



intoit

Issue 29 | February 2010



Come together

In this issue



Australia

Country focus

4

Australia

Data Analysis in Australian Government audits

10

Brazil

Information security at the Brazilian Court of Audit:
complying with our own recommendations

12

China

Sharing Audit experiences from one auditor to the others

18

EUROSAI Survey

IT audit in EUROSAI IT-working group countries

20

Scandinavia

Information Security audits in the Nordic countries

22

Pakistan

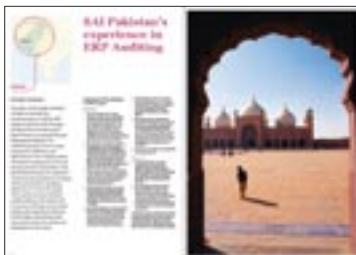
SAI Pakistan's experience in ERP Auditing

26

Switzerland

The Swiss ICT project management method

38



Editorial



Nigel Salt
Interim Editor

Welcome to issue 29 of Into IT we are grateful to all contributors to this issue which outlines the achievements of some INTOSAI members in countering the threat to deliver better services safely.

Organisations depend on the security of the information they hold and access to information about the environment they operate in.

The findings of the information system security conference of the Nordic SAIs, reported in this edition, highlight the wide range of issues that need to be addressed in a co-ordinated way in order to reach an adequate level of security. The international community has responded by developing the ISO 27000 series of security management standards which form a sound basis for a minimum level of security to be implemented by organisations and their partners. The ISO series addresses one part of the wider subject of information system governance. Achieving sound governance involves security but also involves implementing best practice in designing, developing and running effective information systems. To complete the set of best practice guidance it is now common to refer to the Information Systems Audit and Control Association (ISACA) Control Objectives for IT (COBIT), the IT Infrastructure Library (ITIL) and Projects in a controlled environment (PRINCE).

Effective electronic services rely on the integrity of the information on which they are based. One key challenge to integrity is holding information about clients in multiple places. Commercial audit tools such as IDEA (see ANAO article on data analysis) and ACL or the freeware Picalo (<http://www.picalo.org/>) can be used to help organisations and their auditors to test for conflicts or mistakes in the data held and may also highlight fraud.

Effective information systems are notoriously hard to deliver. Use of a sound development framework such as the Hermes method set out in the Swiss article in this edition is an essential part of ensuring that requirements are captured and that the development process proceeds smoothly to deliver the outcomes that the sponsor of the system envisaged.


Information systems work best when they can share data across system boundaries and automate the process of prompting users to take the actions necessary to complete a business process. Enterprise Resource Planning (ERP) systems grew out of this observation. Implementing ERPs such as SAP or Oracle is not a simple process and often requires massive organisational and security changes. The article from Pakistan in the current edition highlights their experience of the implementation of SAP and illustrates the challenges involved. SAP consultants often observe that it is easier to redesign the organisation to fit the way SAP works than to customise SAP.

The article from SAI China highlights the value to be gained from the auditor using IT as a tool to help meet audit objectives and makes the point that it takes time and skill to develop effective audit applications. Getting best value from the development of audit methods and tools to support them requires a mechanism for sharing the results with other auditors.

We would like to take this opportunity to announce some exciting developments. Volumes, resource costs and environmental impacts of printing documentation are generally rising. To help counteract this trend this will be the last printed version of INTO IT as we are moving to electronic copies only from issue 30. Would any INTOSAI colleagues unable to access on-line material routinely please let the editor know. Also, after serving as the editor of INTO IT for many years, the UK NAO has decided that it is time for us to hand on that baton. We will therefore be looking to stand down after INCOSAI 2010 and we would like to invite another SAI to take on the role of editor. It is an interesting and rewarding role and one that adds considerable value and interest to the work of INTOSAI's IT professionals and other colleagues alike. Again would any INTOSAI colleague interested in taking on the role of editor of INTO IT please let us know.

For now though please continue sending your articles to intoit@nao.gsi.gov.uk. We are happy to receive these at any time and provide any help and guidance required to make sure that your article gets published to the best advantage especially where English is not your first language.

We look forward to hearing from you.



IntoIT is the journal of the INTOSAI Working Group on IT Audit. The journal is normally published twice a year, and aims to provide an interesting mix of news, views and comments on the audit of ICT and its use in Supreme Audit Institutions (SAIs). Material in the journal is not copyrighted for members of INTOSAI. Articles from intoIT can be copied freely for distribution within SAIs, reproduced in internal magazines and used on training courses. The Editor welcomes unsolicited articles on relevant topics, preferably accompanied by a photograph and short biography of the author, and short news items for inclusion in future issues.

The views expressed by contributors to this journal are not necessarily those of the editor or publisher.

Contributions should be sent to:

The Editor of intoIT

National Audit Office

157-197 Buckingham Palace Road

London SW1W 9SP

United Kingdom,

E-mail: intoit@nao.gsi.gov.uk, Web site: www.intosaiitaudit.org



AUSTRALIA

Australian and ANAO Facts

Australia is, in geographical terms, the sixth largest country in the world. It is almost as large as the continental United States of America (excluding Alaska and Hawaii), about twice the size of the European Union, and 32 times greater than that of the United Kingdom.

Australia's coastline stretches almost 50,000 kilometres and is linked by over 10,000 beaches, more than any other country in the world. More than 85 per cent of citizens live within 50 kilometres of the coast, making it an integral part of the Australian lifestyle.

Country Focus **Australia**





History of the ANAO

When the first Commonwealth Parliament assembled in May 1901, its immediate task was to begin building the necessary institutions of national government. The fourth Act passed by this Parliament was the Audit Act 1901, which created the office of the Auditor-General.

The *Auditor-General Act 1997* (which replaced the Audit Act) was enacted in October 1997 and marked a new era for the Australian National Audit Office (ANAO). The Office's audit independence and mandate were strengthened and the Auditor-General became an 'Officer of the Parliament'.

The ANAO mandate covers all government entities, including audit of their financial statements and a broad performance audit program.

The ANAO has a special relationship with the Joint Committee of Public Accounts and Audit (JCPAA). The JCPAA takes particular interest in the role and functioning of the ANAO and is required to review all audit reports tabled in the parliament.



In 2001 the ANAO celebrated 100 years as a Commonwealth institution. To commemorate this milestone the ANAO commissioned a documented history, which was published as: *From Accounting to Accountability: A Centenary History of the Australian National Audit Office*. The ANAO has a head office based in Canberra with a small regional office located in Sydney. Approximately 340 staff are now employed within the Office.

Australian Statistics

Population	21.9 million
Area	7,692,024 sq km
Population density	2 people per sq km
National Capital	Canberra, Australian Capital Territory
Regions	Divided into six states and two territories. States: New South Wales Victoria Queensland Tasmania South Australia Western Australia Territories: Australian Capital Territory Northern Territory
Life expectancy	Men: 79 Women: 84
Highest peak	Mt. Kosciuszko (2,228 m)
Longest River system	Murray-Darling (3750 km)
Internet top-level domains	Australia: .au Government: .gov.au

Religions	Catholic: 26.6% Other Christian: 20.6% Anglican: 20.7% Buddhism: 1.9% Islam: 1.5% Other religions: 1.5% No religion: 27.2%
Languages	English is Australia's national language. The cultural diversity within the population has resulted in over 200 languages being spoken in the community. There are more than 60 different languages spoken by Aboriginal and Torres Strait Islander Australians.
Indigenous statistics	The estimated resident Indigenous population at 30 June 2006 was 517,200 people, or 2.5% of the total Australian population. In the period 1996-2001, life expectancy at birth was estimated to be 59.4 years for Indigenous males and 64.8 years for Indigenous females.
Country of Birth	In 2006 the number of overseas-born Australians reached five million, representing almost a quarter (24%) of the total population. The top six countries represented are: Great Britain, New Zealand, Italy, China, Vietnam and India.



Integrated Financial Statement Auditing

In Australia, under section 57 of the Financial Management and Accountability Act 1997 (FMA Act) the Auditor-General is required to report each year to the relevant Minister, on whether the financial statements of agencies have been prepared in accordance with the Finance Minister's Orders (FMOs) and whether they give a true and fair view of the matters required by those Orders.

A central element of the ANAO's financial statement audit methodology, and the focus of the interim phase of our audits, is a sound understanding of an agency's internal controls. To do this, the ANAO uses the framework contained in the Australian Auditing Standards ASA 315 (Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement). The key elements of internal control are the control environment; the risk assessment process; information systems, including the related

business processes relevant to financial reporting, and communication; control activities and monitoring of controls.

The ANAO auditors obtain an understanding of the internal control over financial reporting, evaluate the design effectiveness of controls, test and evaluate the operating effectiveness of the controls and the control weaknesses and form an opinion on the effectiveness of the internal controls over the financial reporting.

All ANAO findings are reported to agency management and summary reports provided to the relevant Minister(s). In addition, our audit processes provide for audit issues identified to be formally reported to agency Chief Executives and their respective Audit Committees.

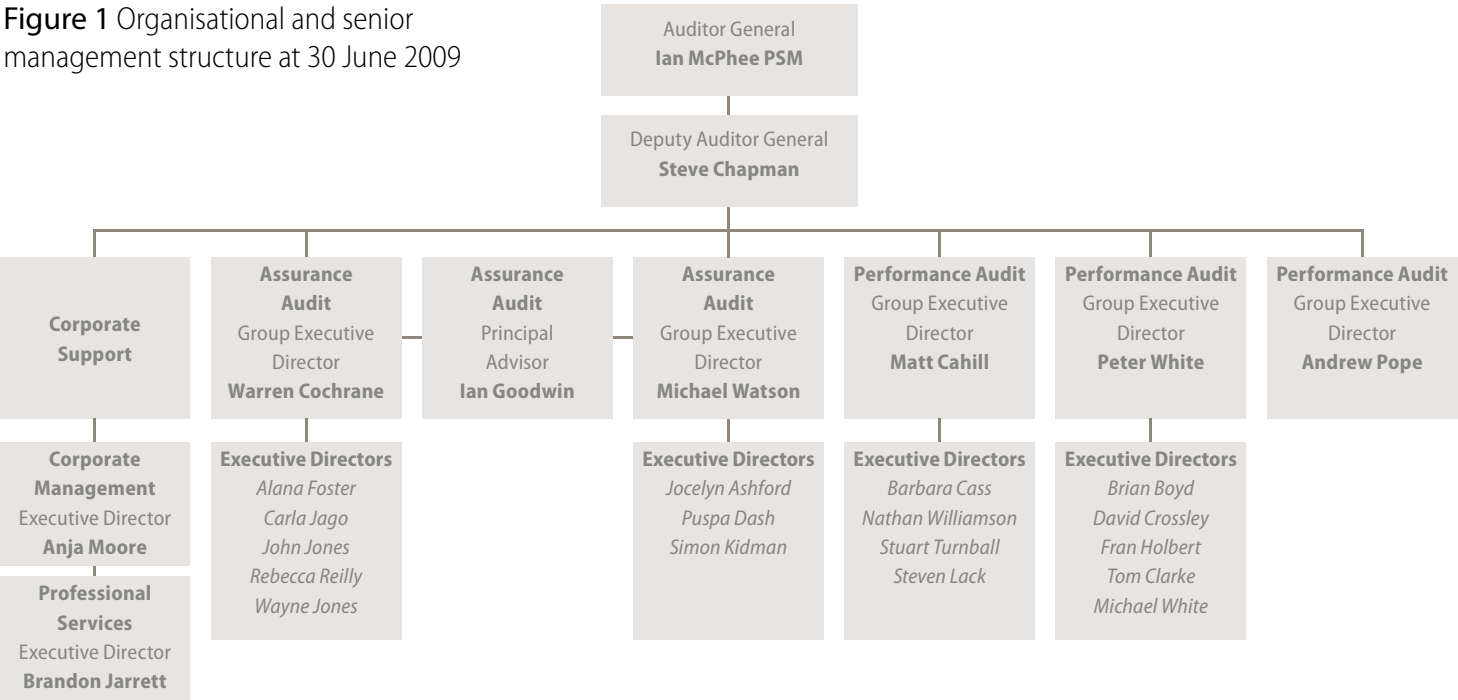
Observations relating to various elements of agencies' internal controls (including the control environment, the risk assessment process, control activities and monitoring of controls) are discussed in summary.

Control Environment

The ANAO assesses whether an agency's control environment includes measures that contribute positively to sound corporate governance in the context of the preparation of an agency's financial statements. These measures should be designed to mitigate identified risks of material misstatement in the financial statements, and reflect the specific governance requirements of each agency.

The Certificate of Compliance process, introduced in 2006-07, involving a mandatory control self assessment and breach disclosure process, has resulted in an ongoing focus on wider compliance issues.

Figure 1 Organisational and senior management structure at 30 June 2009



Synopsis of 'From Accounting to Accountability: A Centenary History of the Australian National Audit Office'

The ANAO remains a fundamental institution of public accountability in the Commonwealth of Australia.

Established in 1902 to perform a relatively limited function, the Audit Office built on its initial role of verifying the public accounts and extended its mandate gradually improving the ways governments are held to account.

