**White Paper**

# Management and Governance Systems – The law of recurring patterns and its impact

## A white paper on the upcoming ISO 9001:2015


Submitted by:
Dr. Helmut Steigele
Director Central Europe

Office: +44 (0) 333 202 1018
Email: helmut.steigele@foxitsm.com

## Introduction

With the planned publication of an update to ISO 9001 next year, you may be forgiven for throwing your arms up and shouting “not another governance system revision”. This could quickly be followed by comments such as “more work to ensure compliance”, “starting from scratch again” and “wasted effort on other frameworks”. However, that needn’t be the case.

What this article argues is that there are recurring patterns not only across standards and frameworks but also within their iterations. Many of the structures and evidential proof of operation needed is already in place and can be repeated or repackaged with minimal rework.

## The Principle of Recurring Patterns

Recurring patterns is a principle that I have seen many times before, and none more so than when looking at integrated management or governance frameworks. Very often you could have the ‘principle of recurring patterns’ at the forefront of your mind when reviewing these, and of course you would be right.

Whether implicitly or clearly stated, each system or framework for governing and managing organisations shows these individual elements:

- Organisational context
- Vision and Mission Statement
- Declaration of Scope
- Requirements
- Descriptions of the offered goods and services
- The process domains for structuring the necessary evidence and compliance of your systems
- Mechanisms for identifying and managing corrective and improving actions.

So for those admirers of integrated governance or management systems and frameworks, nothing appeared too new when the first articles and inputs became available for the forthcoming revision of ISO 9001, to be known as ISO 9001:2015.

The same recurring patterns, albeit maybe with a clearer dedicated scope statement, can equally be found elsewhere, such as in the following:

| Framework | Scope |
|---|---|
| **COSO** | Governing Corporate Value Generation, Risk and Resource Optimisation |
| **CobIT** | Governance of Enterprise IT (e.g. Value Generation, Risk and Resource Optimisation) |
| **ISO/IEC 20000: 2011** | Managing the Quality of IT Services |
| **ISO/IEC 27001: 2013** | Managing Information Security |
| **ISO 22301** | Managing Business Continuity |
| **ISO 37500** | Managing Outsourcing and Outsourcing Relationships |

So if you look at the associated chapter structures and the relevant implementation rules, even a novice would figure out that there could have been some sort of correlation of thoughts between those who have created these systems.

But this shouldn't be considered a disadvantage because patterns like these can be used, and indeed are used, avoiding duplication of effort in, for example, the creation of supporting documentation.

This synchronisation between different management systems and frameworks enables effort to be saved by developing a single source of trusted documentation and evidence.

For example, why should an incident management process be described within CobIT or ISO/IEC 20000 in a different way to that found in ISO/IEC 27000? Even in ISO/IEC 20000 there is a substantial interest to protect the integrity, availability and confidentiality – so there in fact is another recurring pattern that we have identified.

Maybe the competition between all of these governance and management systems has challenged the so-called 'masters' and 'experts' involved in developing ISO standards to move their stable, process-orientated and quite flexible framework into new holistic, goods and service-orientated versions.

One particular factor is clear, and was stated by ISO (International Organization for Standardization) itself: the new version of ISO 9001 will give consistency in terms, architecture and references between the 'mother ISO 9001' and a lot of specialised sub-products, like the 14000, 20000 or 27000 series.

## Recurring Pattern: Directional Layer

No doubt the puritans amongst the auditors and compliance specialists reading this paper will be raising their eyebrows right now! So I will provide some thoughts concerning the style of presentation between governance layers and the management layer definition, and I'll use a synthesis that I've named 'directional layer'.

The headline titles within the forthcoming ISO 9001:2015, from chapter 1 to 5, cover almost the same fields as the entry points of governance frameworks like COSO and CobIT:

1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organisation
    - Understanding the organisation (*What is the organisation offering*) and its context (*Stakeholders, Laws and Regulations*)
    - Needs and requirements
    - Scope
    - Management System
5. Leadership
    - General
    - Management commitment
    - Policy
    - Roles, responsibility and authority

But there is one key difference and that is with the scoping statement. Within an ISO standard you base a scope on dedicated quality features, on preventing specific risks, or on proving specific requirements are met. Within COSO and CobIT, you have a clear focus on resource optimisation, risk-balancing, and on overall value generation.

