3-11-2009

Centralization issues in IT governance: The role and responsibilities of the IT Control Officer from a European perspective

Egon W. Berghout
e.w.berghout@rug.nl

Alea Fairchild
a.m.fairchild@eco.rug.nl

芽|Sprouts Working Papers on Information Systems ISSN 1535-6078

Centralization issues in IT governance: The role and responsibilities of the IT Control Officer from a European perspective

Egon W. Berghout
Alea Fairchild

Abstract
The need for transparency in IT governance, due to several factors such as cost and regulatory pressure, has led to organisations putting into place an IT Control Officer to oversee and audit IT activities. This paper examines the initial results of a European CIO-level survey designed to increase the understanding regarding the possible roles of the IT Control Officer and the authority given to that person. This research confirms the intuitive idea that increasing the role of the IT Control Officer also improves IT control. The increasing role in this sense is a more centralised and more senior position with additional responsibilities and administrative controls. This research also examines a perspective on the various intermediate possibilities of decentralised and less senior scenarios.

Keywords: IT Control IT Governance IT Organisation Information Systems Evaluation MIS Theoretical frameworks empirical research case studies corporate politics

Permanent URL: http://sprouts.aisnet.org/5-31

Reference: Berghout, Egon, Fairchild, Alea (2005). "Centralization issues in IT governance: The role and responsibilities of the IT Control Officer from a European perspective," University of Groningen, Netherlands . *Sprouts: Working Papers on Information Systems*, 5(31). http://sprouts.aisnet.org/5-31

citer

Centralization Issues in IT Governance: The Role and Responsibilities of the IT Control Officer from a European Perspective

Egon Berghout
Alea Fairchild

University of Groningen
Centre of IT Economic Research
P.O. Box 800
9700 AV Groningen
The Netherlands

CITER WP/002/EBAF

22 July 2005

CITER Mission

CITER is an independent research group within the Department of Economics, University of Groningen. Our research is focused on the economics of information technologies. Our research aims at understanding and analyzing the dynamics and the processes of development, distribution and implementation of information and communications technologies and improving their efficiency and effectiveness.

We investigate particular economic issues in the economics of information technologies. For instance, the differences between 'Open' and 'proprietary' technologies, the characteristics of hardware and software commercial demand and supply and the diffusion of new technologies. We also study the efficient and effective use of those technologies, how we can improve IT management and increase the benefits of investment in information technologies.

The objectives of our research are especially useful for organizations using information technologies and to firms competing in this arena, as well as to policy makers and to society as a whole.

Our research is conducted in close cooperation with industry, non-profit organizations and governmental partners, as our field of research is subject to frequent technological and political changes.

Contact information

University of Groningen
CITER-WSN457
P.O. Box 800
9700 AV Groningen
The Netherlands
Tel. +31-50-363-3721
info@CITER.nl

Projects and main venues of research

- Cost/benefit management of IT.
- Decision-support methods for implementation decisions within organizations.
- Evaluation of legacy systems.
- Innovation and technical change in ICT.
- 'Open' vs. 'proprietary' software modes of development.
- Software patenting and appropriation strategies.
- Tools and strategies for the IT Control Officer.

Sponsors

UWV

Getronics

Researchers

Prof. dr. E.W. Berghout	e.w.berghout@rug.nl
Drs. C.E. Elsenga	c.e.elsenga@rug.nl
Dr. A.F.M. Fairchild	a.f.m.fairchild@rug.nl
E. Harison, MEng.	e.harison@rug.nl
Dr. ir. M.H. Nijland	m.h.nijland@lse.ac.uk
Dr. T.J.W. Renkema	t.j.w.renkema@rug.nl
H. Sassenburg, MSc.	hsassenburg@se-cure.ch
Drs. E.J. Stokking	e.j.stokking@rug.nl
S. Orie, MSc.	Sieraadj@asset-control.com

citer

Centralization Issues in IT Governance: The Role and Responsibilities of the IT Control Officer from a European Perspective

Egon Berghout
University of Groningen
Centre of IT Economics Research
e.w.berghout@eco.rug.nl

Alea Fairchild
University of Groningen
Centre of IT Economics Research
a.m.fairchild@eco.rug.nl

Abstract
The need for transparency in IT governance, due to several factors such as cost and regulatory pressure, has led to organisations putting into place an IT Control Officer to oversee and audit IT activities. This paper examines the initial results of a European CIO-level survey designed to increase the understanding regarding the possible roles of the IT Control Officer and the authority given to that person.