Successive Auditors-General have strenuously fought for their independence from government and the bureaucracy, and also felt the need to defend their mandate at particular times. In 1997 the Auditor-General was declared an Independent Officer of the Parliament, to protect the independence of the Office and express a closer working relationship to the Parliament.



Australia's Financial System and Regulatory Framework

Financial systems

The financial system in Australia has three overlapping components.

The first consists of financial enterprises (e.g. banks) and regulatory authorities (the Reserve Bank and the Australian Prudential Regulation Authority (APRA)).

The second consists of financial markets (e.g. the bond market) and their participants (issuers such as governments, and investors such as superannuation funds).

The third is the payments system (i.e., the cash, cheque and electronic means by which payments are effected) and its participants (e.g. banks).

The interaction of these three components enables funds for investment or consumption to be made available from savings in other parts of the national or international economy.

Regulatory Framework

From 1 July 1998, a new financial regulatory framework came into effect. Under the new structure, a single prudential supervisor, (APRA), was established to take responsibility for the supervision of banks, life and general insurance companies, and superannuation funds. The Australian Securities and Investments Commission assumed responsibility for market integrity and consumer protection across the financial system. The Reserve Bank retained responsibility for monetary policy and the maintenance of financial stability, including stability of the payments system.

Risk Assessment Process

An understanding of an agency's risk assessment framework is an essential element of the ANAO's financial statement audits. Agencies are expected to manage the key risks specific to their environment and our interim audits include a review of controls relating to risks that may have a material impact on agencies' financial statements. The ANAO found that the majority of agencies have a well-established risk assessment process and the results are generally reviewed by audit committees.

Information Technology

Information technology (IT) facilitates the way in which Australian Government agencies operate, and supports the business processes that deliver services to the Australian community. The ANAO noted improvements in a number of agencies' IT control environment; most noticeable has been the implementation of more effective IT security, incident and problem management procedures. These improvements have enhanced the overall level of security and integrity of key financial systems.

ANAO's IT Audit works in close collaboration with the financial statement auditors and assists them to gain reasonable assurance over their audit of the government entity's preparation of the financial statements.

ANAO IT auditors' review of the internal controls and application reviews of the financial statement preparation process provide assurance to the financial statement auditors, who in turn may choose to perform substantive tests as necessary to gain the required level of confidence over the financial statement line items reporting.



Findings relating to the audit of technology systems focusing on the IT control environment, IT security, systems delivery and application controls in financial management and human resource management information systems are discussed with the clients.

Control Activities

ANAO's interim phase of the audit of financial statements of general government sector agencies encompass a review of governance arrangements related to agencies' financial reporting responsibilities, and an examination of relevant internal controls, including IT system controls.

An examination of such issues is designed to assess the reliance that can be placed on internal controls to produce complete and accurate information for financial reporting purposes.

The results of the Audit Report, 'Interim Phase of the Audit of Financial Statements of General Government Sector Agencies for the Year ending 30 June 2009', indicated that, overall, control activities relating to financial and accounting processes have been maintained at an effective level.

Monitoring of Controls

Many activities undertaken by an agency contribute to their regime of monitoring controls. These include quality assurance arrangements, internal and external reviews, control self-assessment processes, and Internal Audit. The ANAO noted that control self-assessment arrangements, first introduced by a number of agencies to assist in meeting their responsibilities to provide a Certificate of Compliance has become an integral part of agencies' control regimes. Internal Audit was also continuing to have a key role in some agencies in assisting in the Certificate of Compliance process.



End to end electronic transactions and emerging technologies

Government agencies are increasingly conducting their business transactions electronically through dedicated communications lines or the Internet. In response to the increased use of computers and other information technology, many government entities process significant information electronically.

Source documents are increasingly being replaced by electronic messages. In image processing systems, documents are scanned and converted to electronic images to facilitate storage and reference, and the source documents may not be retained after conversion.

The Australian Auditing Standard ASA 500 'Audit Evidence' indicates that audit evidence is more reliable when it exists in documentary form, whether paper, electronic or other medium. The standard further elaborates that some of the accounting data and other information may be available only in electronic form or only at certain points or periods in time, and it may not be retrievable after a specified period of time, if files are changed and if back up files do not exist.

The potential for improper initiation or alteration of information to occur and not be detected may be greater if information is produced, maintained, or accessed in electronic form. The intended purpose of electronic evidence does not differ from traditional forms of evidence; however, the competence of electronic evidence generally depends on the effectiveness of internal controls over its validity and completeness.

Therefore, ANAO auditors test the internal controls relevant to the electronic evidence (for example, controls over generation, storage, manipulation, and transmission), to ensure the electronic evidence is credible. When information is in electronic form, certain audit procedures are best performed through electronic analysis and automated tools such as SAP Assure.

Increasingly, the financial reporting process for Australian Government entities is driven by information systems. IT and systems are embedded into business processes to initiate, authorise, process and manage financial transactions. Today's financial management systems have complex interfaces with internal business systems, interface with numerous IT processing or reporting systems and receive or transfer financial information concerning government payments or grant payments. Government entities are also increasingly implementing 'shared services', whereby one government entity has responsibility for the processing and/or system management of financial transactions on behalf of another government reporting entity.

In order to encourage flexible working practices, IT services are introducing and expanding functionality that allows users' access to the financial management system via web-portals, 'remote access' and virtual networks. Increasingly, government entities are adopting the use of synchronised sign-on or single sign-on (SSO) to facilitate identity management. As a result, IT systems are not only inextricably linked to the overall financial reporting process but form the foundation of an effective system of internal control for financial reporting.

ANAO extensively uses audit tools to assist its audit efforts. ANAO's audit findings and recommendations are reinforced through the issue of Better Practice Guides (BPG), which are designed to provide practical guidance and promote better practice in specific areas of public administration.

A BPG was issued in 2008-09 on strengthening the controls within the SAP computer system – used by many Australian Government agencies, to improve the preparation processes for their financial statements. In 2008-09 a BPG was also issued on Business Continuity Management, as an essential component of good public sector governance – to support and sustain an entity's business strategy, goals and objectives in the face of disruptive events.

All ANAO's reports, publications and Better Practice Guides are available for download from www.anao.gov.au

Auditing Outsourcing

Australian Government agencies often outsource their IT related processes, in the areas of software development, application support and maintenance and infrastructure management services to reduce costs, enable the agency to focus on its core activities, overcome shortage of skilled staff, and improve the quality of service.

The risks associated with outsourcing, such as continuous availability of services, acceptable levels of service, and security of information are adequately and effectively mitigated through appropriate controls that are implemented and functioning. The risks associated with outsourcing depend on the nature of the outsourced work, and the audit should focus on the areas of risk and evaluate the control measures pertinent to those risks. There are many varieties of outsourcing, as newer models of outsourcing are continuously evolving to meet specific needs of customers.

Because government organisations are becoming increasingly reliant on third-party service providers, it is important that internal controls be evaluated in these environments.

ANAO's IT Audit section contributes to the above process, by assessing and providing an opinion over the general and application controls environment of IT of government agencies. This includes the



review of the third party management assurance activities, in terms of the agencies' adherence to governance, controls, and legislative frameworks. For example, during the planning phase of the audit of third party services, Australian Auditing Standard ASA 402 'Audit Considerations Relating to Entities Using Service Organisations', is considered to determine how use of a service organisation affects the entity's internal control.

Additionally, the risk management, contracts management, definition and delivery of the statement of work and monitoring of the third party and outsourced services are considered. The auditor should assess, as per ASA 402, the effect that a service entity has on audit risk to enable the auditor to plan and develop an effective audit approach.

Contribution to Asia Pacific Region

The ANAO, in addition to its primary function of providing an independent view of the performance and financial management of Australian Government entities, recognises that it has a role to play in the international public sector auditing community. ANAO contributes to the development of international auditing standards and professional practices and the capacity building efforts of auditing bodies.

The ANAO has significant experience and expertise in financial statement and performance auditing and establishment



Australia's Resources

Mining

Australia continues to rank as one of the world's leading mining nations with substantial identified resources of major minerals and fuel close to the surface. The mining industry makes a significant contribution to Australia's gross domestic product each year, more recently in the order of 7%. In 2009, mining exports overtook manufacturing for the first time in Australia, accounting for 42% of the total value of exports. This was principally from the metal ore and coal mining industries.

Agriculture

Australian agriculture is based on extensive pastoral and cropping activities. Much of this produce is exported, with Australian wool, beef, wheat, and dairy products contributing significantly to global markets. Australia is also an important source of cotton and sugar.

Forestry

Australia's native and plantation forests are an important natural resource. They provide the vast majority of timber and paper products used by Australians and support other products and services, such as honey, wildflowers, natural oils, firewood and craft wood. In recent times, commercial tree growing has increasingly become an integral part of farm operations in the higher rainfall regions.

Fishing

The Australian Fishing Zone covers an area larger than its land mass making it the third largest fishing zone in the world. A significant proportion of Australian fisheries production – edible and non-edible – is exported with the main destinations being Hong Kong, Japan, the United States of America and China.

of corporate governance and management frameworks. This experience and expertise is of great benefit to our peers, particularly those in developing nations.

The ANAO's vision is to be a 'recognised international leader in the provision of public sector audit and related services'. ANAO provides briefings to international visitors on the auditing framework in Australia, the role of the ANAO and the importance of a sound governance framework in the Australian Public Service (APS). In addition to contributing to the international auditing community the ANAO seeks to support the Australian Government's overseas aid program.

ANAO's participations in the region

The ANAO has close links with the Indonesian Board of Audit (BPK) and the Papua New Guinea Audit Office (PNGAO). Those links have been developed over the past three years through our participation in international capacity-building programs funded by AusAID (the Australian Government's overseas aid program).

ANAO receives delegations and study groups from around the region to exchange knowledge on management frameworks and policies and legislations underpinning the frameworks.

Secondees from the countries in the region such as from Papua New Guinea and Indonesia visit and undergo training in auditing and participate in cross cultural awareness programs to build better understanding and cooperation. Also, the ANAO hosts secondees from Canada and Ireland on a reciprocal basis

INTOSAI

The ANAO has representatives on three INTOSAI Working Groups:

- Audit of Privatisation, Economic Regulation and Public Private Partnerships
- Environmental Auditing
- IT Audit

ASOSAI

The ANAO has an ASOSAI representative on the INTOSAI Performance Audit Sub Committee.

PASAI

The ANAO became a member of PASAI in 2007. The 12th Annual PASAI Congress 20-24th July 2009, held in Palau, was attended by ANAO representatives.



Lakshmi Radhakrishnan

Lakshmi is an IT Audit Director from the Australian National Audit Office with public and private sector IT audit experience. She is a member of the local ISACA Board.



Wayne Woodford

Wayne is an IT Audit Director on secondment to the Australian National Audit Office from Centrelink. He has an extensive technology background.

Data Analysis in Australian Government audits





The Australian National Audit Office's (ANAO) annual program of audits includes those that examine the quality and integrity of agency client records and report on the effectiveness of the management of the data and how it impacts on service delivery.

This article discusses two performance audits that used a PC data analysis software tool, IDEA¹, to assess the effectiveness of Australian Government agencies' management of data integrity in major business systems. These analyses also illustrate how the quality of that data affects the agencies' capacity to manage and support their core business operations. IDEA testing enables extraction, sampling and analysis of data in order to identify errors, omissions and other specific integrity issues. This testing includes both the inherent soundness of the data being stored and the agencies' adherence to their own business rules.

The agencies audited have a range of IT systems and applications to store, retrieve and process client and non-client information. These systems include both legacy mainframe and newer systems. A challenge for Australian Government agencies in this environment is balancing the resources required to maintain legacy systems while developing new IT capability with its greater functionality and opportunities to maintain better data integrity.

IDEA was used to examine the records of clients and other information to test that the content of the data was reliable, complete and up-to-date within acceptable parameters, and contained evidence to meet both legislative and policy requirements and agency business rules. IDEA testing included an examination of: date fields and other data such as links between records to assess the integrity and currency of the data; keyword searches through free-text fields to detect potentially anomalous records; duplicate,

near duplicate or records with identical data in certain combinations of fields; internal inconsistency within or between related records; and key data fields that establish client identity and program eligibility.

The audits revealed that there was considerable scope in both Australian Government agencies to improve the management of their information systems and, in particular, the quality and integrity of data. This in turn, would support improved service delivery. The quality of the data would also have been substantially improved through the development and use of an effective accountability regime, including quality control, to assure the quality of records over time. Additional assurance of data quality would be gained from a greater focus on data collection standards and controls, and procedural compliance around data input and records maintenance, including timely deletion or relocation of outdated and erroneous data.

The benefits realised by the ANAO in using IDEA include improved knowledge and understanding of data structures and IT environments audited, the capacity to analyse large quantities of data, and time and resource efficiencies conducting the data analysis. Increasingly, Australian Government agencies are also using similar data extraction and analysis techniques as a means of obtaining greater management assurance about the integrity of their information systems, and the ANAO encourages agencies to do so.

ANAO Audit Report References

Audit Report No 28, 2008-09 *Quality and Integrity of the Department of Veterans' Affairs Income Support Records*, Department of Veterans' Affairs.

Audit Report No 35, 2008-09 *Management of the Movement Alert List*, Department of Immigration and Citizenship

¹ IDEA, a registered trademark of CaseWare International Inc.



