BEST PRACTICE

Information Security Management with ITIL® V3

Jacques A. Cazemier
Paul Overbeek
Louk Peters

Other publications by Van Haren Publishing

Van Haren Publishing (VHP) specializes in titles on Best Practices, methods and standards within four domains:

- IT management,
- Architecture (Enterprise and IT),
- Business management and
- Project management

VHP is also publisher on behalf of leading companies and institutions:
The Open Group, IPMA-NL, PMI-NL, CA, Getronics, Quint, ITSqc, LLC, The Sox Institute and ASL BiSL Foundation

Topics are (per domain):

IT (Service) Management / IT Governance
ASL
BiSL
CATS
CMMI
CobiT
ISO 17799
ISO 27001
ISO 27002
ISO/IEC 20000
ISPL
IT Service CMM
ITIL® V2
ITIL® V3
ITSM
MOF
MSF
ABC of ICT

Architecture (Enterprise and IT)
Archimate®
GEA®
TOGAF™

Business Management
EFQM
ISA-95
ISO 9000
ISO 9001:2000
SixSigma
SOX
SqEME®
eSCM

Project/Programme/ Risk Management
A4-Projectmanagement
ICB / NCB
MINCE®
M_o_R®
MSP™
PMBOK® Guide
PRINCE2™

For the latest information on VHP publications, visit our website: www.vanharen.net.

Information Security Management with ITIL® Version 3

Jacques A. Cazemier,
Paul Overbeek,
Louk Peters

Van Haren PUBLISHING

Colophon

Title:	Information Security Management with ITIL® V3
Series:	Best Practice
Authors:	Jacques A. Cazemier, Paul Overbeek, Louk Peters
Editor:	Jane Chittenden
Publisher:	Van Haren Publishing, Zaltbommel, www.vanharen.net
ISBN:	978 90 8753 552 0
Print:	First edition, first impression, January 2010
Design and Layout:	CO2 Premedia, Amersfoort-NL
Copyright:	© Van Haren Publishing, 2010
Printer:	Wilco, Amersfoort – NL

For any further enquiries about Van Haren Publishing, please send an e-mail to: info@vanharen.net

Contents

1 Introduction 1
1.1 This book 1

2 Fundamentals of information security 9
2.1 Perspectives on information security 9
2.2 Security architectures 20

3 Fundamentals of management of information security 27
3.1 Information Security Management – the continuous effort 28
3.2 Information Security Management as a PDCA cycle 28

4 ITIL version 3 and information security 37
4.1 Service Strategy 41
4.2 Service Design 54
4.3 Service Transition 59
4.4 Continual Service Improvement 68
4.5 Service Operation 77
4.6 Brief reflection on ITIL v3 90

5 Guidelines for implementing Information Security Management 91
5.1 Implementing or improving ITIL Information Security Management 91
5.2 Awareness 94
5.3 Organization of Information Security Management 96
5.4 Documentation 102
5.5 Natural growth path through maturity levels 104
5.6 Pitfalls and success factors 113
5.7 Partnerships and outsourcing 114

Annex A: Information Security Management and standardization 117

Annex B: Cross-references for ISO/IEC 27002 and ITIL Information Security Management 129

Annex C: Literature and links 131

About the authors

Ing. Jacques A. Cazemier is Management Consultant at Verdonck, Klooster & Associates (VKA), an independent consulting company in the Netherlands.

Dr. ir. Paul Overbeek RE is partner with OIS Information Risk & Security Management and lectures at the universities of Amsterdam, Rotterdam and Tilburg.

Drs. Louk Peters is senior business consultant for Getronics Consulting, one of the founding organizations for ITIL.

Acknowledgements

In theory, there is no difference between theory and practice. In practice there is.

This book has been written to show theory and practice of dealing with Information Security Management. We share our experiences of aiding organizations in incorporating information security management. Those experiences would not have been possible without the continuous contributions from people who – just like us – are dealing with information risks on a daily basis.