This research confirms the intuitive idea that increasing the role of the IT Control Officer also improves IT control. The increasing role in this sense is a more centralised and more senior position with additional responsibilities and administrative controls. This research also examines a perspective on the various intermediate possibilities of decentralised and less senior scenarios.

Keywords: IT Control, IT Governance, IT Organisation, Information Systems, Evaluation, MIS, Theoretical frameworks, empirical research, case studies, corporate politics.

1. Introduction to IT Control

Increased pressure from regulatory legislation, concerns from both auditors and shareholders, and a renewed focus on enterprise security have contributed towards greater international focus on corporate governance, and therefore the associated aspects of IT governance. Section 404 of the Sarbanes-Oxley Act (SOX) requires auditors to evaluate a company's internal controls. SAS 94, *The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit*, emphasizes the importance of IT on internal controls and evidential matter.

Given a marked shift towards corporate transparency, IT governance trends focus on providing transparent control for the internal and external audit of IT procedures (IT Governance Institute, 2004), where IT control was defined as:

> *The policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and*

> *that undesired events will be prevented, or detected and corrected* [IT Governance Institute, 2004, p.10].

This paper examines the role of IT control in governance; specifically the role of an IT control officer within a corporate organization and the need for a specific IT controller in an organizational governance mechanism. This study includes IT governance interviews at several major European industrial organisations.

The structure of the paper is as follows: first, we provide background on IT control and the role of an IT Control Officer. Then we discuss the methodology of the research and the framework, which is based on contingency theory. Finally, we examine the research findings and end with a summary of the research and possible directions for future work.

2. Background

2.1 Definition of IT Control

Fayol defines government ('gouvernement'), as '*managing a business towards an objective using particular resources'* (Fayol, 1930). From these practices flows the organizations' direction, which dictates activities. The enterprise's activities use its resources. IT governance can be defined as "the organizational capacity exercised by the Board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT" (Van Grembergen, 2002). IT is also governed by best practices to ensure that the enterprise's information and related technology support its business objectives, its resources are used responsibly and its risks are managed appropriately.

IT best practices form a basis for direction of IT activities, which can be characterized from COBIT into four segments: (1) plan and organise, (2) acquire and implement, (3) deliver and support, and (4) monitor and evaluate. These practices both manage risks (to gain security, reliability and compliance) and help realize benefits (increasing effectiveness and efficiency)(COBIT Student Book, 2004). In this regard, IT control can be seen as the mechanisms or assurances that allow governance to work. IT control frameworks enable best practices for IT actions, processes and monitoring within organisations, and are believed to lead to more effective IT governance (Warland and Ridley, 2005).

In 1996, the Information Systems Audit and Control Association (ISACA) published the first version of *Control Objectives for Information and Related Technology* (*COBIT*), now in its 3rd edition. COBIT is designed to provide a framework of generally applicable and accepted IT control practices that can be used to evaluate an organization's current and planned IT environment. The COBIT framework is intended to be useful to management and users (business process owners), in addition to auditors. For management, users, and auditors, COBIT establishes a framework to evaluate IT investments and risks, as well as providing assurances that IT-related business objectives are achieved. COBIT strengthens the understanding, design, exercise and evaluation of internal controls (Fedorowicz and Gelinas, 1999).

2.2 Definition of IT Control Officer

In our research, we define an IT Control Officer to be: "*an employee who is responsible for the financial control over IT functions*". We focus on financial control as financial flows are how most organizations define their risk and investment strategies. The role of an IT Control Officer is to utilise a control framework, which includes tools and processes, to manage risk and create benefits from the IT investments and usage.