BRAZIL

Modern organizations, whether public or private, do their businesses based on information management. Information is an important organizational asset just as environments and means of dealing with it, and they all must be securely kept. In this scenario, adopting information security (IS) practices is no longer an option, but a mandatory action, essential to organizations survival.

Introduction

Information security practices comprise a set of procedures and tools that ensure information security principles (confidentiality, availability and integrity) not only concerning physical and technological issues (facilities, equipments, infrastructure, systems, databases and other information technology resources), but also organizational issues (people and work processes) (FONTES, 2008; SÉMOLA, 2003).

The Brazilian Court of Audit (TCU) is an organization that deals essentially with information in order to aid the Parliament (National Congress) in exercising the external control of Public Administration. Such control exercised externally to the structure of the Control Power, as Wurman (2005, p. 11) states, aims at the "preservation and balance of democratic political institutions in Brazil".

The work developed by TCU is delivered to Parliament and society by means of rulings, orders, instructions and normative decisions. It is based on information received by the agencies under

Information security at the Brazilian Court of Audit: complying with our own recommendations



its jurisdiction, the press and society as a whole, after audit activities, accountability and account rendering, denunciations and other mechanisms. In short, both the input and output of TCU's activities are, ultimately, information.

Since TCU is aware of that and in exercising its pedagogical and guiding function it has been performing actions to support the adoption of IS good practices in Federal Public Administration agencies and other agencies under its jurisdiction. Among these actions we highlight:

- a elaboration of "Information Security Good Practices" (Boas Práticas em Segurança da Informação) booklet (BRASIL, 2007), published in 2003 and revised in 2007, with the objective of raising IS awareness in government agencies and serving as an important reference source for Public Administration improvement in this area;
- b creation of the Information Technology Audit Department in 2006 in order to improve and enhance information

technology (IT) auditing activities by TCU's technical staff. One of its focus areas is checking IS compliance and IT performance of governmental actions; and

- c Issuance of rulings that recommend and/or determine the adoption of IS good practices.

On the other hand, from the legitimacy viewpoint, these actions create for TCU the need to become a reference with regard to the adoption of information security practices. Suchman (1995, p.4) defines legitimacy as "a generalized perception or assumption that institutional actions are desired, proper or appropriate within some socially built norms, values, beliefs and definitions". Pfeffer and Salancik (1978) state that legitimacy is a status granted by society to a given organization, after evaluating the utility of and endorsing its activities.

The consistency between discourse and practice is one of the ways through which legitimacy is achieved by organizations (MORGAN, 1996). According to the typology

presented by Suchman (1995), this legitimacy is called moral legitimacy. In this sense, TCU has been trying to set the example for the agencies under its jurisdiction by making an effort to internally follow the IS measures recommended in its deliberations.

Discourse as practice

Knowing its discourse well is the first step to be taken by an organization that attempts to attain moral legitimacy (ORLANDI, 1999). The next step is to drive actions in the same direction. Hence, looking at its recommendations to other institutions is an essential requirement for TCU to guide its information security initiatives.

Although information security issues have been present in TCU's decisions for years, the inclusion of IS recommendations has become more frequent as of 2003, not by coincidence the year when the first edition of the previously mentioned booklet "Information Security Good Practices" (Boas Práticas em Segurança da Informação) was published.



If we then take the year 2003 as a starting point and August 2009 as the end, a brief survey on TCU's jurisprudence databases reveals the existence of 50 rulings that deal with information security. A more in-depth analysis shows that about 90% of these rulings recommend at least one of the following actions:

- a information security policy elaboration or review;
- b adoption of a specific organizational structure to deal with information security;
- c information classification implementation;
- d access control implementation; and
- e business continuity management implementation.

It is worth mentioning that TCU has been using the NBR ISO/IEC 17799:2005¹ standard as reference in its IS recommendations. This is due to the acknowledgement of the Brazilian Technical Standards Association's technical excellence, as well as to the fact that the equivalent international version of this particular standard, the ISO/IEC 17799, is renowned and broadly used for the same purpose by Supreme Audit Institutions and government bodies throughout the world. Amongst the rulings issued by TCU, Ruling nº 1.603 – Plenary, of August 13th, 2008, and nº 2.471 – Plenary, of November 5th, 2008 should be highlighted. In these rulings, the Brazilian Court of Audit brings an innovative character and, in order to show its intention

to be reference for the agencies under its jurisdiction, it recommends to itself the adoption of measures for managing information security.

Having said that, TCU's organizational discourse and the path to be taken become clear and consistent. At this moment, the organization completed the stage of “knowing” the discourse and went further by defining goals to be achieved. What was left had to do with “practicing”.

It is worth highlighting that even before the issuance of the above mentioned rulings, several IS initiatives were already in place at TCU. Aside from external control guiding actions, TCU had already internally ruled on some aspects related to this theme, such as procedures for safeguarding confidential documents; access, circulation and permanence of people and vehicles in TCU's buildings; information security policy; criteria for registering information in corporate databases; document management procedures and actions; designation of management units for IT solutions and criteria for internet access through TCU's network.

Moreover, among internal actions, we highlight the information security maturity and compliance diagnostics based on the NBR ISO/IEC 27002:2005 standard, concluded in July 2008. This diagnostics resulted in recommendations for IS improvement in TCU, as well as the creation of a strategic area for information security coordination and review of IS policy in force at the time.

Strategy to implement information security at TCU

Reaching objectives depends much on the adopted strategy, i.e., on the definition of a pathway to be followed by the organization (KOTLER, 1975; ANSOFF, 1993). So, once it had the list of actions to be carried out, TCU needed to define priorities, allocate resources, and make efforts to put them in practice.

More than that, TCU needed to clarify the importance of information security internally. For that, top management commitment and involvement have been fundamental. In 2007, top management commitment was evident by the appointment of Minister Augusto Sherman Cavalcanti to carry out the strategic coordination of IT policies and guidelines definition at TCU. With strategy defined and strong top management support, TCU started to comply with its own recommendations.

Definition of a specific IS structure

Information security good practices (ABNT, 2005; BRASIL, 2007; DIAS, 2000) recommend that the organizational structure include an area in charge of information security actively supported by top management. This area must elaborate the information security policy, coordinate its implementation, approval and revision, and work towards the correct dissemination and enforcement of this policy, in a way that everyone – employees, suppliers and clients – understands their responsibilities regarding information security in the organization.

Following this recommendation, TCU's IS corporate policy (PCSI/TCU), approved by Resolution – TCU nº 217, of October 15th, 2008 (BRASIL, 2008b), establishes that this role be performed by the General Secretariat of the Presidency (Segepres), by means of the Information Security and Information Technology Governance Advisory Office (Assig), and the Information Security Committee (CSI).

Assig is a specialized advisory unit, established by Segepres in April 2008, and its mandate is to coordinate and control the implementation of PCSI/TCU and complementary norms, approve work processes and needed operating procedures, periodically monitor and assess IS practices adopted by TCU.

CSI is a consultative collegiate body established by PCSI/TCU, and it is aimed at formulating and enforcing guidelines for TCU's information security policy, periodically analyzing its effectiveness, proposing institutional norms and mechanisms for continuous improvement, and advising TCU's General Coordination Commission (CCG) and Presidency in related matters.

Such committee is comprised of two representatives of each General Secretariat, aside from a representative of the IT

Ruling nº 1.603/2008 – PL

9.1.3. to provide guidance on the importance of information security management, through norms, actions that enable the creation and /or improvement of business continuity management, change management, capacity management, information classification, incident management, IT risk assessment, information security specific management, information security policy and access control procedures;

9.6. to recommend to TCU's General Secretariat of the Presidency – Segepres and to the General Secretariat of Administration – Segedam the adoption of the measures mentioned in item 9.1;

Ruling nº 2.471/2008 – PL

9.6.1. to establish procedures for the elaboration of Information Security Policies, Access Control Policies, Backup Policies, Risk Assessment and Business Continuity Plans. Such policies, plans and assessments must be implemented in the agencies under its jurisdiction by means of norms;

9.16. to recommend, based on art. 43, I, of Act nº 8.443/92, to TCU's General Secretariat of the Presidency, the adoption of the measures mentioned in items “9.4.”, “9.6.”, “9.8” and “9.10” above;



¹ Renamed to NBR ISO/IEC 27002:2005.

Department and the officer in charge of Assig. The heterogeneous and representative composition of different TCU sectors, with different interests, meets IS good practices (ABNT, 2005; PINHEIRO, 2009), leads to a broad discussion and grants legitimacy to the proposals submitted by this committee to higher instances.

Information security corporate policy updating

The information security maturity and compliance diagnostics based on the NBR ISO/IEC 27002:2005 standard (ABNT, 2005) and its recommendation that IS policies be critically analyzed at planned intervals or when significant changes occur have motivated PCSI/TCU's old version (BRASIL, 1999) updating.

Formalization, updating and dissemination of PCSI/TCU are also actions in line with TCU's decisions, especially regarding Rulings nº 1.603/2008-PL and nº 2.471/2008-PL, so that the overseen agencies can elaborate, formalize, disseminate and update IS policies that will guide information security management activities in these organizations.

The updating started with Assig's assessment of the diagnostics report. Such report highlighted that the IS policy in force at the time presented limiting factors, such as an overly technological approach opposed to the concept that information security does not encompass only technologies but also organization's processes and people; non-delegation of IS responsibilities, which makes it harder to implement actions derived from the policy; inclusion of specific themes that should have been included in complementary standards, such as rules on the correct use of electronic email at TCU.

After analyzing the report and suggestions collected in meetings with IS-related departments at TCU, Assig elaborated a PCSI/TCU draft, which was approved by Resolution – TCU nº 217/2008. The guidelines established in this resolution set out the major security lines to be followed by everyone when dealing with information produced and held in custody by TCU.

Regarding the previous ruling, it must be highlighted that PCSI/TCU delegates competence to Segepres, by means of Assig, to coordinate and control the implementation of this policy and its complementary norms; creates the CSI; defines and attributes responsibilities for information managers and custodians, TCU directors and unit heads; and excludes from its contents electronic mail issues.

In PCSI/TCU, as a set of principles, objectives, and guidelines that drive information security management at TCU, we have common topics in IS policies, recommended by the ABNT standard (2005), such as: information security definition and goals, general responsibilities in

managing information security, mention to complementary norms and procedures that support the policy, consequences of norms violations, IS training needs and education etc.

With the objective of making policy content clearer to all stakeholders – public servants, TCU's departments, contractors, trainees or any other collaborators who have authorized access to the information produced or held in custody by TCU, we have written the booklet "Information Security at TCU: commented corporate policy" (BRASIL, 2008a) and the folder "Information Security Corporate Policy at TCU" (BRASIL, 2009).

Issuance of complementary norms

Just as in any policy, PCSI/TCU focuses on principles and guidelines. It is the major part of many other documents such as the ones commented below, with detailed information on IS procedures and standards to be applied in given circumstances.

Information classification

After PCSI/TCU approval, CSI, in its prerogative of proposing institutional norms and mechanisms for continuously improving information security, and in compliance with Ruling – TCU nº 1.603/2008-PL, has approved and submitted to CCG a norm draft on the classification of information produced or held in custody by TCU.

The information classification regulation is worth highlighting because it involves all TCU activities and is a structuring tool so that information management is properly achieved in TCU's work processes. Such regulation meets not only the requirements stated in the said ruling, but it also promotes the creation of a fundamental mechanism for sustainable implementation of electronic process at TCU. It also makes it possible to implement security requirements that favor information exchange among TCU, the agencies under its jurisdiction, the control network bodies and entities, and other cooperation agreements.

Access control

Driven by information security debates during PCSI/TCU updating, TCU has approved, before the publication of the revised policy, procedures and rules for granting access profiles to IT solutions to contractors and trainees which requires them to sign a term of responsibility for IT resources use. As a complement, Assig has issued a technical note on the profile concession and suspension process implemented by TCU's access management system, with recommendations to formalize the access control policy from work processes already adopted, including the joint definition of responsibilities, procedures and terms by IT solution managers and the IT Department.

Information security incident management

Following the good practice of instructing users to notify any suspicion of information security frailty and of establishing a channel for registering this notification (ABNT, 2005), PCSI/TCU has granted to internal users and TCU collaborators the responsibility of reporting to Assig about any IS incidents they are aware of. Therefore, Assig is the main communication channel for registering IS incident notifications.

Users who don't know if a fact can be classified as an information security incident or who are in doubt can also get in touch with the Ombudsman Office or the IT Department Call Center. Their notification will be registered and they won't need to make another call to Assig. So, these units act as alternative channels for registering incident notifications.

After registration, the information collected from users are submitted to the appropriate unit which will then analyze the incident, identify its causes, report the adopted solution, measures to prevent recurrence etc. Depending on the incident's seriousness, Assig is immediately communicated so that a corrective action is taken in a timely manner.

With regard to Ruling nº 1.603/2008-PL on incident management, Assig, which is in charge of coordinating and controlling the implementation of PCSI/TCU and its complementary norms, as well as periodically monitoring and evaluating IS practices adopted by TCU, is also responsible for the consolidated analysis and control of registered IS incidents.