Regardless, the language used and some of the structure can be considered similar.

As long as you are governing something, you should be stating both the principles and policies of operation, whilst also taking into consideration the "shalls" and the "shoulds" of the applicable standard for which you are seeking certification. But that is still not enough – you also need to consider stakeholder interests and the overall company strategy and goals.

But if you manage something, you should bring governance into real life. Therefore you plan, you assign resources, you measure and you improve.

And if you look at the new structure of ISO 9001: 2015 you will realise that in fact chapters 1 to 4 can and will be used for governance issues and risk management too. Maybe it was revised with the entities that do not have the depth and breadth of large or global enterprises in mind, but irrespective this structure delivers a suitable instrument for governing risk, overall quality and resource optimisation – within both profit and non-profit orientated organisations.

## Recurring Pattern: Needs and Requirements – PDCA

It is rare that you can generate value for both customers and yourself if you do not first capture the requirements from your customers (or potential customers) of the goods and services that they want. So without identifying and capturing potential customer interest (one if not the most important of all stakeholders, and stakeholder drivers), then there is no real reason for the consumption of those goods and services.

If you do not consider exactly this when developing your ISO 9001:2015 quality management system, then all of your process policies, process descriptions and even the definition of evidence criteria and supporting documentation will be fluffy and indifferent, and no doubt equally heavy duty.

Within COSO or CobIT you have pre-described goal cascades that you can hang on balanced scorecard systems or KPI trees; within ISO you have to think of your own. You have to plan what you want, perform those activities, check the results and then you aim to improve your desired outcomes along a predefined scope.

So for this pattern, what is new in ISO 9001:2015? Well, what was maybe formerly assumed as a precondition is now defined as a clear requirement:

- State who your stakeholders are, focus on those drivers which drive your scope in the framework, and measure and improve your processes, procedures and outcomes along the value generation path.

## Recurring Pattern: Organisational Context

This links directly to the point referred to above. Organisations are driven by the interests of their stakeholders; Voice of the Customer is one of the key aspects. Here you concentrate more on understanding the whole organisation, so you always ask: What is this organisation doing? What is it delivering?

A clear idea of what an organisation wants to achieve is expressed in their vision and mission statements, on their codes of conduct, and most certainly in what should be a clearly structured set of product and service descriptions.

So an organisational unit seeking ISO certification has to deliver a presentation and description of what is delivered, under which overall principles, policies and rules this is done, and for which markets it is performed.

ISO/IEC 20000 requires a clearly defined service catalogue and processes for how the offering of services to customers and internal stakeholders are maintained, and how they provide input for the other enabling processes in order to deliver value within this context. ISO 9001:2015 with its statement in respect of valued goods and services is now re-adapting what was already clear for one of their children (i.e. ISO/IEC 20000).

So ISO 9001:2015 is a clear option for all those ‘hybrid’ organisations that use IT for their value chains, but do not stay in their data centres and interact only in a virtual way with their customers.