Meta Group in 2002 suggested IT executives can enhance strategic value by establishing an IT controller role (Bushell, 2002). Meta Group believed that the IT controller role "will expand from a tactical, internal IT budget watchdog, to a strategic business collaborator and liaison, often with dotted-line reporting to the corporate CFO." Meta Group notes that "an empowered IT controller can better align IT initiatives and budgets with business objectives and metrics, ensuring compliance with financial and accounting practices, reporting and visibility."(Bushell, 2002).

Where someone who holds this role may fit within the reporting structure could be either at the Board of Directors level, or at the business unit level, depending on the centralization of ICT within the corporation and the diversity of the organizational portfolio.

The kinds of processes and tools used by this individual may be based on the formalised or informal structures of IT evaluation of the organization. Much of the literature on IT evaluation takes a formal-rational view and sees evaluation as a largely quantitative process of calculating the likely cost/benefit on the basis of defined criteria (Walsham, 1993).

2.3 Business Rationale for IT Control Officer

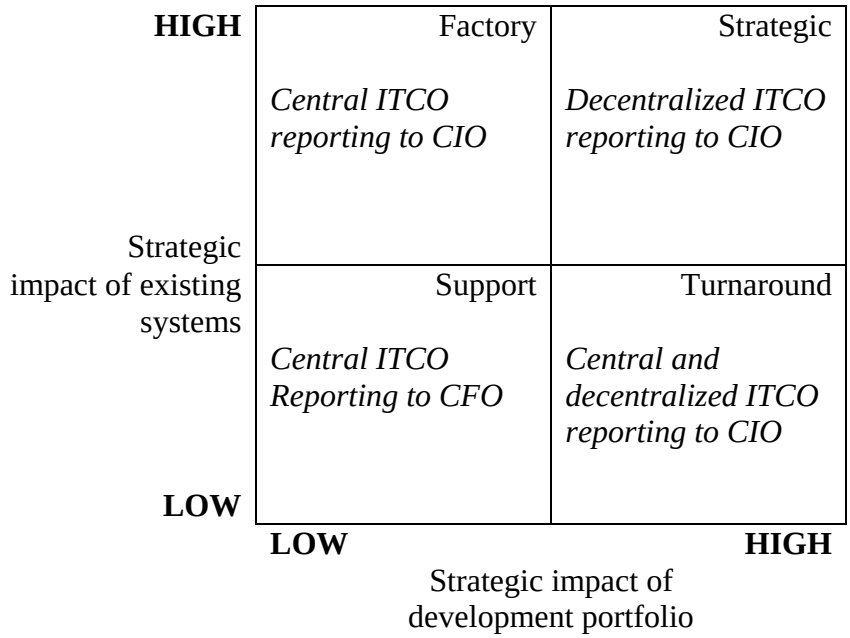
In terms of business strategy, an IT Control Officer can be seen as a functional responsibility and would be required in cases where the various IT control activities are not adequately addressed by others (CIO/project management) and where major improvements may still be possible. These would be cases where the benefits could outweigh overall organizational cost. Substantial business dynamics and potential IT savings are essential here.

Part of the need for the IT Control Officer is that the CIO and CFO responsibilities can overlap. A CIO is responsible for the overall IT function, defined as the alignment of business and IT, efficient use of IT resources, and IT risk management. The CFO is responsible for the financial function e.g. administrative activities and financing. In many organizations IT is an important cost driver and an important tool for the financial function.

In a stable environment, it is, therefore, logical to make the CFO responsible for IT. The IT Control Officer could also report to the CFO. Increasing business dynamics and technological dynamics (as well as potential IT cost savings) also increase the

importance of the CIO/IT Control Officer (ITCO) relationship. These dynamics could be linked to McFarlan/McKenney's 'Strategic Grid', as shown in Figure 1.

Figure 1. Adapted McFarlan/McKenney's 'Strategic Grid' on CIO/CFO relationship to IT Control Officer



An IT Control Officer is responsible for the financial assessment of the IT function: identifying and controlling the major cost and benefit categories. This concerns:

1. Strategic management tasks:
    a. Investment analysis policy.
    b. Business case requirements specification.
    c. Supporting the investment appraisal process.
2. System development tasks:
    a. Portfolio management
    b. Implementation management
    c. Project evaluation management
3. Operational Management:
    a. Charge-out management and IT transfer pricing
    b. IT asset management and sourcing
    c. Benchmarking
    d. Legacy management

The decentralized IT Control Officer is more focused to system development control and evaluation. The centralized IT Control Officer is more focused to overall IT cost control, sourcing and benefit management.