One action leads to another

In trying to comply with its own recommendations, aside from those described in Rulings nº 1.603/2008-PL and nº 2.471/2008-PL, other actions have proven to be necessary to add on to the efforts of effectively practicing information security at TCU.

In terms of structure, TCU has created under the IT Department, the IT Security Service which is in charge of promoting and monitoring the implementation of actions for information security in line with PCSI/TCU; of coordinating work processes management, methods and tools for business continuity management, information security incidents management etc.

In terms of norms, aside from the information classification draft, CSI has approved and submitted to CCG drafts on the use of electronic mail, computer network, portable devices and other IT resources. CSI is still deliberating on drafts to regulate backup procedures and software installation in workstations.



Moreover, Assig has elaborated a template for the confidentiality and responsibility term to be signed by trainees and other collaborators whenever they are authorized to access non-public information. Assig has also disclosed security guidelines to TCU's internal public when working outside TCU and the use of paper shredders for hard copy document disposal. Also worth mentioning is the IS awareness program and the elaboration of technical notes on security certificates and on logic access control.

IS awareness program

Aiming on keeping TCU's technical staff trained in IS practices and aware of the importance of this theme for the institution, Assig has established an information security awareness program for servants and authorities at TCU. Such program's focus is not to cover IS special technical needs but to disseminate IS basic concepts, general practices and work habits.

The awareness program is a continuous activity and, as such, it is comprised of periodic actions, such as the dissemination of internal policies and norms, tips, guidelines and news of what TCU is doing regarding information security in the "Information Security" community hosted in the corporate web portal and in the bimonthly newsletter in TCU's internal bulletin (União). Direct contact with servants and authorities during visits to TCU's units to discuss issues, clarify doubts and get different perceptions about information

security are all part of the program.

In the program, every year there will be a "TCU Information Security Day", with lectures by guest speakers, entertainment and educational activities. The first edition of this internal event, on October 29th, 2009, counted on the participation of lecturers from TCU's IT Audit Department and Petrobras, aside from a theater play and awards to winners of an information security quiz.

Future plans

Although several actions have been carried out within TCU, challenges remain. Amongst them, for the next year we plan to establish the business continuity management program (BCP), update norms and reinforce physical access control.

The business continuity management program is aimed at "avoiding interruption of business activities and protecting critical processes against effects from significant failure or disasters, and ensuring their recovery within reasonable time, if it is the case" (ABNT, 2005). Since the interruption of business activities may lead to legal, financial, or image-related issues, BCP's relevance is more and more evident for both public and private institutions.

In order to implement BCP at TCU, the strategy designed by Assig and approved by CSI stems from the cooperation with other Public Administration organizations that have already gone through this experience. The idea is to get as much

information as possible and absorb methods and procedures to identify TCU's critical processes during business impact analysis (BIA).

With regard to physical access control, it is worth mentioning that TCU's norm on this subject has been in place since 1995 and comprehends issues such as garage access control and personal identification of servants, collaborators and visitors. We need to periodically update this norm in order to make it compatible with organizational needs to prevent or minimize IS risks.

Final remarks

In view of the above, one can say that TCU is on the right track to attain moral legitimacy before the agencies under its jurisdiction. The actions and activities summarized herein are in line with international IS guidelines and TCU's decisions.

Particularly regarding Rulings nº 1.603/2008-PL and nº 2.471/2008-PL, all recommendations have either been fulfilled or are ongoing at TCU. It is worth clarifying that although change and capacity management actions mentioned in these decisions are related to information security, their focus is on IT service management. This is why such subjects have not been approached directly in this article, even if the implementation of these recommendations is underway at TCU, supported by ITIL² good practices.



Notwithstanding the steps taken towards following our own recommendations and, thus, be a reference to the agencies under our jurisdiction, several challenges still have to be faced by TCU. Even regarding the actions already taken, the work remains, given the need to periodically review IS themes in order to keep actions and norms updated according to TCU's needs.

When referring to information security, conjugating verbs in the past does not seem appropriate. It is an ongoing activity and the strategy for success assumes broadening borders without overlooking what has already been achieved. There is a need for norms and policies, definition and implementation of proper structure and controls. However, when performing each one of these actions, one cannot say the whole work has been done. It is necessary to continuously assess risks and, based on the outcomes, each one of the actions mentioned must be updated.

This is why we have used a gerund form in the title of this article. In an effort to set the example for the agencies under its jurisdiction and to put discourse and practice in the same track, TCU is "complying" with its own recommendations. And it should make an even greater effort or it will lose legitimacy when recommending IS practices. Hence, TCU must persevere and be diligent, in order to consolidate the actions already developed, conclude those already ongoing and build an information security culture in the organization as a whole.

References

- Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002 - Tecnologia da informação: técnicas de segurança - código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005. 120p.
- ANSOFF, H. Igor. Implantando a administração estratégica. São Paulo: Atlas, 1993.
- BRASIL. Tribunal de Contas da União. Resolução - TCU nº 126, de 3 de novembro de 1999. Dispõe sobre a Política de Segurança de Informações do Tribunal de Contas da União (PSI/TCU).
- Boas práticas em segurança da informação. 2ª ed. Brasília: TCU, 2007. 70p.
- Segurança da informação no TCU: política corporativa comentada. Brasília: TCU, Segepres, 2008. 29p.
- Resolução - TCU nº 217, de 15 de outubro de 2008. Dispõe sobre a Política Corporativa de Segurança da Informação do Tribunal de Contas da União (PCSI/TCU).
- Política corporativa de segurança da informação do TCU. Brasília: TCU, Assig, 2009.
- DIAS, Cláudia. Segurança e auditoria da tecnologia da informação. Rio de Janeiro: Axcel Books, 2000. 218p.
- FONTES, Edison. Praticando a segurança da informação. Rio de Janeiro: Brasport, 2008.
- KOTLER, Philip. Administração de marketing. São Paulo: Atlas, 1975.
- MORGAN, Gareth. Imagens da organização. São Paulo: Atlas, 1996.
- ORLANDI, Eni. Análise de discurso: princípios e procedimentos. 2ª ed. Campinas: Pontes, 1999.
- PFEFFER, Jeffrey & SALANCIK, Gerald R. The external control of organizations: a resource dependence perspective. New York: Harpes & Row, 1978.
- PINHEIRO, Patrícia. Direito digital. 3ª ed. rev., atual. e ampl. São Paulo: Saraiva, 2009. 411p.
- SÊMOLA, Marcos. Gestão da segurança da informação: uma visão executiva. Rio de Janeiro: Campus, 2003.
- SUCHMAN, Mark C. Managing legitimacy: strategic and institutional approaches. Academy Management Review, v.20, n.3, p. 571-560, jul. 1995.
- WURMAN, Samy. Controle externo. 2ª ed. Brasília, 2005.



Cláudia Augusto Dias

Federal Auditor at the Information Security and Information Technology Governance Advisory Office of the Brazilian Court of Audit, majored in Electrical Engineering, Master's and PhD in Information Science at the University of Brasília (UnB).



Felício Ribas Torres

Federal Auditor of the Brazilian Court of Audit, majored in Economics, specialist in Information Technology, Master's in Administration at the University of Brasília (UnB) and graduated in Finance and Public Planning and Budget. Presently, Head of TCU's Information Security and Information Technology Governance Advisory Office.



Sharing Audit experiences from one auditor to the others

This article details the National Audit Office of China's (CNAO) work collecting Expert Experiences on IT audit from 2005 to the present.

The CNAO developed AO software to be used for field audit and deployed it to 3000 audit organizations. It was supplied free to nearly 80000 auditors in the country. Chinese Audit has moved into a new era; using IT and auditing electronic data. Audit methods have changed greatly from using abacuses and auditing paper accounting materials to IT Audit today.

There is an old saying "Each age brings forth new genius on this noble land". A group of auditors integrated their IT knowledge and audit experiences to create a new and fresh approach for IT Audit. Dr. SHI Aizhong, the deputy Auditor General of CNAO, requested that dispersed knowledge should be brought together so that individual audit experiences could be used as a reference for others.

CNAO collected the experiences from auditors throughout the country. These experiences were then evaluated by specialists. Selected cases were publicized in electronic form and shared within the audit organizations. There are now a total of 1161 selected IT Audit cases in the experiences database.

Because of the requirements of evaluation, CNAO asked that all IT Audit cases should be submitted in the same format. A qualified IT auditor should and could use IT to deal with electronic data, embody their ideas and fulfill concrete audit targets. At the same time the submitted case should meet the following requirements:

- 1 The title should be clear, concise and comprehensive so that the content of the case can be easily ascertained.
- 2 The type of audit should be identified indicating under which area the case comes: financial audit, monetary audit, enterprise audit etc. There are six types and nineteen sub types in the audit classification tree.

- 3 The circumstances of the audit should be described including which step the case comes from, the general analyses of the auditee, the focus areas of the audit, or any special investigations needed in unusual circumstances.
- 4 The description: The auditor should identify the necessity of this case for the whole audit project, the content and the aim of the case and write down the main idea for the audit items.
- 5 The materials needed: These should not be generalized by the word "accounting materials" because the materials are different from those needed in manual audits. IT audit usually deals with data in the management system of the audited party. The data collection and transformation functions in AO could meet the auditor's requirement for this.
- 6 The Audit processes should be described clearly indicating how to use the audit materials. Some audit items are easily completed in just one step, for instance, if the auditor wants to check whether there is any cash withdrawn illegally, he only needs to sort the credit side of the cash item from the financial records. After that, the auditor can sample the data as a further check. Complicated audit items should be explained step by step with staggered aims. Not all these steps are done with AO because sometimes the auditor will need to conduct interviews or field checks need to be completed. Based on the results of field checks, the next step is identified.
- 7 Experience model: The audit process should be depicted with a standard flowchart. It is a challenge for Chinese auditors used to traditional audit techniques who have only seen these symbols in training materials. Now more and more auditors are used to communicating with these standard and unambiguous symbols.

- 8 SQL description: SQL is a common database structured query language. An auditor can write the audit process and experience model into SQL for reuse. It is a really difficult transition for traditional auditors to IT audit thinking. Among the IT medium training courses set by CNAO, the course on databases is an important one which has the lowest pass rate due to the difficulties of SQL.
- 9 The applicable laws and regulations should be indicated where they are used for audit items. Based on them, auditors can judge whether or not the audit case is correct.
- 10 The typical case is described in detail to help other auditors understand the IT audit experience in depth. Thus auditors can identify the audit method and process for the case. An excellent case should not only inspire new ideas

in other auditors but also in specialists, outstanding cases can always get more attention.

- 11 The writer's name. Recording the name means that not only does the writer get recognition but also promotion and added responsibility.

What auditors want to get from cases is not just an overview. CNAO transformed the IT audit cases into the IT audit method which has been run in AO since 2005. There are now 938 such cases in AO. For instance, if the auditors want to judge whether the depreciation of fixed assets are calculated correctly and they have the required data field, they can select the model "audit for depreciation of large scaled fixed assets" from the audit method tree. Then the expected result can be produced. See as the following picture.



The collection of the IT audit cases is on going. It is highly appreciated by the Chinese e-governance specialists. "What we are working hard to do is diffuse the IT audit experiences to 80000 auditors instead of just putting them on a shelf. Then auditors can get higher audit capability," said Mr. WANG Zhiyu, the Director General of IT Center, CNAO.



Mrs XIONG Wanjiao

Works in IT Centre of CNAO mainly on the Golden Auditing Project.

IT audit in EUROSAI IT Working Group countries

A vital enquiry

An IT audit survey developed by the ITASA subgroup of the EUROSAI IT working group was recently prepared at the National Audit Office of Finland and sent to all 31 member countries. This important survey, drawn up using webropol-software, contained questions on the following areas:

- tools or systems used in managing and documenting audits and collecting, analysing and storing data
- how IT audit is organised
- education, training, certification and work experience of IT auditors
- IT risk analysis and standards, models and best practices in IT audit.

In asking these questions, the subgroup wanted to acquire essential benchmarking information about what is going on at a European level in this special area. Although the list of questions was long, 19 SAIs returned a completed questionnaire – an impressive rate of 61 %. A range of different-sized countries were equally represented among the respondents. The results of the survey were used by the ITASA subgroup of the EUROSAI IT Working Group to better understand the practices of IT audit.

We are grateful that so many countries took time to answer the questionnaire. We would also like to thank those who contributed to its success by reading and commenting on the draft version. Special thanks to the SAI of Switzerland, which as chair of the EUROSAI IT Working Group made it possible for us to carry out the survey.

Results of the survey

IT audits strategies

12 SAIs, the majority smaller institutions, set out their IT audit strategic objectives in writing.

Using tools and systems

The questionnaire revealed that more than half (11 of the 19) of the respondents use an audit management system, most frequently TeamMate. Disappointingly, audit documentation systems and data warehouse solutions are used in fewer than 10 SAIs, and there seems to be no relation between the use of such systems and tools and the size of the SAI. There is a more positive situation regarding tools for collecting and analyzing data, so-called CAATs (Computer Assisted Auditing Techniques); all of the respondent SAIs used at least one such tool, the most common being IDEA and ACL.