We would like to thank the reviewers who provided valuable comments on the texts we had written. In alphabetical order they are:
Dr Gary Hinson, IsecT Ltd
David Jones, Pink Elephant UK
David Lynas, SABSA Foundation
Paul Peursum, DNV-CIBIT, The Netherlands
Rita Pilon, EXIN International
Dr Gad J Selig, University of Bridgeport, USA
Dr Abbas Shahim, Atos Consulting, The Netherlands
Takanori Tsukada, Hitachi Software Engineering Co., Ltd., Japan
Xander van der Voort, vanderVoort Projects, The Netherlands

Executive summary

Challenges

In recent years there have been developments that require more confidence in information and information processing. Those developments range from regulations and directives to pressure from stakeholders and from changes in use of technology to increased liability.

As organizations have become increasingly dependent on electronic delivery of services, the importance of maintaining high standards for information technology (IT) performance is increased as well. Information is one of the most important assets for business; sharing of information with other organizations adds to that importance.

Information is also becoming more vulnerable: it can deteriorate, it may fall in the hands of an unauthorized person, it may be corrupted, and it might not be available when needed. It is increasingly threatened by deliberate attack and by unintentional security incidents such as the loss of huge numbers of personal records stored electronically.

In addition, legislation and regulations mandate governance and compliance. Information security provides the basis for these aspects: assurance that information is reliable and information processing is sound. Information has to be provided to prove compliance. Add to that the need to manage IT costs and it is clear that maintaining the required level of information security is a major challenge.

Solutions

For IT, information and the power to process this essential asset is the core of its existence. Endangering information or its processing will immediately threaten the business. For that reason, securing information as well as the IT that processes it is an important subject.

Just maintaining the required level of information security is not sufficient. It is essential to have continuous security improvement to the level where risks are still acceptable. This does not stop at building more technology to repel threats or strengthening procedures. It also means managing the required level of security.

This book provides the background to enable adequate information security. It is an update of ITIL® (IT Infrastructure Library) version 2 Security Management book [CAZ] and fits within the ITIL version 3 service lifecycle. It also makes reference to international standards like ISO/IEC 20000 and ISO/IEC 27001. ITIL® is a registered trademark of the UK Office of Government Commerce.

This book describes Information Security Management with ITIL version 3 and builds on the ITIL version 3 processes and activities that are required to manage IT effectively.

Results

The benefits of sufficiently secure information extend to the entire business, from corporate image and position in the market to effectiveness and efficiency. It provides inherent flexibility: because information and IT security is controlled, robustness and reliability are ensured. Demonstrable compliance and continuous adherence to regulations form the basis for all business processes that require use of information and information processing.

Information Security Management gives IT resilience to survive, whatever the storms that threaten the business.

1 Introduction

1.1 This book

Information security is one of the subjects with wide coverage on the Internet. Texts on improving security, as well as breaching security, are just a few clicks away. This phenomenon is one of the reasons that maintaining information security is such an important subject: ignorance of your own information security is an open invitation to serious problems in everything that your information is used for. Without continuous effort to maintain an adequate level of protection, all investments in reliable information processing will lose their value and processes dependent on trustworthy information will fail.

Information security is an essential requirement for organizations that use and rely upon information since information is a volatile corporate asset. Commonplace security risks to information assets include:

- fraudsters inside or outside your organization who exploit missing or weak process controls for personal advantage
- theft or unauthorized disclosure of proprietary or personal data (e.g. industrial espionage, inappropriate web publication)
- human errors and omissions by information users, system/network administrators and operators (e.g. inaccurate or incomplete data entry, mis-configuration of technical security controls)
- malware – malicious software such as network worms and Trojan horse programs
- hackers who deliberately attempt unauthorized access to systems
- technical vulnerabilities arising from programming errors and design flaws in computer software, firmware and hardware (bugs and so forth)
- physical damage or loss of IT equipment and information storage media arising from storms, floods, lightning, sabotage, accidents and thefts.

In the ITIL context, many of these risks are likely to affect the organization's provision of IT services unless suitable information security controls are in place. However, information security controls require resources to design, implement, manage and utilise, hence management needs to strike a balance based on the costs and benefits of security.

Management effort is required in order to maintain the required level of security. Since information security is not limited to one aspect of technology, personnel or process, management will need to have relationships with all processes in the organization. The consequence is that Information Security Management needs to be part of every process. In this book, Information Security Management is shown to be present in all phases of the lifecycle of ITIL version 3.