Therefore, the need in organization for an IT Control Officer role may depend on several aspects of the organization, including organizational structure, reporting mechanisms, experiences with ICT, and regulatory pressures.

2.4 Framework Using Contingency Theory and Organizational Drivers

In examining the need for an IT control officer, this research uses contingency theory based on the logic that contingency theory is one of instrumental utility, or the premise that decision-makers rationally strive to align their organizations with situational conditions, and that their organizations benefit to the degree the alignment is achieved (Lawrence and Lorsch, 1967; Donaldson, 2001). Contingency theory is based on the premise that the suitability of a structure depends on the situation (Donaldson, 2001), including environmental conditions (Burns and Stalker, 1961), organizational size (Child, 1975), and strategy (Chandler, 1962; Miles and Snow, 1978). A contingency perspective has been applied to explain a wide array of organization design variables, but it is most often associated with explaining organizational structure, such as the adoption of the divisional form, structural differentiation, formalization, and decentralization (Donaldson, 2001).

There are several drivers for firms to examine IT audit and control at this time in industry. One driver is cost reduction, both by less people employed and by less transaction cost for the information flow of the organization. Research on IT value such as the work of Brynolfsson (1993) have shown us that IT investments have traditionally not created benefits through cost reductions but they can, however, transform the organisation's cost structure through intangible benefits, such as greater communication and streamlining of processes.

Another primary driver in IT governance is regulatory policy, starting with provisions of the US Sarbanes-Oxley Act (SOX) of 2002 that require corporate management to assure investors and satisfy audit committees about the adequacy of operational controls (COBIT Student Book, 2004). Tools such as control self-assessment (CSA), also referred to as control self-assurance, are extensions of the internal control mechanism. CSA is a tool designed first by COSO[1] to assist in the internal audit function, and to test the effectiveness of internal controls. CSA also ensures that employees are aware of the risks to the business and they conduct periodic proactive reviews of controls. CSA is an effective tool for successful implementation of IT governance. Considering the security incidences, limited internal audit resources and requirements of SOX, CSA will help medium and large organizations build security consciousness among IT users and will provide a mechanism to comply with the Act's provisions.

3. Research Objective and Approach

The purpose of this research is to more clearly identify the IT control function in organisations, including the use of an IT Control Officer. In our research, we define an IT Control Officer to be: *an employee who is responsible for the financial control over IT functions*.

This includes reporting aspects in the organisation, structure and type of organisations that utilize IT control activities, and major responsibilities of the IT control function.

In this research, we conduct a set of exploratory interviews with top IT executives in large corporations to examine alternative structural arrangements of IT control, with

[1] Committee of Sponsoring Organizations

an initial hypothesis based on contingency theory that certain factors will affect the likelihood that an IT control officer will exist in the organization and where they would be in the reporting structure.

Our hypotheses, based on our assumptions shown in Table 1, discuss how under particular circumstances an organization should choose for a particular type and organizational position of the IT Controllers.

This can be further defined into two parts, based on both literature and the objective of an IT Control Officer:

Hypothesis 1a*: The more centralised the organization, the more likely it will have an IT Control Officer.*

Hypothesis 1b: *The more diverse the business portfolio the firm has, the less centralized IT control will be, but then a high level IT executive will likely exist at the headquarters level.*

Contingency theories are a class of behavioral theory that contend that there is no one best way of leading and that a leadership style that is effective in some situations may not be successful in others. Contingency theory takes a broader view than situational theory in that it includes contingent factors about leader capability and other variables within the situation.