Haphazard consultation

Happily, the survey found that some form of IT audit is conducted in all of the SAIs, although sometimes this is not very extensive. In about half the institutions, audits are carried out by specialist auditors from a separate IT audit department, but in most cases they are performed by auditors from the financial or performance audit departments.

The number of auditors performing IT audit varies considerably between the SAIs. Surprisingly, the results of the survey showed that in some smaller SAIs, the number of auditors performing IT audits was higher both in proportional and absolute terms than in larger institutions. In most SAIs, the IT audit department is consulted in the planning stage of financial, compliance and performance audits, although this is usually on a voluntary basis and occurs somewhat haphazardly. This is also the case when outside experts are called in to help with IT audits, as happens in eight of the respondent SAIs.

IT auditing experience preferred

Nearly 80% of the SAIs questioned require university or equivalent qualification from their IT auditors. About half the SAIs oblige auditors to maintain their knowledge through further training, with one SAI expecting its



auditors to invest more than 40 hours per year. Other ways to maintain knowledge of auditing skills such as self-education, participation in seminars and workshops etc. are also encouraged. Previous work experience is required in 13 SAs, particularly in the smaller institutions. This experience usually relates to auditing in general, but experience in IT-related issues and/or IT auditing itself is also sometimes preferred. Whereas a small minority of SAs expect international certification such as CISA, CISM etc. from their IT auditors, these qualifications are merely encouraged in others.

Too little risk analysis

It was pleasing to discover that twelve of the respondents use IT audit risk analysis, which in six SAs is based on an internationally accepted risk analysis model or best practice such as COBIT. In other audit institutions, risk analysis is part of other common analysis structures or in the development phase. IT audit risk analysis is most often performed at agency and/or government ministry level.

However, IT audit risk analysis is rarely performed on a regular annual basis and is unknown in some SAs. Fewer than half the respondents carry out risk analysis in every single IT audit.

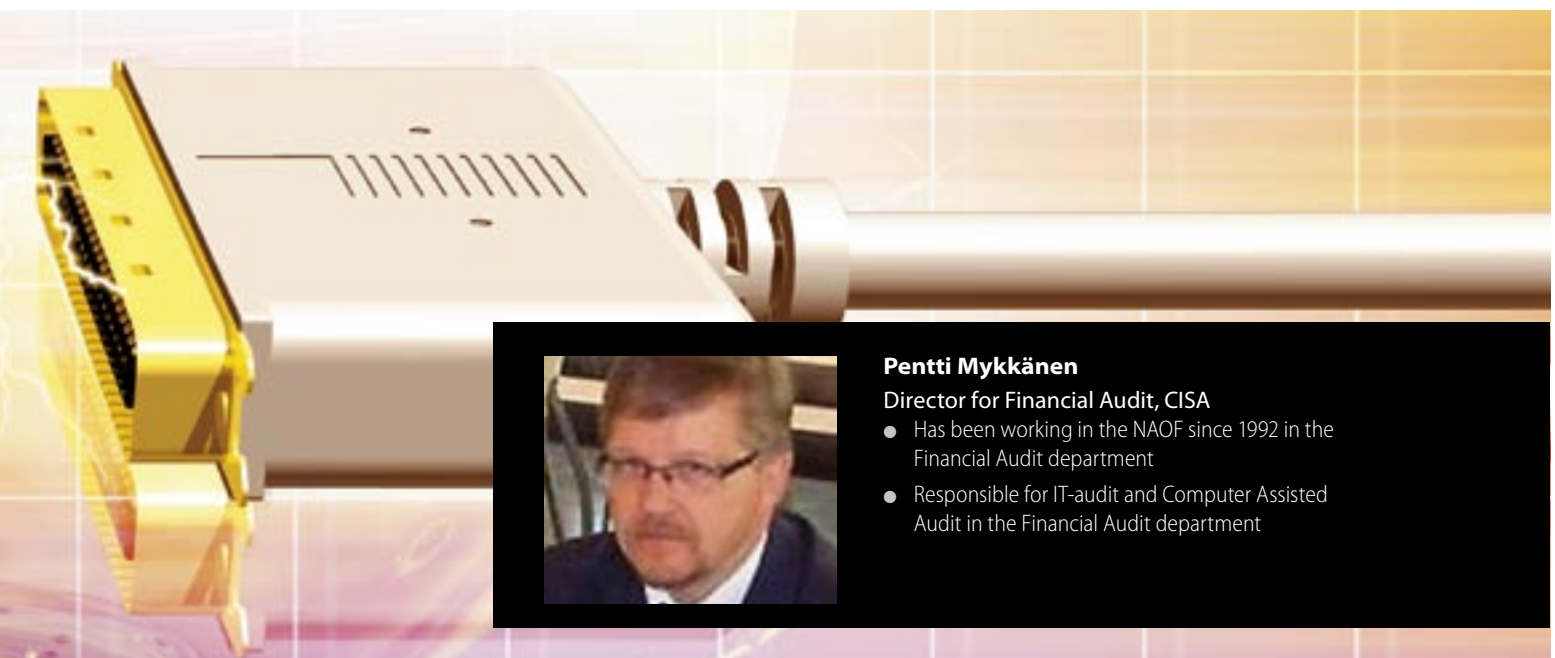
Strong on standards, weak on external evaluation

Pleasingly, all but two of the SAs perform IT audits according to international standards such as ISO27001 (or BS7799) and using commonly accepted models such as COBIT. In contrast, in only two of the nineteen SAs have IT audit procedures and functions been evaluated or assessed by an evaluator outside the SA during the last three years. In some cases, evaluation is performed as a part of some control or review procedure made by the SA itself. The survey also asked SAs to choose from a list of five audit areas which had been the most important area to audit during the last five years. These areas covered data security, data protection, IT procurement procedures and IT investments. In the responses, none of these areas stood out; it is clear that the audits listed were generally SA and country-specific audits.

Recommendations

What, then, can be concluded from the results of this important survey? It seems that, generally speaking, IT audit procedures and functions are not particularly clear or well specified in the majority of SAs. Unfortunately, this is also true of IT audit strategy in some countries. Larger institutions are not automatically better organised than smaller SAs; in fact, the situation is generally slightly better in the latter.

This suggests, then, that a more accurate IT strategy needs to be drawn up in those SAs where such a strategy currently does not exist. Standards of expertise should be set for IT auditors and international certification encouraged. There is also considerable room for improvement in the fields of IT audit risk analysis, evaluation and benchmarking. All SAs are reminded of the ITASA (IT Audit Self-assessment) tool which can be used to assess IT audit procedures in their institution. The use of this tool is strongly recommended. If you would like help in organising an ITASA, please contact the colleagues in Switzerland, who will be more than happy to assist you.



Pentti Mykkänen

Director for Financial Audit, CISA

- Has been working in the NAOF since 1992 in the Financial Audit department
- Responsible for IT-audit and Computer Assisted Audit in the Financial Audit department



Information Security audits in the Nordic countries

In November 2007 the Nordic SAI in Denmark, Finland, Norway and Sweden met in Stockholm to discuss auditing Information Security in the public administration. The purpose was to share important experiences and knowledge in the area of Information and IT Security.



SAI Denmark: Ib Bentzien, Kurt Keldebaek, SAI Finland: Pentti Mykkänen, Hannu Stordell, SAI Norway: Anne Marie Hausland, Arthur Lio, Egil Andresen, SAI Sweden: Bengt E W Andersson, Björn Undall, Stefan Gollbo.

All statements and conclusions are our own personal statements and not necessarily the views shared by the SAI.

Since this article was written the Danish SAI has changed its focus from being on DS 484 to being risk-based. Furthermore, the Ministry of Finance has decided that from 2013 Denmark must follow ISO 27001 instead of DS 484. In addition to this Rigsrevisionen has adjusted its way of reporting.

This article constitutes a summary of the discussions on similarities and differences in audit conditions and audit findings in the Nordic Countries.

As a base for discussions each SAI distributed memos describing the IT audit function within the SAI, conditions for auditing IT and Information Security in public administration, and a summary of audit findings.

1. Increasing danger of incidents in the agencies' IT-based operations

The need for information and IT security

IT systems have become an important part of most societal functions, such as the banking and finance systems, electricity and water supply, traffic control systems and systems in the health and social welfare sector. In order to improve the efficiency IT systems have increasingly been linked, both within enterprises and across organisational boundaries. This has increased the mutual dependency of IT systems and enterprises.

Nearly all important IT systems are in constant danger of being attacked. In audits 2005 – 2006 SAI Sweden revealed the following serious incidents in the agencies' operations:

- There are examples of agencies that have failed to avert virus attacks, as a result of which they have been unable to function. The officials were without access to necessary information.
- Serious incidents have occurred when agencies have changed their IT systems or introduced new IT systems. Government services on the Internet that are important to society, to citizens and to businesses, were closed down for up to two weeks. Officials had difficulties in carrying out their duties in a new system.
- Deficiencies in the protection of agencies' websites have led to unauthorised persons gaining access to and also being able to change sensitive information.

The picture of incidents is similar in the other Nordic countries.

There is a risk of a lowering of public confidence in agencies' e-services if the information cannot be protected. If that happens, there is a considerable risk of the entire investment in e-administration being jeopardised.

Deficiencies in information security can also affect national emergency management systems. Central government agencies have as a rule an important role to play in society's ability to forestall, prevent and manage emergencies. The agencies are therefore assumed to have a certain basic capability to enable them to fulfil their role and to help society cope with emergencies. This basic capability is dependent on how well designed the agency's information security is.

The environment for information security management (ISM)

The following points characterise this environment:

- Threats are evolving. The amateur hacker is history. Cyber crime is evolving. First instances of, so far very limited, Cyberwarfare have been noted/suspected.
- Systems are evolving. Dependency on online services is ever increasing. Connecting SCADA systems and administrative systems creates new threats. Automated access to data between agencies is increasing.
- Unclear lines of demarcation and lack of coordination between government bodies. Cooperation between agencies is often hard to achieve
- Complex organisation of security work. Responsibility for security is spread over a number of different players

2. Findings from auditing Information and IT security

Findings on the Government's control of information security work within public administration

SAI Norway and SAI Sweden have performed audits at this level. The findings were in most respects similar in both countries.

The Government has not followed up to ensure that the internal management and control of information security in public administration is satisfactory. The Government has not taken sufficient initiative to improve the conditions for the administration's work on information security. Few new measures to develop a good culture of security have been implemented or initiated.

Inexplicit requirements and mandate

Not many measures have as yet (November 2007) been taken to support the agencies' management and control of information security.

The top management of the audited agencies have no clear understanding of what requirements and rules apply to their information security work, for example as regards management accountability and the agencies' risk analyses.

The Government's strategy for information security provides no explicit guidance. It is aimed at society as a whole and does not lay down specific requirements for the agencies. In keeping with tradition, the Strategy "addresses" various security "issues" instead of directing the "resolution" of security "problems" – tiptoeing around the problems instead of dealing with them head-on and demanding results.

In support of the public administration and in support of its work on managing the agencies, the Government has set up a number of expert agencies¹ with responsibility for various issues relating to information security. The Government has not however given the expert agencies a sufficiently explicit mandate, which has meant that they have had difficulties in giving the Government a complete picture of the information security problems at the agencies.

The Government has not followed up the agencies' work on information security

The Government has been unable to present any complete picture of the problems affecting public administration. Furthermore the Government has not required the central government agencies to report on the principal problems affecting information security. Finally the management issues in central government agencies have not been touched upon in the directive to the government investigations relating to information security issues.

Deficiencies in the Government's preparation of information security issues

The Government's organisation of the work done by the Government Offices on information security issues and the management of the expert agencies is together insufficient to handle the agencies' problems with their information security. No ministry is explicitly responsible for carrying out an overall assessment of the agencies' internal management and control of information security. Strong signals are required (such as serious security incidents) for the Government Offices to become aware of deficiencies in individual agencies. Strong signals are also required in order to identify general problems in public administration.

Other relevant management problems

Incident warning systems for digital infrastructures have a limited number of participants and information to the general public is limited to a brief monthly summary of registered incidents. Government has not solved problems of financing cross-sector measures. There is a lack of coordination of regulations of information security.

Findings on agency level as to internal control of information security work within the agencies

All Nordic SAI have been active at this level. SAI Finland, Norway and Sweden have made similar findings. They are described below. SAI Denmark did report a much brighter picture of the information security situation in Denmark this is also commented on in the Conclusions section.

On the basis of current standards (whether or not they have been adopted as regulations of the government) the overall conclusion of the SAI is that agencies are not working systematically on their management and control of information security.

Management problems

The incidents have been caused by among other things deficiencies in the work on information security done by the top management of the agencies concerned. The most important management problems are:

- Management is not visible and are uncertain as to what their tasks are in the information security work and how those tasks should be carried out.
- Lack of formally decided, documented and updated operational policies and procedures
- Management do not request any clear documentation showing the kind of risks and threats that exist for the agency concerned.
- Management do not therefore have sufficient insight into what measures they should prioritise to protect the agency.