1.1.1 Context

This book is an update of the ITIL book Security Management, which is a title in the ITIL version 2 series. The reason for this update is twofold: it reflects the updates of ITIL version 3 and it adds new developments and changes to the previous version.

The update consists of:
- explaining the most important changes of ITIL version 3, as far as information security management is concerned
- incorporating the changes to Information Security Management as a result of updated standards and best practices
- describing new trends in information security and its management
- highlighting the increased importance of outsourcing and service orientation
- focusing on business aspects and practices.

In this book, Information Security Management is covered from setting the initial security objectives to implementation and maintenance. It shows the relationships to all processes and activities that interface with information.

Information Security Management is a management process. It is not restricted to information technology. It is not sufficient to limit information security management to computers, networks and software. Information on other media – like paper – will have to be protected as well. It is not restricted to people; and it is not restricted to processes. For example, countermeasures for threats to information security will be found in areas as diverse as organizational architecture, human resources, computer hardware and software, physical access to buildings and supply of electrical power.

Taking ITILv3 as the starting point also gives some limitations. The focus of Information Security Management in this context is more on information, IT and business alignment and less on topics that are also relevant for security including legal aspects, organizational change, HR management and facilities.

Target audience
This book is intended for IT managers and business managers who are looking for practical directions to maintain Information Security Management. It may also be useful to business process managers to understand what Information Security Management is about.

1.1.2 Best practice
The value of this book lies in its character as best practice. It integrates current standards and best practices. It is not a standard that would be used for a certification process, it is not a regulation to be followed to the letter. It provides ideas and experiences that may or may not be appropriate in your situation. We believe that the overall advice in this book is useful in the majority of cases; however, it may need to be adapted to your organization's situation.

The book enables comparison of experiences and informed discussions about implementation of Information Security Management. In addition, it may serve as a benchmark when organizations are comparing their efforts in this field.

1.1.3 The subject
Information security management is the process to ensure that both information and information processing is (and remains) reliable, confidential and available when and for whom it is required. It limits access to information and information processing to authorized people and functions.

Information Security Management deals with establishing and maintaining all that is needed to keep that required level of information security.

The basis for this required level is the specification of information security in the Service Level Agreement that has been agreed between the business and the service provider.

The goal of Information Security Management is to provide confidence and assurance to the business that the business assets are protected and the overall security process supports the business mission. Security has long been seen as a subject for the IT department, with much emphasis on technology. Solving business problems was never considered as a reason for security measures. Although the introduction of the standard BS7799 (later ISO/IEC 27002) made it clear that security is about more than technology alone, in practice we still see a silo approach towards security, so that security restricts business processes and even sometimes becomes a showstopper or restraint.

With a 'guard-dog' attitude, IT departments used to think that a secure IT infrastructure could only be established by just enforcing more rules, more and longer passwords, more limitations on access, more firewalls and the like. This approach has given security a bad reputation, sometimes called 'the business prevention department'.

Security is not an end in itself but a property relative to a specific (business) context. What is good for one organization does not necessarily have to apply to another. For others, there will be other risks. There is a definite need for 'tailored security'.

How to define and reach the required level of security – that is, how to determine which control objectives are needed and what controls are to be put in place to reach the required level of security – is one part of Information Security Management. It contains topics such as establishing the proper business requirement for information security, risk analysis, defining control objectives, the definition of the right countermeasures, creating a standard minimum level of information security, the implementation of controls and operational monitoring such as intrusion detection.

The other part of Information Security Management deals with maintaining information security at the required level and providing appropriate assurance. Security maintenance topics are incident registration and handling, trend analysis and reporting, escalation support, access management, hardening, maintaining standards, etc.

The first part, defining and reaching the required level of security, is performed first. When information security is 'in place', operational and functioning, the second part (maintaining the required level) is a continuous effort as part of the lifecycle. The activities are essentially the same as for the first part, but become progressively better informed by metrics and experience of the operational security management system. Of course, the requirements for security have to be maintained as well. These are not static since both the importance of information as well as the threats in the ever-changing IT and organizational infrastructure vary.

The Information Security Management process coordinates and directs the security activities, using a standard process management cycle.