* The Plan-phase in ISMS is applied to establish context and scope the ISMS, together with planning for ISRM. In BPM, the steps in the modelling-phase maps existing BPs and plan/re-design BPs for enactment and analysis. Similar for both approaches is that they both establish the context and scope in this phase, the BPM uses BPs while IS uses e.g. an asset-based approach to establish organizational context. ISO/IEC 27005:2011 [6] names BPs as one of two primary assets, which may open for a combined approach of BPM context establishment.
2) *Do - "System Configuration" & "Implementation and Enact/Execution":* The steps in the Do-phase of the ISMS-lifecycle consists of implementing the processes associated with the ISMS. Usually in form of implementing risk treatment plans as a result of the ISRM program.
The system configuration and implementation-phase in BPM implements designs by configuring process aware information systems and the underlying infrastructure. While the Enact/Execution phase executes and enacts the BP model. Both these BPM-phases correspond to the Do-phase in the PDCA cycle. Similar for both the ISMS and BPM lifecycles is that they both *implement* plans.
3) *Check - Analyze/Monitor:* This ISMS-phase monitors and reviews the effectiveness of implemented security process and residual risks. While the BPM-phase monitors and analyzes BPs for optimization. Both the IS and BPM lifecycles utilizes this phase for *monitoring and analysis* of the implemented processes.
4) *Act - Manage/Diagnosis:* The ISMS act-phase is mainly used to improve existing security processes based on analysis. The Manage and Diagnosis phase is utilized to adjust and improve BPs based on results from the previous lifecycle phase. This phase is also used to reallocate resources between BPs and manage large collections of BPs. Common for both lifecycles is implementing improvements based on analysis results from the previous phase.

We see from this comparison that the approaches are closely related; they are both founded on the PDCA principle, and the main tasks of each step is also similar.

VII. A COMPARISON OF ORGANIZATIONAL VIEWS

People employed at different levels of the organization both perceive and worry about different risks [12], which is also similar for the different concerns in the BPM hierarchy [5]. There is therefore a difference in what kind of information is needed to conduct tasks for both BPM and ISM at different levels of the organization. The purpose of this section is therefore to compare and map the organizational views and associated tasks presented in BPM and ISRM literature.

The BPM Methodology Framework represents a view of BPM sorted into levels including enterprise, process and implementation level, with recommended BPM steps per level (see [3], [5], [8]). NIST SP 800-39 [7] presents three different tiers for ISRM views, the comparison between the organizational views can be seen in table II.

TABLE II
A COMPARISON OF ORGANIZATIONAL VIEWS FROM THE NIST SP 800-39 [7] AND BPM METHODOLOGY FRAMEWORK [3], [5], [8]

Abstraction level	**Category**	**Multitier Org -Wide RM**	**BPM Methodology Framework**
Level 1	**Perspective**	Organizational	Enterprise
	Management	Top management	Organizational Management
	Main Tasks	Strategic risk management	Corporate Strategy in BPM, Supply chain
Level 2	**Perspective**	Mission/ Business Processes	Processes
	Management	Middle management	Process Management
	Main Tasks	RM of M/BP	Process Improvement
Level 3	**Perspective**	Information Systems	Implementation Level
	Management	Operations	Activity Management
	Main Tasks	Tactical Risk	Implementation of Information systems

The top-level comparison of the organizational views reveal a strong similarity. This is not surprising as one of NIST SP 800-39's main focus areas is securing BPs. Looking closer at the comparison we see a strong similarity in perspectives, tasks and responsibilities at each level:

- *Level 1* - We consider top management and organizational management to represent the same point of view. Both have a top-level management focus and are concerned

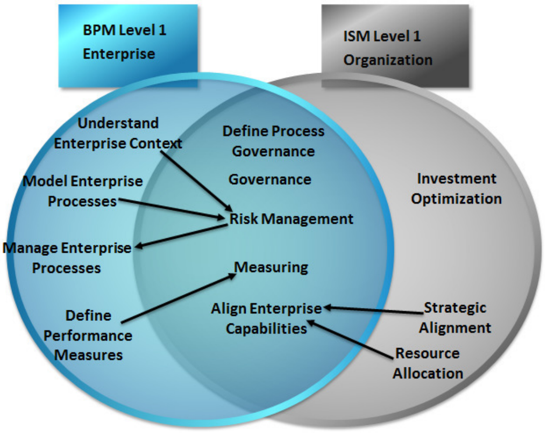
BPM Level 1
Enterprise
ISM Level 1
Organization
Understand Enterprise Context
Define Process Governance
Model Enterprise Processes
Governance
Investment Optimization
Risk Management
Manage Enterprise Processes
Measuring
Define Performance Measures
Align Enterprise Capabilities
Strategic Alignment
Resource Allocation

Fig. 5. Illustration of common BPM & ISM Level 1 tasks. Arrows indicate that a task is part of an activity, and that conducting the individual task will not complete the activity.