- International standards are still little known in public administration. Denmark being the exception due to the DS 484 standard (equal to ISO 17799, a former version of ISO 27001 – ISMS Information Security Management Systems-Requirements and ISO 27002 Code of practice for information security management). This is quite well known in public service since its adoption as ordinance.
- Management's decisions regarding security measures are not complied with.
- Also, management do not follow up to ensure that the security fulfils management's requirements.
- Management do not make sure that they are informed that important measures such as continuity plans, reporting and handling of incidents have been carried out and are functioning as intended.
- Management underestimate the importance of staff training and information, including training of and information to other management personnel and boards.
- Only a minority of agencies have up-to-date emergency preparedness plans.

Other problems related to this level:

- Some work has been started to define what infrastructure is critical for society, but authorities do not yet have a clear overview of what critical IT infrastructure is and of the systems of which the infrastructure consists.
- The public bodies working on IT security have prepared guides for conducting risk and vulnerability analyses, and many activities are being carried out to further develop methods and tools. However, the authorities have to a lesser extent placed emphasis on making arrangements for these methods to actually be used. Nor have any arrangements been made to enable the use of knowledge obtained from the analyses when prioritising security measures irrespective of sector.
- Segregation of duties is not mirrored in rights of access.
- Weaknesses are common in access controls to sensitive data and programs. Sign on / log in procedures are often deficient, passwords used are unsafe.
- Weak procedures for change and termination of access when an employee has a leave of absence, change of workplace or employment comes to an end. This is also valid when it comes to access rights for external consultants.
- There are often many unused login accounts, impersonal accounts and too many people with administrator rights

¹ The Emergency Management Agency, the Security Service, the National Post and Telecom Agency, the National Defence Radio Establishment, the Administrative Development Agency (Verva), the Armed Forces, and the Defence Materiel Administration.



- There is often no system for monitoring logs, and weaknesses in protection of log files. Lack of possibility to trace a transaction.
- Policy on outside use of laptops and retrieval of data is often lacking
- Failure to remediate weaknesses uncovered long ago
- Outsourcing: Information security issues, responsibilities etc. are not comprehensively defined in agreements, procedures are not adequately described; lack of written descriptions, SLA is not used to determine responsibilities
- Physical security: Protection of IT premises is deficient e.g. regarding locking procedures, the location of premises, use of water, fire, smoke protection in premises is insufficient
- Agencies often lack valid licences for software
- Production, training and testing environments are not separated, e.g. testing or training is performed in production environment
- Backups are not taken systematically and restoring data from backups is not properly tested
- Backup hardware does not exist or it has not been not tested; and often plan/guidelines how to use reserve equipment is lacking
- Recovery plans – both technically and organisational are often lacking or deficient
- Encrypted connections to the Internet are not used when necessary
- Virus protection and firewalls is not used or updated comprehensively
- Security weaknesses in applications are often not properly compensated with better controls in other domains

Findings on project level and in information systems as to information security

Information system projects are often delayed and overrun their budget. This often gives little time to consider security issues. These issues are therefore taken into account much too late or not at all. New systems are implemented despite the absence of acceptance testing and with absence of a documented approval for operation.

Vendor – customer responsibilities are often unclear, especially regarding outsourcing and where many suppliers are involved. There are often deficiencies in ordering changes/modifications. The suppliers seem to “dictate” the content, and security considerations are often not handled properly in the contracts.

3. Conditions for the SAls to perform IT and Information Security audits

One major conclusion is that SAI Denmark performs IT audits under quite different conditions compared with the other Nordic SAls. In Denmark there seem to be, in our opinion, stronger IT governance (including Information Security governance) on political level and on agency top manager level. Consequently there is a stronger formal legislation for Information Security in public administration.

These conditions give the SAI Denmark good arguments to perform IT audits focusing on risk management based on undisputable audit criteria. The audits are done in a rather quick manner with short reports. The audit design gives the SAI time to make frequent follow up audits (up to 50 audits each year). The other Nordic SAls have weaker legislation for IT and Information security. The audits purpose is often to find weaknesses in the Information Security measures. The audits are rather time consuming. The Performance Audit reports are often quite long.

Driving forces

In Denmark, compared with the other Nordic countries, there has for several years been a strong engagement and awareness for IT governance, including the development of e-government and electronic data exchange in public sector, from political level and consequently from Top Manager in the public sector.

The driving forces for the use of IT in Denmark seem, in our opinion, to be stronger and have more impact on the public sector compared with other Nordic countries. As a consequence of strong driving forces for the use of IT in Denmark, SAI Denmark has an IT Audit with clear status in the SAI, among agencies and also on the political level.

Regulations to be used in auditing Information Security

In November 2007, there are differences between the Nordic countries concerning the regulations for Information Security. The differences have consequences for the SAls IT audit perspectives, questions, norms and activities.

In Norway there is no formal regulation for Information Security, except for confidentiality. There is no common guidance for the public sector. In Sweden there has been guidance for the public sector but no formal regulation for Information Security, except for confidentiality. Late in the autumn of 2007 the Swedish agencies got a legal rule issued by an agency under the Government. The Information Security Rule is based on the standard ISO 27001. In Finland there is no formal regulation, Instead there is Information Security guidelines made by Government Information Security Management Board.

In Denmark since 2003 there has been a formal regulation called DS 484 for Information Security based on the standard ISO 17799 (a former version of 27001).

In November 2007 Denmark seems to have the most formal (strongest) regulation, and Norway maybe has the weakest regulation. As a consequence the status of the audit norms in November 2007 was very different in Nordic countries. Given a strong regulation, you get strong audit norms with clear audit questions. If you have a weaker or non existing regulation the SAI needs to develop the norms and questions, perhaps with help from standards, and also to convince the agencies that the norms and questions are justified and fair.

Designing Information Security audit projects and reporting audit findings

There are rather big differences in the design of audits between on one hand SAI Sweden, Norway and Finland and on the other hand SAI Denmark. The differences could be explained by different audit cultures and different external conditions (driving forces for the use of IT, and the existence of formal regulations) for the SAI.

SAI Sweden, Norway and Finland

- SAI Sweden, Norway and Finland make overall audits. The SAls focus on different aspects of the Information Security Environment, collect audit evidences of insufficient information security on several levels.
- Management: IT-management level and lower levels
- Processes/procedures: The Information Security Procedures
- Security measures: Proving weaknesses in the Information Security activities
- Security status: Controlling Information Security within the Information System

The audit projects are rather time consuming, from a couple of months to half a year or more. Without a given formal regulation for Information Security, the SAI need to develop rather complex audit criteria in order to ask questions about and to understand the Information Security procedures and measures being taken by the audit entity. The results from the audit projects are often long reports.

In SAI Sweden the Financial Audit function audited the Information Security in ten agencies. The audit findings pointed out common management problems. The problem picture was the starting point to make a performance audit of the Government's (Cabinet's) Information Security Governance.

SAI Denmark

In Denmark the base for the audits in the public sector is the standard DS 484. The standard has a Top Manager focus. This means that top managers should look upon

the use of IT as an integrated part of the agency's daily activities. From this point of view top managers and managers on lower levels have the responsibility for running well functioning and secured information systems. Given this external condition SAI Denmark focuses on auditing the management of the risk areas concerning the use of IT and related Information Security matters.

The audit starts with a risk evaluation as a base for developing audit questions. The way to collect audit information is via interviews with the business managers, the IT manager and persons responsible for the daily running of the IT-systems. The questions focus on the management of identified risks: How have you controlled? How do you act on the control results? The results of the audits are reports on two levels. A short 2 – 3 pages memo for the managers and a more detailed report with findings, risks etc. There is also a special memo given to the financial auditors about consequences of the IT-security findings. The audits often don't take more than one month. The SAI has the capacity to perform 50 IT audits each year, mostly follow up audits.

One important factor is the rapid IT development. We all agreed to the strong need for auditors in general and IT auditors in particular to strive for more knowledge about the IT development, threats and their consequences for the public sector. The Nordic national security agencies have an important role to discover threats and share this knowledge to all public agencies.

4. Conclusions

Summary of Audit Findings

Findings on government control of information security work within the public administration

SAI Norway and SAI Sweden have performed audits at this level during 2005 – 2007. The findings were in most respects similar in both countries. The Government has not followed up to ensure that the internal management and control of information security in the public administration is satisfactory. The Government has not taken sufficient initiative to improve the conditions for the administration's work on information security. Few new measures to develop a good culture of security have been implemented or initiated.

Findings on agency level as to internal control of information security work

All Nordic SAIs have been active at this level. SAI Finland, Norway and Sweden have made similar findings. SAI Denmark reported a much brighter picture of the information security situation in Denmark.

On the basis of current standards (whether or not they have been adopted as regulations of the government) the overall conclusion of the SAIs is that agencies are not working systematically on their internal management and control of information security.



The importance of security standards imposed on agencies, and government offices/ministries, IT security is illustrated by the Danish experience. In 2002 audits showed weak focus on IT governance. There were no appropriate controls in place in many agencies. In January of 2004 the Danish government decided to implement the DS 484 standard on information security (equal to ISO 17799). SAI Denmark focused on the management's acceptance of the standard. In 2007 the DS 484 standard was nearly implemented in all the ministries and most of the agencies. The present situation is described by the SAI as follows:

- General acceptance of the risk evaluation concept
- General good IT governance from the top (both in departments and agencies)
- Generally acceptable level of controls in the IT environment
- Recovery plans – both technically and organisational are one of the weaker areas
- The SAI's overall opinion is that there is now a quite good level of security.

SAI Denmark feels reassured that the standard has had these good effects. We know that also other governments among the Nordic countries are contemplating this step, having watched what has happened in Denmark.

Findings on project and Information System level as to information security

Information system projects are often delayed and overrun their budgets. This often gives little time to consider security issues. These issues are therefore taken into account much too late or not at all.

New systems are implemented despite the absence of acceptance testing and with the absence of a documented approval for operation.

Vendor – customer responsibilities are often unclear, especially regarding outsourcing and where many suppliers are involved.

There are often deficiencies in ordering changes/modifications. The suppliers seem to "dictate" the content and security considerations are often not handled properly

Conditions for IT and Information Security audits

In the light of the experiences of SAI Denmark we discussed differences in audit questions, developing audit norms, finding data sources, using different methods for collecting and analyzing data, and reporting.

One major conclusion is that SAI Denmark performs IT audits under quite different conditions compared with other Nordic SAIs. In Denmark there seems to be, in our opinion, stronger IT governance, including Information Security governance, on the political level and on agency top management level. Consequently there is stronger legislation for Information Security in public administration.

These conditions give SAI Denmark good arguments to perform IT audits focusing on risk management based on undisputable audit criteria. The audits are done in a rather quick manner with short reports. The audit design gives the SAI time to make frequent follow up audits (up to 50 audits each year). The other Nordic SAIs have weaker legislation for Information security. The audits purpose is often to find weaknesses in the Information Security measures. The audits are rather time consuming. The Performance Audit reports are often quite long.

Other conclusions

All SAIs reported that centralization of IT operations, outsourcing to IT service centers, is a growing tendency that will require attention from auditors. Administrative systems for accounting, payroll and HRM and other similar applications will be standardized (1 brand for all) and will to a much lesser degree be handled in-house as the case is today. In this respect we will return to conditions that existed in the 1980s.



SAI Pakistan's experience in ERP Auditing

Executive Summary

The office of the Auditor-General of Pakistan initiated the implementation of SAP/R3 ERP system in the year 2001 through the World Bank funded project titled "Project to Improve Financial Reporting & Auditing". The underlying purpose was to bring transparency, efficiency and effectiveness in the existing system of financial management across all the government organizations. Risk Based Methodology was adopted in testing the appropriateness of design of the system and its operating effectiveness. To test the design of the system we have obtained understanding of the system and its processes relating to transaction posting and reporting of financial results. Major observations that were made during the analysis are highlighted in this article.

Assessment of Data Sufficiency in SAP/R3 System:

FI Module

- Financial Statements for the year 2006-07 and 2007-08 are prepared in accordance with International Public Sector Accounting Standards – Cash Basis ("IPSAS"). The System assists in preparation of the IPSAS Financial Statements only to the extent of data available in the system, but does not itself generate such Financial Statements.
- Data migration from legacy system has not taken place. This has resulted in insufficient data due to unavailability of financial information in the System prior to the date the site became productive. Where site means a District Accounts Office or other Office where transactional level data is booked in the system.
- There has been delay in implementation of the System; not all sites are productive, several remain with partially workflow where the site became productive sometime during the year.
- Standardized formal year-end closing procedures are not followed resulting in significant difficulties faced while closing the financial year 2007-08. The financial year 2007-08 was not closed till 31 October.
- Fixed Assets Module is not productive for the year 2007-08. However, subsequent to the year end, steps have been taken to partially make it productive through mapping capital expenditures and recording in the Fixed Assets Module.

- Project Module is also not functional and the related losses are not reported by departments, therefore, the System is unable to generate the Project Expenditure Statement and Losses Report.
- Bank Reconciliation Statements are provided in the System and can be used for day end reconciliation with banks on a running basis. However, these reconciliations do not provide an "as at" status for reconciling items since there are significant amounts prior to the SAP implementation that still remain unreconciled.
- The petty cash module is not operational for the year 2007-08.