Table 1. Elements in organziation that may impact need for IT Control Officer

Elements	Includes	Impact on need for IT Control
IT control maturity	ICT experience, number of COBIT areas which are covered	More experience, less need for a specific IT control function, likely handled at the business unit level
Technical dynamics	Overall IT experience, risk management	Less ICT previously covered, more IT control required.
Business dynamics	Diversity of business portfolio	Higher diversity -> less centralized control, but then a high level IT executive at the headquarters level
Organizational structure	Centralised, decentralised, federated, other alternatives	More centralised, more likely to have an IT Control Officer
Pressure due to legislation and shareholders	SOX, SEC, transparency of activities for shareholders	The more publicly visible a firm is, the more likely they have someone in a IT Control Officer role.

4. Methodology of Interviews

The aim of this section of the paper is to describe the research method applied during this phase, before summarizing the results of the exploratory study. It should be noted, that as we are currently extending the size of the sample, this paper represents a progress report, rather than the finished product. This study concerns a research in-progress, as not all the research results could already be included in this paper.

A set of questions was developed based on both the COBIT research framework and the hypotheses on contingency theory and organizational structure. The questions were conceived from the standpoint that an IT Control Officer would be involved in COBIT implementation and reporting of risk to the organization's Board.

The questions were focused on three core components of the organization's control framework:

1. Implementation of COBIT, using the four main domains and assessment of COBIT maturity in the organization;
2. Importance of IT control in the organization, as shown by governance structure and level of reporting for IT control in organization;
3. Design of IT control in the organization, as demonstrated by framework, tools and assessment processes used for control.

The initial set of surveys were limited to seven large corporations in several industries to test the hypothesis for further research. Table 2 outlines the breakdown of the initial interviews.

Table 2. Initial Interviews [Nov 2004- Feb 2005]

Firm	Industry	Location
KPN	Telecom	The Netherlands
Corus	Steel	The Netherlands
UWV	Not for Profit social organization	The Netherlands
GEA	IT Services	Germany
Vattenfall	Utilities	Sweden
TDC	Telecom	Denmark
Akzo Nobel	Pharmaceutical	The Netherlands

5. Survey Findings

The aim of this section of the paper is to present a summarized review of the results of the exploratory, empirical analysis. We also address how the findings address our initial hypotheses. This analysis focuses primarily on the three core components of implementation, importance and design of IT control, examining the role of the IT Control Officer in these areas.

In our conclusion in the following section, we examine these findings in light of our initial hypotheses and our previous discussion on the definition of the role of the IT Control Officer as a function of organizational and technological dynamics.

5.1 COBIT Implementation

Overall, all seven firms were active in using COBIT in the organization. However, for many it was a recent implementation within the last two years with the main driver being SOX.

In assessing the level of control assessment in the organization, the seven firms were asked where on the COBIT maturity model they saw their organization witin the four domains of planning and organization, acquisition and implementation, delivery and support, and monitoring. Half of them felt that acquisition and implementation was the weak spot, based on the need for control of specific IT projects.

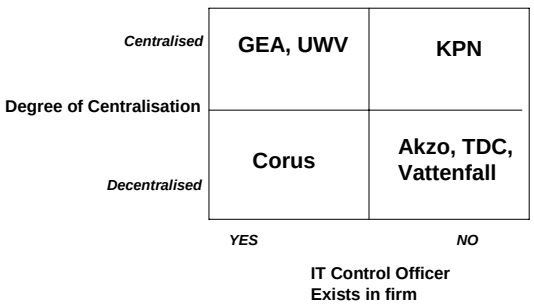
The main issue for COBIT and IT control was not what areas were not covered within COBIT, but who was in charge of the implementation. This was a related to whether or not the firm used an IT controller in a centralized function, or if IT control came under the auspices of individual business units. This was not seen as a function of the technology governance structure but an echo of the corporate governance structure.

5.2 Organization and Importance of IT Control

One of the questions was asking about the technology governance function in the organization, asking if the configuration was centralised, decentralised, federal (a mix of the first two where infrastructure is centralized) or another form of organization. Five of the seven firms have a federal structure, with the other two having hybrid organizations that are slightly different to a federal structure. However, these organizations do lean either one way or the other in respect to centralisation.