## Recurring Pattern: Domains and Process – Landscapes

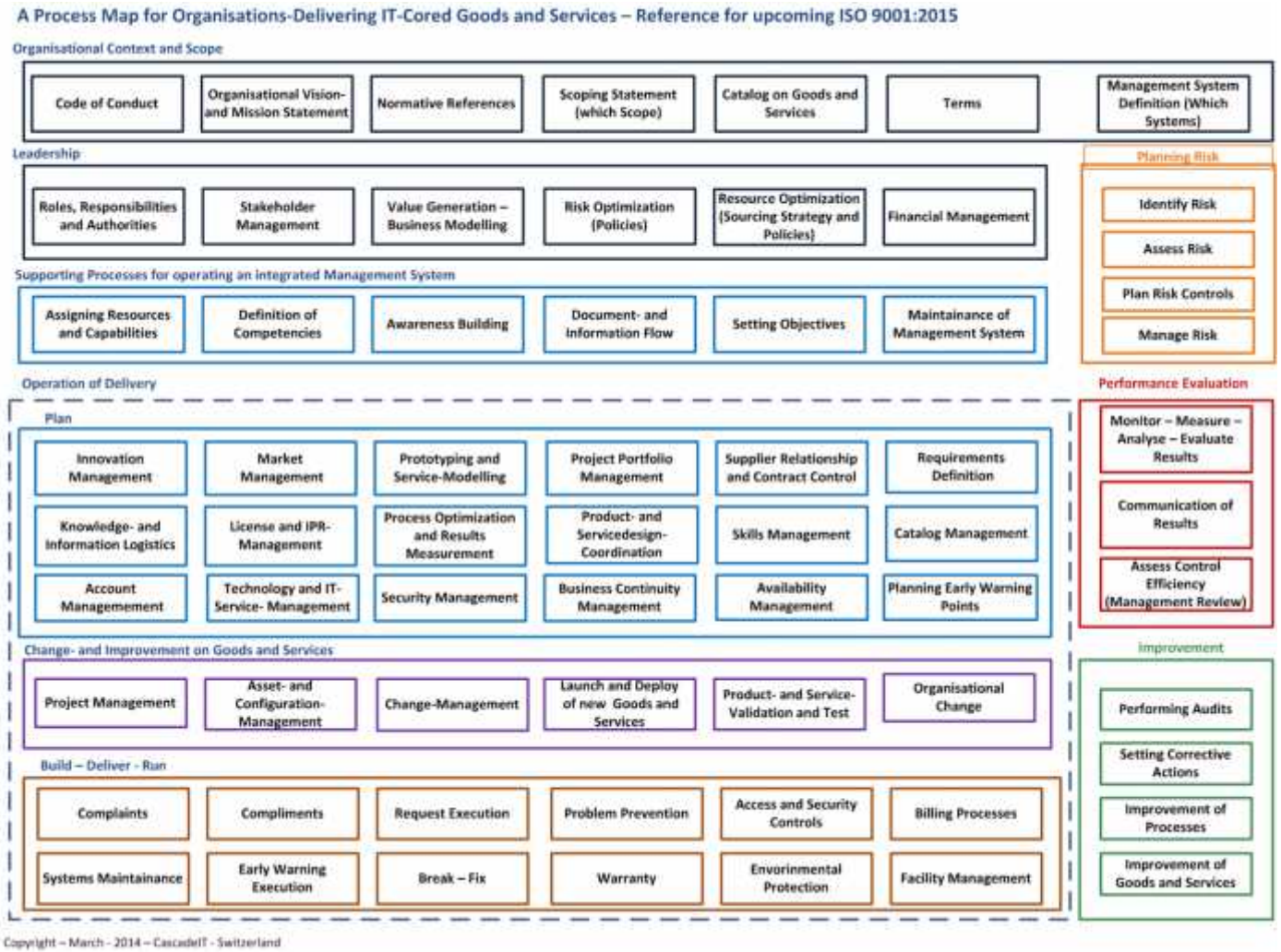
This statement may appear as satiric, but if you work with frameworks like ISO/IEC 20000 (somewhat aligned with ITIL®) or CobIT, then your emphasis in more on “reading after”.

If you want to work with ISO 9001:2015 then you are forced to think for yourself. But one of the key issues with its earlier brethren ISO 9001:2008 was the question of where to package all of the business processes which are relevant to delivering something?

There was only one chapter to cover all of this (Chapter 7), so the instrument of a process map was chosen as a mechanism to solve this implementation obstacle. And within ISO the following statement holds true:

- Everything which is not forbidden can be assumed as being allowed

Therefore drafting a process model containing the applicable domains and processes, and which should facilitate the design of a documentation structure supporting the requirements of an ISO 9001 quality management system, would be one option – and here it is:


A Process Map for Organisations-Delivering IT-Cored Goods and Services – Reference for upcoming ISO 9001:2015
Organisational Context and Scope
Code of Conduct
Organisational Vision- and Mission Statement
Normative References
Scoping Statement (which Scope)
Catalog on Goods and Services
Terms
Management System Definition (Which Systems)
Leadership
Roles, Responsibilities and Authorities
Stakeholder Management
Value Generation – Business Modelling
Risk Optimization (Policies)
Resource Optimization (Sourcing Strategy and Policies)
Financial Management
Supporting Processes for operating an integrated Management System
Assigning Resources and Capabilities
Definition of Competencies
Awareness Building
Document- and Information Flow
Setting Objectives
Maintainance of Management System
Planning Risk
Identify Risk
Assess Risk
Plan Risk Controls
Manage Risk
Operation of Delivery
Plan
Innovation Management
Market Management
Prototyping and Service-Modelling
Project Portfolio Management
Supplier Relationship and Contract Control
Requirements Definition
Knowledge- and Information Logistics
License and IPR-Management
Process Optimization and Results Measurement
Product- and Servicedesign-Coordination
Skills Management
Catalog Management
Account Managemement
Technology and IT-Service- Management
Security Management
Business Continuity Management
Availability Management
Planning Early Warning Points
Performance Evaluation
Monitor – Measure – Analyse – Evaluate Results
Communication of Results
Assess Control Efficiency (Management Review)
Change- and Improvement on Goods and Services
Project Management
Asset- and Configuration-Management
Change-Management
Launch and Deploy of new Goods and Services
Product- and Service-Validation and Test
Organisational Change
Improvement
Performing Audits
Setting Corrective Actions
Improvement of Processes
Improvement of Goods and Services
Build – Deliver - Run
Complaints
Compliments
Request Execution
Problem Prevention
Access and Security Controls
Billing Processes
Systems Maintainance
Early Warning Execution
Break – Fix
Warranty
Envorinmental Protection
Facility Management
Copyright – March - 2014 – CascadeIT - Switzerland

So as a starting point for the 'adopt and adapt' mantra for setting-up your own management or governance framework, then such process maps seem to be a valued instrument to simplify your implementation activities.

## Recurring Pattern: Scope – Principles – Policy – Process – Control – Evidence

This has been witnessed across frameworks as well. If you do not have a defined scope, principles and processes for your value driven and risk preventing activities then you cannot really measure effectiveness, efficiency and management control.

So if you set up the scope and organizational principles within your documentation in chapters 1 to 5 you have set-up the base for governing your organisation. Sounds simple I know, but it can prove a hard job if you do not plan and have pre-described paths and trails.

If there is a policy then there also needs to be structured activities to fulfil the policy requirements. Likewise, you have to consider controls or control mechanisms to check the fulfilment of these requirements.

The result should be documented and traceable evidence which shows that all what is in the documentation is fulfilled with real value driven deliverables.

The need for document structured evidence often leads to individuals and companies deciding against the ISO path with such questions as:

- How can I document all this in a timely manner?
- How can I ensure the content and evidence in my documentation as a management instrument?
- How can I prevent redundant effort in maintaining more than one framework with different scopes?

## Summary: The return on investment of using recurring patterns

Never change successful patterns. Re-use what has been defined before and concentrate on meeting the requirements with the 'why' and 'how' questions, as the 'what' content has been prepared before.

Even the thought leaders and experts of the governance and management framework generation do not have the energy and satisfaction in reinventing the wheel with every new iteration of their frameworks. Therefore, why not concentrate in the facilitation of structuring, documenting and presenting the content.

This saves time, cost and the risk of failing during the implementation because it provides:

- security
- trust in what is done
- lowering the cost of entry for achieving ISO certification
- quicker delivery and results
- momentum in overcoming the dips in moral in implementation projects
- increased concentration on the why and the how.

***Dr. Helmut Steigele***

*Director, Central Europe, Fox IT*

## About Fox IT

Fox IT® has been a leading Information Technology Service Management (ITSM) and governance business for over 30 years. We provide a range of practical and effective consultancy solutions designed to create agile, proactive, responsive IT organisations providing excellent IT services in alignment with our clients' goals to support and drive continuous business innovation. We achieve this by empowering your people with best practice training, developing and implementing the right operational processes and using properly configured and integrated tools to enable IT Services transformation.

To discuss how we can assist you in transforming your IT services or in obtaining ISO/IEC 20000 certification please call us now on +44 (0) 333 202 1018.

Please come and join in the latest ITSM conversations on our social media pages:

Facebook: www.facebook.com/FoxIT.ITSM

Twitter: @FoxIT_ITSM

LinkedIn Company Page: www.linkedin.com/company/fox-it

LinkedIn Group: https://www.linkedin.com/groups/Fox-IT-ITSM-Today-7456241/about