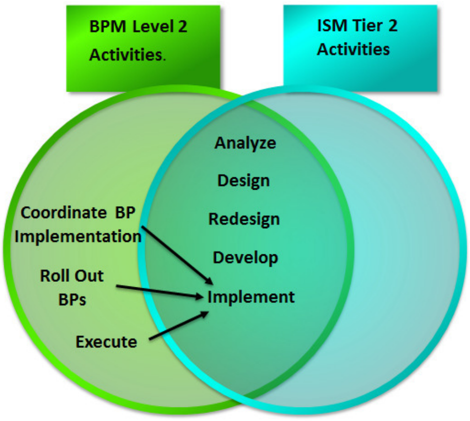

Fig. 6. Illustration of common BPM & ISM Level 2 tasks. Arrows indicate that a task is part of an activity, and that conducting the individual task will not complete the activity.

with governance and strategy tasks. We use the BPM tasks as described by [3], [8] to compare the subtasks from ISRM. Since there is no standardized steps per level from NIST SP 800-39, we analyzed and summarized the following steps for level 1 [7]: (i) Governance - assign roles and responsibilities to provide strategic direction, mission and objective achievement, risk management and resource usage, (ii) Strategic Alignment - of mission and business functions, (iii) Execution of Risk Management - frame, assess, respond to, and monitor risk (iv) Resource Allocation - of RM resources, (v) Measuring - monitoring and reporting RM metrics to ensure aligment, and (vi) Investment optimization - based on RM in support of organizational objectives.

The results from the comparison between ISRM and BPM level 1 sub-tasks can be seen in Fig. 5. The comparison show that the NIST RM function cover both *understanding the enterprise context* and *modelling enterprise processes* under Risk Framing, both activities necessary to conduct ISRM. However, the RM function only contributes to *Managing enterprise processes* which also includes activities such as establishing a BP services charter [3]. The same can be said for *Strategic aligment* of risk decisions, which is a part of completing *Aligning enterprise capabilities*, but does not complete the task. Our comparison show that there is no support for *Investment optimization* based on risk management at this level in BPM. Conducting resource allocation of RM resources will not complete any BPM tasks, but is a part of the *aligning enterprise capabilities* activity.

Comparing the other way, we see that there is no single ISRM Level 1 subtask to understand enterprise context and model enterprise context, but both are necessary steps in *execution of RM* task. While *defining performance measures* is a part of the ISRM activity *measuring*, we cannot say that completing the BPM activity also completes the ISRM task. However, managing enterprise processes also measures processes and allocates resources.

- *Level 2* - Middle management and Process management are descriptions of the same responsibilities and points of view, only differentiated by organizational structure (e.g. matrix based for process management, or traditional department-based organization for middle management) [5]. Both have a BP perspective, and are concerned with modeling, prioritizing and re-designing processes. Further comparison of level 2 subtasks is seen in Fig. 6, where we see that the Level 2 BPM activities resemble the BPM lifecycle. As there are no standard steps in NIST SP 800-39, we have summarized the following level 2 steps from [7] for developing Risk-aware BPs: (i) Design - Existing BP (AS-IS), (ii) Develop - secure BP (TO-BE), (iii) Implement - secure BP. The standard also suggests to develop Secure Enterprise Architecture (EA) as a Level 2 task, which comprises maximizing effectiveness of BPs and information resources. We regard this task as present in all the BP-ISRM steps, and therefore do not count it as a standalone task.
  Our understanding of the NIST SP 800-39 tier two steps is that implementing a secure BP includes the BPM tasks "Coordination" (preparing for implementation), "Rolling out" and "Executing". Which means that all the BPM activities are supported in the ISRM approach. Comparing the other way shows that the "Analyze" and "Redesign" activities are covered by the ISRM steps, and that three remaining tasks together complete the ISRM "Implement" activity.
- *Level 3* - The information systems and implementation level perspective represents the operations and activity management point of view. The processes are found at the lower levels in the BPM hierarchy (see section 1), and represents where "the rubber meets the road" [3]. We consider this to represent the same management and perspective. Although both BPM and ISRM share the