For *Hypothesis 1a*, when we segment these federalised and hybrid structures into two categories of either more decentralised or centralised in respect to IT governance, based on their answers to the COBIT questions about who handles what IT functionality, we find three more centralised and four more decentralised in polarity. If we then compare the existence of an IT control function to this described organizational structure of the firm, we get the pattern shown below in Figure 2:

Figure 2: Correlation of organizational structure to presence of IT Control Officer



Even with a small sample size, most decentralised firms did not have a defined IT contol officer function, whereas it was more likely that a centralised firm had someone in charge of the IT control function.

For *Hypothesis 1b*, the interesting question was whether they had an IT Control Officer and where that IT Control Officer should report in the organization.

Figure 3: Correlation of organizational portfolio to presence of IT Control Officer

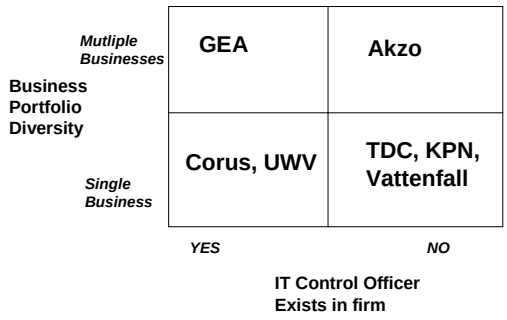


Figure 3 shows that the multiple businesses had a certain degree of centralization of the IT control function, but it was more of an issue of how focused on both the application diversity and the level of IT governance the overall business had, based on certain regulatory pressures (e.g. SOX). Looking at all the firms, for the ones that did not see an IT Control Officer in their organization, they saw that functionality reporting at the IT Director level (e.g. not a financial aspect, more of a technological reporting structure). The others who did have someone in that function either felt it was a Board level report, or a Divisional Head report (where decentralization was occurring), as this role was working in collaboration with the business strategy aspects of the firm. Again, this differentiation on reporting structure appears to be a function of corporate governance and strategy more than technological governance.

5.3 Importance of IT Control

Most of the firms also felt that financial control of IT was fairly important in the organization (median: 4 out of 5, 5 being highest), but not all were that satisfied with the current level of control, with one firm being fairly unhappy with this at a 2 out of 5 (a 1 was not satisfied).

Given as previously mentioned that half of them felt that acquisition and implementation activities in COBIT was their weak spot, this could be a related comment, which could be tested in future research.

5.4 Design of IT Control

The questions asked in regards to the design of IT control mechanisms covered internal frameworks used, tools and assessment processes to evaluate IT investments, and benchmarking activities the organization employed.

Internal frameworks used by these firms include all major approaches standard in industry, but with transfer pricing, quality management systems and

hardware/software depreciation being the least frequently to be used for managing IT control. Tools and assessment processes usually included the use of business case evaluations, financial indicators and evaluation of organizational requirements. Measurement of productivity always included SLAs and other financial metrics (ROI, ROE), and usually measures that tied to business unit performance. The fundamental finding is that there was no one metric that they did not use – most claimed to use all tools, but to quote one respondent: "not as well as they would have liked".

Benchmarking was done externally by five of the seven firms, with the other two focusing more on internal benchmarking activities. Outsourcing for both procurement and IT control was the trend seen amongst these seven firms, with cost efficiency and governance seen as the main drivers.

6. Conclusions

Table 3 highlights the findings from the initial interviews towards our first hypotheses based on contingency theory.

Table 3. Elements assessed from initial interviews

Elements	Initial thoughts on need for IT Control	Comments based on Findings
IT control maturity	More experience, less need for a specific IT control function, likely handled at the business unit level	Most reasonably chronologically young in IT control frameworks, still had a mix of business unit control (for implementation) and IT centralization (for aspects of acquisition, monitoring)
Technical dynamics	Less ICT previously covered, more IT control required.	Not enough data to conclude – most firms fairly IT knowledgeable or IT-based (telecom, pharmacy)
Business dynamics	Higher diversity implies less centralized control, but then a high level IT executive at the headquarters level	More an issue of diversity of IT portfolio, more control / audit needed centrally when organization is diverse.
Organizational structure	More centralised, more likely to have an IT Control Officer	Most of a Federal structure, level of decentralised control a factor in IT Control Officer adoption
Pressure due to legislation and shareholders	The more publicly visible a firm is, the more likely they have someone in a IT Control Officer role.	The firms that did not have a IT Control Officer were either reasonably new to SOX (immature in adoption) or globally spread-out enough that this was already covered in another way in the firm (mature infrastructure).