HR Module

- The Pension Module is partially implemented and only pension payments' reports of fresh pension cases subsequent to the productive date are available in the System, whereas payments are still being authorized manually.
- Non-availability of historical data in the GP Fund Module restricts the System's ability to provide reliable information showing the overall position of progressive balances of GP Fund subscribers. The GP Fund Ledger cannot be updated due to the lack of availability of such data.

Furthermore, in some of the instances where outstanding balances of previous advances have been adjusted, these are not being carried forward to the following year in the System due to some configuration problems.



Assessment of General Computer Controls and Application Controls in SAP/R3 System

- It was observed that backup hardware for critical information assets such as servers, switches, routers etc had not been arranged at audit sites to cope with any interruption to business.
- No disaster recovery site had been arranged to handle a disaster.
- Policies relating to important areas such as Business Continuity, Network Management, Virus Protection, Information Security had not been formulated.
- It was found that no protecting equipment such as firewalls, Intrusion Detection Systems etc had been installed to protect information assets from external as well as internal attacks.
- No network based anti-virus software was procured and installed at any one of the three sites rendering the respective networks vulnerable to the virus attacks from outside or from within the network.
- It was found that the documentation record for award/revocation/modification of authorizations was not proper and the written authorized user creation requests were mostly not found. Moreover, it was observed at AG NWFP & Punjab that the authorizations were not timely revoked or changed upon transfer or status change of the employee.
- While auditing, it was observed that the important feature of audit logging was not activated. This fact could lead to the unauthorized usage of the system without any accountability.
- While conducting audit, it was observed that the server sites at AG NWFP and Punjab were not located at physically secure places. Moreover, no arrangements in the form of security guards or any biometric recognition system were there to restrict people from server room access where equipment worth millions of rupees is housed.
- No training programs had been developed to make the employees aware of security of information assets.
- During the audit it was found that none of the wiring diagrams for the sites had been developed. This fact has made the network quite prone to failures for longer periods of time.
- The servers installed at AG NWFP and Punjab were not found to be meeting with the data processing needs i.e. their processing capability was not in line with the business requirements. This resulted in extra ordinary slow performance of the network.
- It was observed that not even a single handheld fire extinguisher had been placed at any of the server sites where expensive IT equipment has been installed. Likewise, no fire suppression system has been procured and installed at any of these sites.

Introduction to SAP R/3

System Application and Products, SAP R/3 ("the System") is a computer system that is designed to support complete business management tasks of a corporation, company or institution. SAP R/3 is used in business systems to handle invoice payment, production resource management and financial account control. These specific tasks are accomplished by employing application modules, often described with acronyms such as FI ("Financial Accounting") and HR ("Human Resources").

Modules process information through each and every component of the organization, using one secure R/3 system to share relevant information between parts of the organization, keeping the corporation up-to-date on latest technology and data information. Modulation is customized to provide specific technical requirements of an organization. A common database is employed among each of the mid-sized to large-size corporations that utilize R/3. R/3 may also be used by small business, allowing business to prosper without having to worry about changing systems.

An additional benefit to using SAP R/3 is that it combines with a corporation's previously existing computer system. R/3 uses the ABAP/4 programming language and allows for the possibility of several computers of differing manufacturers to conjoin into one solid working database, operating in the open system or client/server environments. SAP R/3 is a Windows and Menus driven application containing graphical objects.

Implementation of the system

The office of the Auditor-General of Pakistan initiated the implementation of SAP/R3 ERP system through the World Bank funded project titled "Project to Improve Financial Reporting & Auditing". The underlying purpose was to bring transparency, efficiency and effectiveness in the existing system of financial management across all the government organizations. At present The Controller General of Accounts Office ("CGA office") has broadly utilized the following modules and sub-modules of the system;

- Human Resource ("HR")
 - Sub modules of HR
 - General Provident Fund
 - Pension
 - Payroll
 - Hiring
- Financial Information ("FI")
 - Sub modules of FI
 - Accounting
 - Controlling
 - Treasury
 - Reporting
 - Fixed Assets

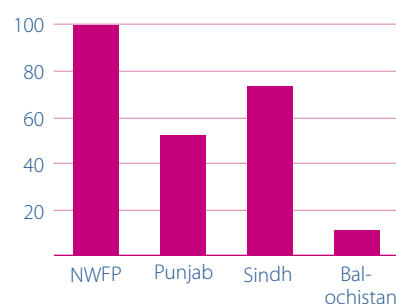
Implementation of SAP is through a gradual process in phases. Each year departmental budget (both current and developmental) is prepared by the Finance Department for each province. Budget reflects receipts and payments both by object and function. The same budget is uploaded on the AG server.

Current implementation status of SAP sites

SAP is being implemented in all the districts of Pakistan, AG offices of all provinces and the Federal Government. There are in total 112 SAP sites (NWFP, PUNJAB, SINDH and BALOCHISTAN), of which 36 are fully live, 55 are partially operational and 21 remain un-operational. The percentages of sites that are fully productive are as follows:

Percentage of Productive Sites

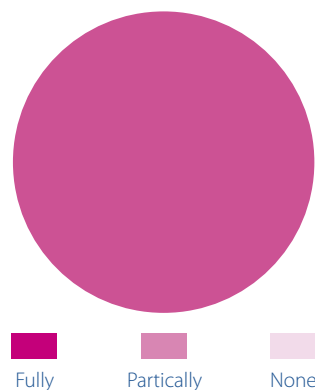
Only those sites are included that were productive through the year



As can be seen from the graph above, almost all sites of NWFP are productive. On the other hand, almost 70% of SAP sites in Sindh are on workflow whereas 49% sites of Punjab and 10% of Balochistan remain operational.

A further breakdown of these sites can be analyzed as follows:

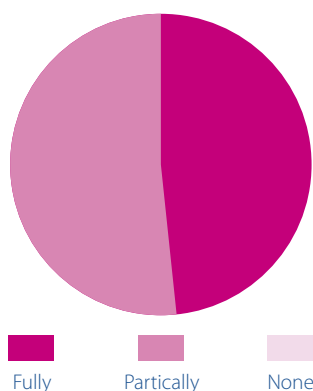
NWFP



All 24 districts of NWFP are productive. SAP has been implemented at these districts during 2005 and 2006. NWFP remains the only Province who's Financial Statements for the year 2007-08 have been generated using amounts supported by SAP System with slight differences as indicated in the above section.

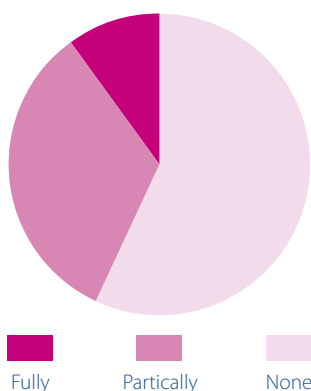


Punjab



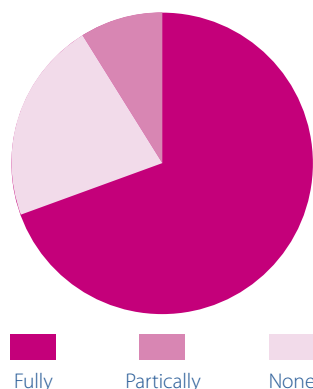
In the province of Punjab, out of 35 districts 17 are online and the remaining 18 are partially online. By 2008 year end all sites were on workflow and it is perceived that the financial statements for the year 2009 shall be prepared using SAP and supported by the underlying records of the System.

Balochistan



Balochistan require immediate attention as most of the sites remain offline or partially on workflow. Only three sites were on workflow during the year. Subsequent to the year end, 11 more sites had been made operational

SINDH



In Sindh, 16 out of 23 sites are on workflow, whereas 2 remain partially online and the remaining 5 are offline. A Mid-Term solution has been used to prepare the financial statements for the year 2008 and if the sites are not made operational in 2009 it is feared that a Mid-Term solution will continue to be used for the next financial year ending 30 June 2009.

Audit Objectives

The following were the objectives of the audit:

- To obtain reasonable assurance as to whether the complete, accurate and reliable financial information is available in SAP and that financial and other reports are generated from, or at minimum, supported by the System as required by the Financial Reporting Manual.
- To assess the effectiveness of General Computer Controls and Application Controls implemented for the SAP/R3 system.

Audit Scope

In order to meet the aforementioned audit objectives, data was collected from all the four provinces of Pakistan. Secondly, three sites; Lahore, Islamabad and Peshawar were selected to ascertain the effectiveness of General Computer Controls.



Audit Objective 1:
Data Sufficiency Analysis in
SAP/R3 System

Purpose of Data Sufficiency
Analysis

The purpose of SAP Data Sufficiency Analysis is to obtain reasonable assurance as to whether complete, accurate and reliable financial information is available in SAP and that financial and other reports are generated from, or at minimum, supported by the System as required by the Financial Reporting Manual. The analysis has been performed to identify any insufficiency, errors or inconsistency in financial data available in SAP.

Financial data is deemed to be reliable when such data can be drilled down to the transaction level, and the transaction record provides comprehensive details of the transaction and related sources of information.

Scope of Analysis

SAP Data Sufficiency Audit Procedures have been designed (refer Data Sufficiency Audit Programme) to obtain sufficient appropriate evidence that specific procedures for collecting and recording of documents, journals and ledgers, maintenance of registers in compliance with the Accounting Policies and Procedures Manual ("APPM") is done using the System.

The analysis is performed to reasonably ensure that the Monthly, Quarterly and Annual Financial Statements are generated from, or at minimum, supported by the System. Data Sufficiency tests the following assertions:-

- Completeness
- Authenticity
- Timeliness (data is entered in the correct accounting period)
- Correct data valuation
- Precise account assignment
- Accurate summation
- Proper posting
- Maintenance of adequate logs at different stages such as where a document is *parked, changed, revised* or otherwise *altered* within the system.

Significant Risks found while
assessing Data Sufficiency in
SAP/R3 SYSTEM

We have obtained an understanding and analyzed the financial data processing systems and identified the potential risks that may result in insufficient data in System. These risks are:

- Improper migration of data from the legacy system may result in insufficient data due to lack of historical information prior to the date the sites became productive.
- Lack of integration between various modules or unavailability of certain modules may result in manual adjustment being made for reporting purposes resulting in inadequate data in the system.
- If posting data is not reconciled on a timely basis, that is, monthly, there is a risk that errors may occur and remain undetected for an extended period of time. These errors may make

it difficult to carry out the year-end closing procedures. Another obvious consequence of this is that management could make decisions based on unreliable information, which would then lead to serious, irreversible errors.

- There is also a risk that management may not be able to identify why or where an error occurred in order to prevent it from recurring and from jeopardizing the System's compliance with sound accounting principles.
- In addition to the risk of errors resulting from reconciliation that does not occur on a timely basis, there are other risks in month-end closing that must be eliminated using system-wide controls and checks. Inadequate data backup will make it difficult to restructure information for external purposes if errors do occur.
- Risks related to the balance sheet and receipt and payment account may arise due to the type of accounts summarized in the individual year-end closing items. If allocations do not match the formal requirements, the year-end closing procedure may be rejected. Incomplete data increases the risk of erroneous information being used by management.
- Unskilled staff involved at the DAO level to enter complete information relating to a particular transaction and subsequent posting may result in inappropriate posting and incomplete information relating to that transaction.
- The lack of available historical data in the System resulting in manual data punching of opening balances for

Financial Information on Module (FI Module)

Summary of productive modules

Province	Receipts	Expenditure	Assets Management	Treasury management	Liabilities	Projects	Commitments	Reporting
NWFP	Productive	Productive	Non productive	Non productive	Non productive	Non productive	Non productive	Non productive
Punjab	Module wise status was not provided to us and we were given an understanding that the said records are not maintain at the AG Office.							
Sindh								
Balochistan	Productive	Productive	Non productive	Partially productive	Non productive	Non productive	Non productive	Partially productive

Preparation of Financial Statements

Accounts for the year 2007-08	SAP	Mid-term Solution
NWFP	✓	×
Punjab	×	✓
Sindh	×	✓
Balochistan	×	✓

balance sheet items raises the risk of wrong opening balances being entered, transposition errors or misclassified opening balances.

- Incomplete data in the System may result in complicated consolidation procedures making it more prone to error and wrong classifications/groupings resulting in inappropriate financial reporting.

The financial statements for the year 2007-08 of NWFP have been prepared as per SAP and the financial statements of other provinces are prepared using a Mid-Term Solution.

Mid-Term Solution

A Mid-Term solution has been adopted for preparation of Provincial Financial Statements as the SAP was not fully implemented in the Punjab, Sindh and Balochistan. The Mid-Term solution is used to enter monthly accounts data at the respective provincial AG's Office for those Districts that are not on workflow and they did not generate financial statements in SAP.

Accounts are received in three different formats i.e. SAP Reports for sites that are productive, MS Excel format for sites that are on workflow but are not productive i.e. their Financial Reporting Modules are not operational and manual/hand written format.

Districts that are on workflow export their data in the specified format, while districts that are not on workflow enter data on excel sheets in a specified format, in some districts accounts are received in hand written format which is entered in the workbook at A.G Office.

Most SAP sites became live during the fiscal year 2007-08 and therefore complete data for that year is not generated through the System. The System provides support data for preparation of financial statements; however, a complete set of IPSAS based financial statements are not generated by the System.