operations view, they have slightly different concerns; IS is focused on securing information systems from tactical risks and managing controls, while BP is concerned with designing systems to implement with BPs.
As BPM employs several methodologies at this level, and the BPTrends associates' BPM Methodology framework does not extend to software and HR development [8], we have no standard tasks to compare to the ISRM. Mahal [3] mentions that one commonly used BPM method at this level is the software development lifecycle (SDLC). Risk managing the SDLC is also the main approach in NIST SP 800-39. Althought concrete HR-strategies are not present in the NIST standard, it does discuss organizational culture and it does also discuss the topic of trust, which we can not see mentioned in the BPM literature.

VIII. A comparison of ISM and BPM domains

The main objective of this section is to compare the ISM and BPM domains to investigate if all control objectives can be integrated using BPM, and that all relevant aspects of BPM are covered in the control objectives. IS encompasses many fields related to information technology and systems, the ISO/IEC-standards in the 27000-series are industry standards and we use them as representatives of what must be covered to achieve IS (Notably ISO/IEC 27001 & 27002 [9], [10]). Therefore, to compare BPM and ISM approaches we use the 14 security domains and controls from ISO/IEC 27002 [10]. We mutually compare the IS domains to the domains of BPM defined by Burlton [34] and refined by Mahal [3] and Harmon [5].

A. *Summary of Comparison, ISM and BPM*

This section contains a summary of the integration results of IS into BPM. Table III shows a high level comparison of how the control clauses are supported by the BPM-domains.

The comparison of the ISM and BPM domains shows that we can integrate the security clauses and controls into the BPM domains of enablers and guides, and model them as BPs. An example is the implementation of the controls from the Information security incident management-security categories, illustrated in Fig. 7, which shows how the guides and enablers support the process.

One significant finding was that the domains of BPM does not directly consider internal or external attackers. This can in some cases be considered as a weakness of BPM as it concerns itself availability and integrity of BPs. RM is suggested as a supporting practice in development of the guides "Policy & Rules" [3]. The attacker might be considered as a part of general RM, but RM is such a wide discipline that it is likely to mean different things to different people [27].

BPM also presents a bit different view of assets; as the context, represented by BPs, is established before identifying the assets. In traditional ISRM, the situation is the other way around; first the asset that needs protection is identified, and then the context is modeled around the asset. Besides from

TABLE III
Summary of BPM-ISM and ISM-BPM comparison.
Legend: - "X" marks how the ISM domains are covered and can be implemented in the BPM domains.
- "0" marks which ISM domains support BPM domains and where.

Domains BPM ISM Domains	1.Organization and Strategy	2.Stakeholder Relationships	3.Policy and Rules	4.Information and Knowledge	5.Human Capital	6.Enabling Technology	7.Support Infrastructure
1.Information Security Policy	X 0		X 0	X 0	X		
2.Organization and IS	X 0	0	X 0	0	X	X	X
3.Human Resources Security	X		X 0	X 0	X 0	X	
4.Asset Managment	X		X 0	X 0	X	X 0	X 0
5.Access Control			X 0	X 0	X 0	X 0	X
6.Cryptography			X 0	0	X	X 0	X
7.Physical and Environment Security			X 0	0	X	X 0	X 0
8.Operations security	X		X 0	X 0	X	X	X
9.Communications sec			X 0	X 0	X	X	X 0
10.System acquis, developm and mainte			X 0	X 0	X	X 0	X
11.Supplier relations		X (0)	X 0	X 0	X 0	X	X
12.IS incident man	X		X 0	X 0	X	X 0	X
13.IS aspect of BCM	X		X 0	X 0	X	X 0	X
14.Compliance			X 0	0	X	X	

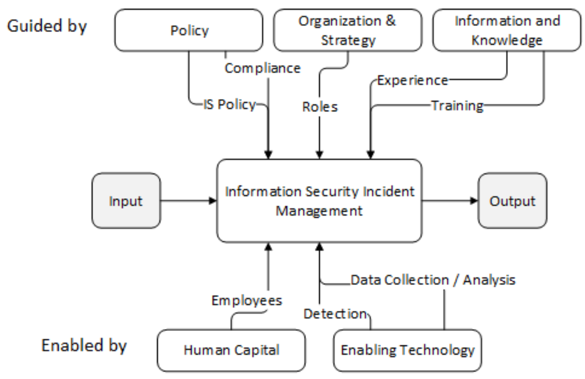

Fig. 7. The illustration shows how the IS Incident Management control can be modelled within the BP domain.

knowledge, intangible assets are not reflected in the BPM domains.