Four of the seven organisations involved in this study had (recently) appointed an IT Control Officer. There seems to be little difference between the applied control mechanisms and the existence of the IT Control Officer. In both cases the same set of techniques are applied. However, in the organisations that do employ an IT Control Officer, this person was primarily reporting at the level of the Board of Directors. We therefore conclude that the *level of control* is substantially higher in the situation where an IT Control Officer exists.

This research, therefore, confirms the well-known notion that control increases both through the establishment and seniority of the IT Control Officer(s) and through positioning this person outside the IT organisation and closer to the board. This also matches our previous discussion on the business rationale for using an IT Control Officer as our more centralized firms used a ITCO and were more focused to overall IT cost control, sourcing and benefit management.

Legislation seems to be the main driver to establish an IT Control Officer. *Business dynamics* and *technological maturity* seem to be the most prominent variables to determine the position of the IT Control Officer in the organisation. Increasing organisational complexity lowers the position IT Control Officer and brings this position closer to the operations. Technological immaturity brings the IT Control Officer outside the IT function.

Most tools available to the IT Control function were already in use in the organizations, with an emphasis on the empirical aspects of control versus more qualitative functions such as quality management.

Future directions for this research is to further test the contingency theory framework on a large number of organisations, with both manufacturing and service industries.

7. References

Brynolfsson, E. (1993) The Productivity Paradox of Information Technology, *Communications of the ACM*, 35, 66-77.

Burns, T. and Stalker, G.M. (1961) *The Management of Innovation*. Tavistock: London.

Bushell, S. (2002) “Learning From Disaster | Part Two - Transparently Obvious”, *CIO*, Online edition, 11/11/2002. Retrieved April 7, 2005, from: http://www.cio.com.au/index.php/id;783755622;fp;4;fpid;14

COBIT Student Book (2004). Retrieved April 16, 2005 from URL: http://www.isaca.org/Content/NavigationMenu/Students_and_Educators/Academic_Relations/COBIT_in_Academia/Cobit_SAMPLE_Student.pdf

Chandler, A.D. (1962) *Strategy and Structure: Chapters in the History of the American Industrial Enterprise*. MIT Press: Cambridge, MA.

Child, J. (1975) "Managerial and organizational factors associated with company performance". *Journal of Managerial Studies* **11**: 174–189.

Donaldson, L. (2001) *The Contingency Theory of Organizations*. Sage: Thousand Oaks, CA.

Fayol, H., *Industrial and general administration*, IMI, Geneva, 1930.

Fedorowicz, J. and Gelinas, Jr.U. (1999). "Adoption and Usage Patterns of an IT Audit and Control Framework", Proceedings of the XXth AMCIS conference.

IT Governance Institute, "COBIT 3 Edition Executive Summary", Available at: http://www.isaca.org/execsum.pdf, Accessed: June 22, 2004, 2000.

Lawrence, P.R. and Lorsch, J.W. (1967) *Organization and Environment*. Graduate School of Business Administration, Harvard University: Boston, MA.

Miles, R.E. and Snow, C.C. (1978) *Organizational Strategy, Structure, and Process*. McGraw-Hill: New York.

Walsham, G. (1993) *Interpreting Information Systems in Organisations*, Wiley & Sons.

Warland, C. and Ridley, G. (2005). "Awareness of IT Control Frameworks in an Australian State Government: A qualitative case study", Proceedings of the 38th HICSS Conference, Kona, Hawaii.

芽|Sprouts

Working Papers on Information Systems | ISSN 1535-6078

Office:
Sprouts
University of Amsterdam
Roetersstraat 11, Room E 2.74
1018 WB Amsterdam, Netherlands
Email: admin@sprouts.aisnet.org

芽|Sprouts