A GUIDE TO ISO/IEC 38500:2015 GOVERNANCE OF IT

DOLF VAN DER HAVEN

ITSM PRESS

A Guide to ISO/IEC 38500:2015 Governance of IT

For Yvette Backer

A Guide to ISO/IEC 38500:2015 Governance of IT

ISBN Paperback: 9781912651160
ISBN eBook: 9781912651177

First Published in Great Britain by ITSM Shop Ltd

ITSM Press is the wholly owned publishing imprint of ITSM Shop Ltd.

Reviewers:

Andre Boutin (Mature ITSM)
Mark Thomas (Escoute Consulting)
Morwan Elgasim (DAL Group, Sudan)
Walter Macuada (Team Professional Services, Chile)

Other ITSM Press Publications:

A Concise Introduction to ISO 14001:2015
A Concise Introduction to ISO 9001:2015
A Concise Introduction to ISO 22301:2012
A Concise Introduction to ISO 45001:2018
Service Management: It's All About the People

ITSM Shop Ltd
95 Duxford Road, Whittlesford, Cambs, CB22 4NJ, UK
+44 (0) 3333 445 286
customerservices@itsmshop.co.uk
www.itsmshop.co.uk/

Contents

Introduction

The ISO/IEC 38500 series of standards is a relatively new set of standards that provides guidance on how an organisation should handle the governance of their Information Technology. This is done based on principles that indicate the preferred way to make decisions for governance of IT.

This may raise a number of questions, including the following:

1. What is governance?
2. Who is it that does this? Is it a group within the organisation itself, some external auditor, an elected or non-elected board of directors?
3. What is Information Technology? The expression itself seems directly focused on the technological means used to handle information in the organisation but can in some regions and contexts be interpreted much wider, to include the complete provision, use and exchange of information within a company between actual people, systems and infrastructures.
4. Where does governance of IT have overlap or interfaces with (IT) service management? Is management of services and the means to provide services not the same as governance of IT?
5. What is this standard to do with corporate governance in general?

The answers to these questions are partially answered by the ISO/IEC 38500 standard and partially not. Discussions around these are taking place continually within the ISO committee and working groups that deal with the ISO/IEC 38500 standard.

This book is based on the author's interpretation of the actual standards documents as well as various other models and frameworks, such as COBIT 5, ISO/IEC 20000-1 and others.

Governance of IT and ISO/IEC 38500 – High-level Overview

The first part of the ISO/IEC 38500 series of standards is a nice, thin, readable document that originated from an Australian standard, AS 8015. ISO and IEC turned it into their standard ISO/IEC 38500 in 2008, which in turn got its latest revision in 2015.

ISO/IEC 38500 defines Governance of IT as '[the] *system by which the current use of IT is directed and controlled*', as part of the broader corporate or organisational governance (which in turn is being developed as the ISO/AWI

37000 standard *Guidance for the Governance of Organizations*). The motivation for having a standard for Governance of IT in the first place, is that IT is often seen exclusively from the perspective of technology, its financial cost and benefits and planning, rather than from the perspective of its business benefits for the organisation. It is for that reason that the standard was created and aimed at a 'governing body', which is the entity that is accountable for the performance of the organisation and its conformance to policies and standards. The governing body can be a board of directors or other entity, as long as it is independent of the daily operation of the organization. By abiding by the guidelines in the standard, the governing body effectively puts the organisation in a better position to meet the usual business targets, such as efficient use of resources and assets, alignment of IT with the business outcomes, business continuity and reaping actual benefits from its investments in IT.

The standard defines three *tasks* of the governing body:

1. **Evaluate**: assess the current and future use of IT;
2. **Direct**: make sure strategies and policies for the use of IT are defined and implemented;
3. **Monitor**: be informed about the performance of IT and about the conformance to the policies; monitor the effectiveness of the direction given.

These tasks are performed in six areas, defined as *principles*:

1. **Responsibility**: the responsibility of people and teams in the organisation with respect to the need for IT and its availability should be defined;
2. **Strategy**: IT's capabilities should be taken into account in the organisation's business strategy;
3. **Acquisition**: the business case for the acquisition of IT services is to be sound and beneficial for the business outcomes;
4. **Performance**: the utility (fit for purpose) and warranty (fit for use) of IT should be safeguarded;
5. **Conformance**: IT should comply with a regulatory and legal requirements or rules;
6. **Human Behaviour**: given it is people who use IT, it better be adapted to their needs; people's competence to use IT resources needs to be taken into account as well as the ability to make IT-related decisions.

The three tasks apply to all these principles. More details will be discussed in a later chapter.

References

[1] ISO/IEC 38500:2015 Information Technology – Governance of IT – For the Organization

[2] ISO/IEC TS 38501:2015 Information technology — Governance of IT — Implementation guide

[3] ISO/IEC TR 38502:2017 Information technology — Governance of IT — Framework and model

[4] ISO/IEC 38503 Information technology — Governance of IT — Assessment of the Governance of IT *(in preparation)*

[5] ISO/IEC TR 38504:2016 Governance of information technology — Guidance for principles-based standards in the governance of information technology

[6] ISO/IEC 38505-1:2017 Information technology -- Governance of IT - Governance of data -- Part 1: Application of ISO/IEC 38500 to the governance of data

[7] ISO/IEC 38505-2 Information technology -- Governance of IT - Governance of data -- Part 2: Implications of 38505-1 for data management *(in preparation)*

[8] ISO/IEC 38506 Information technology -- Governance of IT – Governance of IT enabled investments *(in preparation)*

[9] ISO/IEC 38507 Information technology -- Governance of IT - Governance implications of AI *(in preparation)*

[10] Johnson, Brian et al. BiSL® Next - A Framework for Business Information Management. Van Haren, 2017.

[11] COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT. ISACA, 2012.

[12] Agutter, Claire et al. VeriSM™: A Service Management Approach for the Digital Age. Van Haren, 2017.

[13] ISO/IEC 20000-1:2018 Information Technology – Service management - Part 1: Service management system requirements

[14] ISO/IEC 20000-2:2019 Information Technology – Service management - Part 2: Guidance on the application of service management systems *(in preparation)*

[15] ISO 31000:2018 Risk management — Principles and guidelines

[16] ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements

[17] ISO 9001:2015 Quality management systems – Requirements

[18] ITIL Continual Service Improvement. The Stationary Office, 2011.

About the Author

Dolf van der Haven was born in Muiderberg, The Netherlands, in 1971. Originally a Geophysicist, he has a broad background in IT, Telecommunications, Management, Psychotherapy and Service Management. He currently works as a Quality, Information Security and Service Management Consultant at Verizon Enterprise Solutions and is Co-founder and Managing Director of Powerful Answers, a Service Management consultancy based in Bulgaria, The Netherlands and the Czech Republic. He is also member of ISO/IEC Joint Technical Committee 1, Subcommittee 40, which develops the ISO/IEC standard series 20000 (Service Management) and other standards. He is Co-editor of Part 2 of the ISO/IEC 20000 series.

Previous publications include *The Healing Elephant* (2008 in Dutch, 2009 in English), about psychotherapy; *The Human Face of Management* (2014) about people management; and *Service Management – It's all about the People* (2018) about service management and integral psychology.

Dolf lives in Groenekan, The Netherlands, with his partner and their 130 chickens.