Another result that can be seen from the comparison is that the enabler "Human Capital", which generally represents employees, are needed to implement and operate every ISM control domain. However, the comparison show that out of fourteen control domains, only four are related to the security of human capital.

B. Summary of Comparison, BPM and ISRM

This section contains a summary of the integration results of BPM into ISM. Our comparison shows that the controls in ISO/IEC 27002:2013 are properly scoped to address four of the seven BPM domains. The enabler-domains were all addressed, but there were issues when addressing three of the Guide-domains:

1) Organization and Strategies: ISO/IEC 27001, section 5.1 a) emphasizes IS policy's compatibility with the organizations strategic direction, however, it is not mentioned in one of ISO/IEC 27002's 114 controls that the IS policy should be aligned with business. We can make the assumption of alignment from clause control objective 5.1, which is to provide management direction and support for IS in accordance with business requirements and compliance. The control itself state that the policy should be defined and approved by management. This points to a difference in perspective between the two disciplines, where BPM hammers organizational alignment of BPs as one of its main mantras.

2) Stakeholder Relationships: Nurturing both internal and external stakeholder relationships is an essential component of BPM; stakeholder identification, steering expectation, ensuring trust and loyalty are essential to BPM success [3], [5], [36]. Section "6.1 Internal organization" [10] covers some stakeholder groups (without using that term), as authorities and "special interest groups" are both types of stakeholders. The suggested controls put emphasis on maintaining contact with these stakeholders. However, these external groups are per BPM definition not important stakeholders, ISO/IEC 27001:2013 address the stakeholder needs in section 4.2 *Understanding the needs and expectations of interested parties*, but we can not see this reflected in the control objectives. The ISMS-program risk failing if key stakeholders lose interest, several instances of failure due to not having sufficiently powerful allies is highlighted in [22]. Although not completely neglected by IS, there is a clear gap between how much emphasis BPM and ISRM put on stakeholder management.

3) Information and Knowledge: It is a given that information is covered by all of the security domains. In BPM, information is utilized as knowledge by employees to fuel BPs [3], and knowledge is generally possessed by employees. The "Return of Assets"- security control (8.1.4) briefly mentions knowledge; *In cases where an employee, contractor or third party user has knowledge that is important to ongoing operations, that information should be documented and transferred to the organization.* This reflects a preventive control at the *end* of an employment. Capturing knowledge presents difficulties, as the interviewer must know exactly what questions to ask and the subject must be cooperative and willing to communicate the information in a comprehensive way.

This brings up the question if an ISRM process can identify and protect critical knowledge. Knowledge is viewed as an intangible asset [37], but e.g. is not included in the asset overviews in [28] or [6]. However, loss of availability due to lack of knowledge is a plausible IS risk (e.g. during incident handling), combined with the importance of knowledge in BPM, makes it an important business area to secure. Depending on the skill of the analyst, knowledge runs the possibility of being overlooked by ISO/IEC 27005:2011 and asset-based approaches.

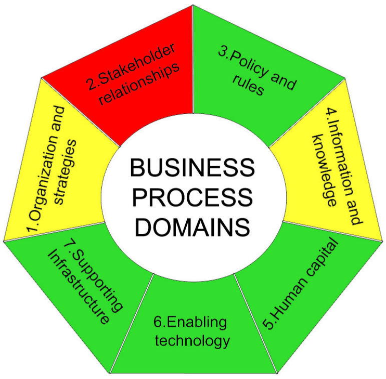
BUSINESS PROCESS DOMAINS
1.Organization and strategies
2.Stakeholder relationships
3.Policy and rules
4.Information and knowledge
5.Human capital
6.Enabling technology
7.Supporting Infrastructure

Fig. 8. Heatmap indicating how well ISM covers the BPM domains, green signals no issues, red signals significant issues.

IX. Conclusion

We have shown in this article that both the top-level BPM and ISM approaches are based on a Deming-cycle (PDCA) of continuous improvement, and that the main tasks of each step are similar.

We have shown that there is a strong similarity between the BPM Methodology framework and the ISRM standard NIST SP 800-39, as both approaches uses similar organizational views, only applying different names. We have also shown that the tasks and goals of each level are similar, with some key differences: the tier/level 1 ISRM approach does not include an activity for managing enterprise processes, and BPM does not include risk based investment optimization and trust-issues.

When comparing BPM and ISM domains we found that the ISM tasks can be supported by BPM, but that BPM does not include the concept of internal or external attackers. Further we found that ISO/IEC 27001/2 standards emphasized, but not controlled that the IS policy was aligned with business requirements. We also found a large gap between how much emphasis ISM and BPM put on stakeholders. Where BPM have fully adopted the principles of stakeholder management and recognized its importance, there is no real approach adopted in ISM to address stakeholders. We also found that the need for securing knowledge possibly is underestimated in ISM.

A. Future Work

As our findings are theoretical, we suggest further validation of the results from this article. This article has also shown that there is some common ground between BPM and ISM, and this warrants further investigation to determine if a joint approach is feasible. This work has revealed the potential for further research concerning stakeholder management in information security.

Acknowledgements

The authors of this paper thanks the anonymus reviewers for their valuable comments and suggestions. The PHD-student is sponsored by COINS Research School for IS.

References

[1] *Information technology, Security techniques, ISMS, Overview and vocabulary*, International Organization for Standardization Norm, ISO/IEC 27000:2009. [Online]. Available: http://dx.doi.org/10.3403/30236519

[2] W. M. van der Aalst, "Business process management: A comprehensive survey," *ISRN Software Engineering*, vol. 2013, 2013. [Online]. Available: http://dx.doi.org/10.1155/2013/507984

[3] A. Mahal, *How Work Gets Done: Business Process Management, Basics and Beyond*. Technics Publications, LLC, 2010.

[4] R. Damelio, *The basics of process mapping*. Taylor & Francis US, 2011.

[5] P. Harmon *et al.*, *Business process change: A guide for business managers and BPM and Six Sigma professionals*. Morgan Kaufmann, 2010. [Online]. Available: http://dx.doi.org/10.1016/b978-012374152-3/50043-4

[6] *Information technology, Security techniques, Information Security Risk Management*, International Organization for Standardization Std., ISO/IEC 27005:2011.

[7] G. Locke and P. Gallagher, "800-39 nist sp, managing information security risks - organization, mission, and information systems view," National Institute of Standards and Technology, Tech. Rep., 2008.

[8] "The bpm methodology framework," http:\\www.BPTrends.com, visited April 2014.

[9] *Information technology - Secuirty techniques - Information security management systems - Requirements*, International Organization for Standardization Norm, ISO/IEC 27001:2013. [Online]. Available: http://dx.doi.org/10.3403/30192065

[10] *Information Technology, Security Techniques, Code of Practice for Information Security Management*, International Organization for Standardization Std., ISO/IEC 27002:2013. [Online]. Available: http://dx.doi.org/10.3403/30186138

[11] S. Jakoubi and S. Tjoa, "A reference model for risk-aware business process management," in *Risks and Security of Internet and Systems (CRiSIS), 2009 Fourth International Conference on*. IEEE, 2009, pp. 82–89. [Online]. Available: http://dx.doi.org/10.1109/crisis.2009.5411973

[12] A. G. Kotulic and J. G. Clark, "Why there aren't more information security research studies," *Information & Management*, vol. 41, no. 5, pp. 597–607, 2004. [Online]. Available: http://dx.doi.org/10.1016/j.im.2003.08.001

[13] N. Milanovic, B. Milic, and M. Malek, "Modeling business process availability," in *Services-Part I, 2008. IEEE Congress on*. IEEE, 2008, pp. 315–321. [Online]. Available: http://dx.doi.org/10.1109/services-1.2008.9

[14] A. Jallow, B. Majeed, K. Vergidis, A. Tiwari, and R. Roy, "Operational risk analysis in business processes," *BT Technology Journal*, vol. 25, no. 1, pp. 168–177, 2007. [Online]. Available: http://dx.doi.org/10.1007/s10550-007-0018-4

[15] Y. Asnar and F. Massacci, "A method for security governance, risk, and compliance (grc): a goal-process approach," in *Foundations of security analysis and design VI*. Springer, 2011, pp. 152–184.

[16] M. Zoet, R. Welke, J. Versendaal, and P. Ravesteyn, "Aligning risk management and compliance considerations with business process development," in *E-Commerce and Web Technologies*. Springer, 2009, pp. 157–168. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-03964-5_16

[17] S. Taubenberger and J. Jürjens, "It security risk analysis based on business process models enhanced with security requirements," in *Modeling Security Workshop, Toulouse, France*, 2008.

[18] S. Kokolakis, A. Demopoulos, and E. A. Kiountouzis, "The use of business process modelling in information systems security analysis and design," *Information Management & Computer Security*, vol. 8, no. 3, pp. 107–116, 2000. [Online]. Available: http://dx.doi.org/10.1108/09685220010339192

[19] P. Herrmann and G. Herrmann, "Security requirement analysis of business processes," *Electronic Commerce Research*, vol. 6, no. 3-4, pp. 305–335, 2006. [Online]. Available: http://dx.doi.org/10.1007/s10660-006-8677-7

[20] A. Ekelhart, S. Fenz, and T. Neubauer, "Aurum: A framework for information security risk management," in *System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on*, 2009, pp. 1–10.

[21] G. Stoneburner, A. Goguen, and A. Feringa, *NIST 800-30, Risk Management Guide for Information Technology Systems, Special publication*, National Institue of Standards and Technology (NIST) Std., 2002.

[22] S. Ozkan and B. Karabacak, "Collaborative risk method for information security management practices: A case context within turkey," *International Journal of Information Management*, vol. 30, no. 6, pp. 567–572, 2010. [Online]. Available: http://dx.doi.org/10.1016/j.ijinfomgt.2010.08.007

[23] R. A. Caralli, J. H. Allen, and D. W. White, *CERT Resilience Management Model (CERT-RMM): A Maturity Model for Managing Operational Resilience*. Addison-Wesley Professional, 2010.

[24] P. H. Gregory, *All in one - CISA - Certified Information Systems Auditor - Exam Guide*. McGraw-Hill Companies, 2012.

[25] *Risk Management - Principles and Guidelines*, International Organization for Standardization Std., ISO/IEC 31000:2009. [Online]. Available: http://dx.doi.org/10.3403/30246105

[26] V. Bier, "Challenges to the acceptance of probabilistic risk analysis," *Risk Analysis*, vol. 19, no. 4, pp. 703–710, 1999. [Online]. Available: http://dx.doi.org/10.1023/A%3A1007093805693

[27] G. Wangen and E. Snekkenes, "A taxonomy of challenges in information security risk management," in *Proceeding of Norwegian Information Security Conference / Norsk informasjonssikkerhetskonferanse - NISK 2013 - Stavanger*, vol. 2013. Akademika forlag, 2013.

[28] J. Wunder, A. Halbardier, and D. Waltermire, *Specification for Asset Identification 1.1*. NIST - US Department of Commerce, National Institute of Standards and Technology, 2011.

[29] R. S. Aguilar-Saven, "Business process modelling: Review and framework," *International Journal of production economics*, vol. 90, no. 2, pp. 129–149, 2004.

[30] B. Wetzstein, Z. Ma, A. Filipowska, M. Kaczmarek, S. Bhiri, S. Losada, J.-M. Lopez-Cob, and L. Cicurel, "Semantic business process management: A lifecycle based requirements analysis." in *SBPM*, 2007.

[31] R. K. Ko, "A computer scientist's introductory guide to business process management (bpm)," *Crossroads*, vol. 15, no. 4, p. 4, 2009. [Online]. Available: http://doi.acm.org/10.1145/1558897.1558901

[32] W. M. Van Der Aalst, A. H. Ter Hofstede, and M. Weske, "Business process management: A survey," in *Business process management*. Springer, 2003, pp. 1–12. [Online]. Available: http://dx.doi.org/10.1007/3-540-44895-0_1

[33] R. K. Ko, S. S. Lee, and E. W. Lee, "Business process management (bpm) standards: a survey," *Business Process Management Journal*, vol. 15, no. 5, pp. 744–791, 2009. [Online]. Available: http://dx.doi.org/10.1108/14637150910987937

[34] R. Burlton, *Business process management: profiting from process*. Pearson Education, 2001.

[35] R. Moen and C. Norman, *Evolution of the PDCA Cycle*. Associates in Process Improvement, 2011.

[36] A. Josey, *TOGAF Version 9: A Pocket Guide*. Van Haren Pub, 2009.

[37] D. J. Teece, "Capturing value from knowledge assets: The new economy, markets for know-how, and intagible assets." *California management review*, vol. 40, no. 3, 1998. [Online]. Available: http://dx.doi.org/10.2307/41165943