Furthermore, information relating to Appropriation Accounts is extracted through the System, whereas, historical data for generation of Finance Accounts prior to implementation is not available.

The reporting format, as incorporated in the System, is in accordance with the requirements of the Financial Reporting Manual (FRM).

Summary of the comparison of the amounts of the financial statements for the year ended 30 June 2008 with the underlying records in SAP is as follows in each province:

NWFP

Transactional Level Data

Statement of Receipts and Payments

Rupees in Millions

For the year 2007-08	As Per Accounts	As Per SAP	Variance	Percentage
Receipts	115,489	92,394	23,095	20.00
Payments	122,608	96,846	25,762	21.01
Assets	138,495	Not Available	–	100.00
Liabilities	138,495	Not Available	–	100.00
Commitments	Not Yet Adopted			

PUNJAB

Transactional Level Data

Statement of Receipts and Payments

Rupees in Millions

For the year 2007-08	As Per Accounts	As Per SAP	Variance	Percentage
Receipts	422,780	66,760	356,020	15.79
Payments	440,787	146,106	294,681	33.15
Assets – Public	318,724	960	317,764	0.30
Account Payments				
Liabilities – Public	326,773	58,853	267,920	18.01
Accounts receipts				
Commitments				

SINDH

Transactional Level Data

Statement of Receipts and Payments

Rupees in Millions

For the year 2007-08	As Per Accounts	As Per SAP	Variance	Percentage
Receipts	–	–	–	–
Payments	–	–	–	–
Assets	–	–	–	–
Liabilities	–	–	–	–
Commitments	–	–	–	–

Balochistan

Transactional Level Data

Statement of Receipts and Payments

Rupees in Millions

For the year 2007-08	As Per Accounts	As Per SAP	Variance	Percentage
Receipts	93,125	4,074	89,051	4.37
Payments	97,817	8,694	89,123	8.89
Assets				
Liabilities				
Commitments				



Since, the implementation of SAP either took place during the year or subsequent to the financial year end. No complete data was available for any province for the preparation of the financial statements.

Grant Expenditure Analysis

Grant-Expenditure Analysis is one of the major reports amongst six reports generated by the System but the required report was not submitted to the Principal Accounting Officer for his comments. No reports for Grant-Expenditure Analysis were available in system for the year ended 2007-08. Reports are available from July 08 onwards.

Due to unavailability of complete year's data, reports generated by the system were incomplete for the year ended 2007-08 and could not be used for the decision making process. Other accounts whose expenses are being met from Grant Expenditure use manual adjustments and are not system generated.

Cash Flow Statement

The System generates Cash Flow Statements, which are reconciled with the underlying records to the extent the data is available in the System. Periodic cash flows are analyzed by type of activity as required by the IPSAS 2. Data for the year 2007-08 is reliable; however, in the absence of historical data in the system, Cash Flow Statements containing opening balances for the year 2007-08 are not reliable.

Year End Closing

Standardized formal year-end closing procedures are not effective, which might cause significant difficulties in closing the financial year 2007-08. Therefore, formal procedures need to be implemented to ensure smooth and timely year-end closing and training is needed on standardized year end closing procedures.




Financial years closed for cash transactions on 30 June remain open for 4 months up to 31 October for further corrections and updating.

A proper trial balance is not generated by the System as required under Section 7.4.4.7 of APPM. Several other reports are generated to obtain the required information; which is appropriate in the Cash Basis Accounting as only year-to-date figures serve the purpose. But for liabilities and assets, the information as reflected by the trial balance is not easy to obtain.

PIFRA

PROJECT FOR IMPROVEMENT IN FINANCIAL REPORTING AND AUDITING


Communication

PIFRA Vision

PIFRA produces accurate, timely and meaningful accounts, which cater to the needs of the users. The project helps produce analysis of budgeted data reported in monthly accounts producing significant deviation between actual budgeted account and total actual expenditures and receipts.

WWW.PIFRA.GOV.PK



Fixed asset Module

Fixed assets register as required under 13.4.5 of APPM is not productive for the year 2007-08. However, subsequent to the year end, steps have been taken to partially make it productive through mapping capital expenditures and recording in the Fixed Assets Module.

Reports regarding additions or deletion of assets are not being maintained in the System because of non-functionality of fixed assets module. As a result, adjustments, additions and disposal of fixed assets cannot be verified in the System.

There is no policy of depreciating fixed assets with respect to their remaining useful life.

Project Accounting

Project Module is also not functional and the related losses are not reported by departments, therefore, the System is unable to generate Project Expenditure Statements and Losses Reports. In the absence of Project-wise expenditure budget codes, separate object-wise project reports cannot be generated for the financial year 2007-08. However, from 2008-09 onwards, separate object-wise project budget codes have been assigned, so that separate project-wise and object-wise reports can be generated.

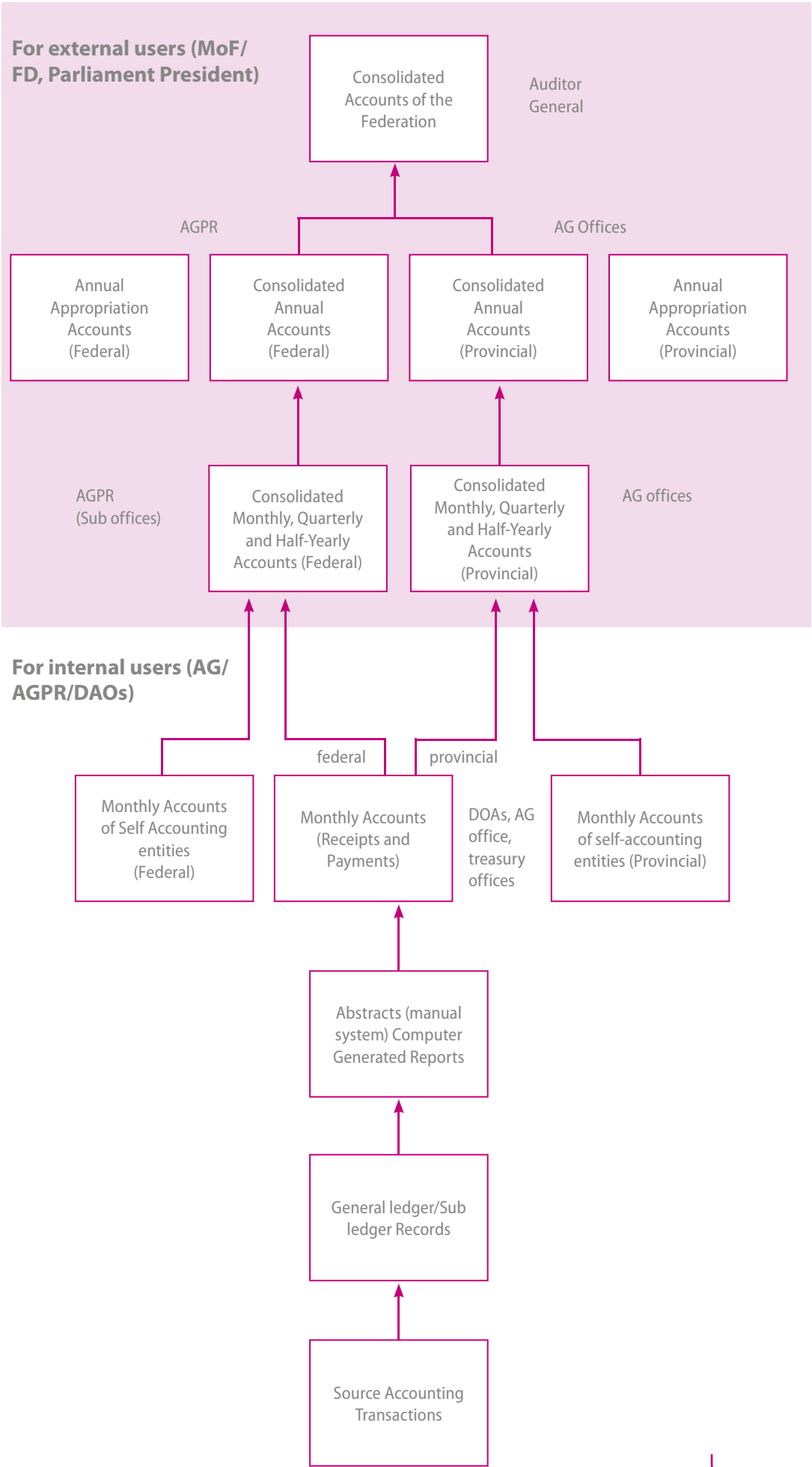
In the absence of project-wise expenditure budget codes, separate object-wise project reports cannot be generated for the financial year 2007-08.

Bank Reconciliation Statements

Bank Reconciliation Statements are provided in the System and can be used for day end reconciliation with banks on running basis. However, these reconciliations do not provide an “as at” status of reconciling items since there are significant amounts prior to the SAP implementation that still are not reconciled.

Balances of Chart of Accounts

We observed that the Receipt and Payment balances of both Consolidated Funds and Public Accounts are correct in the System for the year, however, correct opening balances have not yet been entered in the System. In the absence of correct opening balance for the year 2007-08, final year end trial balance cannot be obtained through the System.



Human Resources Module (HR Module)

Summary of productive modules

Province	Payroll	Pension	GP Fund
NWFP	Productive	Partially Productive	Non productive
Punjab	The information has not been made available		
Sindh			
Balochistan	Partially Productive	Partially Productive	Non productive

In order to ensure that HR Module and its sub-modules are operating effectively and the data provided by it is sufficient, we performed procedures to ensure that:

- Total amount as per HR module reconciles with the reported amount and to reconcile the payroll amount with the amount paid out of the bank and to ensure that there are no manual adjustments made to the payroll;
- The Payroll/Establishment Registers are maintained in the system (requirement of Section 16.3.3 of APPM);
- The adjustments to the "Payroll/Establishment Register" are made by the delegated officer in the payroll section (the notification is preferably to be maintained on the system).

NWFP

During our meeting with ADPO-HR it was demonstrated with figures for the month of June 2008 booked under the relevant GL heads that total payments authorized in the HR module and those actually booked in the accounts do not reconcile because of the fact that some manual payments were also authorized.

During our meeting with FRE we were informed that the requirement 16.3.3 of APPM is not met by the System as no access to DDOs' is available at present. However, DDO-wise Payroll Register is being maintained under the HR module by DAO/AG.

All the payments authorized through the HR module and posted in GL are principally required to be reconciled with figures of AB reports but comparisons of payments through the HR module and those reported in AB reports for the month of June 2008 and July 2008 shows differences as given below:

Summary of productive modules

Month	Payment as per HR module	Amount as per AB report (FI)	Difference	Remarks
June 2008	310,263,912	310,265,384	1,472	Needs further clarifications
July 2008	356,236,980	356,243,321	6,341	Needs further clarifications

Punjab

In the absence of the HR module report we were unable to compare the reported amount and the amount as per payroll.

Balochistan

We were only provided with the total CPS month-wise breakup booked under the relevant GL heads, but total payment authorized in the HR module and those actually booked in the accounts could not be ascertained because the concerned personnel were not aware of the requisite report in the System and we were not provided with the AB report.

There exists no system for reconciliation of total reported amounts of the HR module with the amounts paid out of the bank.

DDO-wise Payroll Register is being maintained under HR module by DAO/AG but no demonstration was given to us.

Pension Module

Procedures were performed to ensure;

- that the amount in the Pension module reconciles with the amount of pension in the accounts; and
- that the Pension Register is maintained in the system.

The Pension Module is partially implemented and only pension payments' reports of fresh pension cases from September 2007 onwards are prepared through the System, whereas, payment is authorized manually. It was further observed that monthly pension payments relating to cases before September 2007 are made by various branches of NBP, which are entered into the system on receipt of daily bank scroll by the respective provincial Treasury Office.

We have also observed that the pension register was not maintained in the System. Only computerized (SAP) reports showing calculation of pension is being generated from the System, which is used as a tool for comparison with the manual pension calculation.

Because of the above mentioned facts, without entry of payments in the Pension module, it is not possible to ascertain whether Pension module reconciles with the amount of pension in the accounts or vice versa.

In the absence of historical data prior to September 2007 in the System, we confined our verification of selected cases for the months September 2007 onwards, payments of which were computed through the System, and observed that payments authorized manually were according to the rules and scale.

GP Fund

We performed procedures to ensure;

- that the amount in the GP Fund Register agrees with the accounts.
- that the GP Fund ledger is maintained in the system and is updated regularly.
- that deductions are automatically made through the Payroll Register as per rules.

The GP Fund module is partially implemented, as deductions of GP Funds are regularly being made and posted in the GP Fund Broad sheets and GP Fund Balance Sheets without historical data prior to workflow.

GP Fund Register and GP Fund Ledger were not provided, however, GP Fund Broad sheets and GP Fund Balance Sheets of the individual subscribers were available in the system serving the purpose of the objective register.

Fifteen payments from the GP Fund that were authorized manually and entered in the System under the individual accounts on case-to-case basis were selected on a random basis, for each province. For some of the selected cases closing balances are not being carried forward to the next year in the System due to some configuration problems. We have been given an understanding that the problem has been communicated to Siemens for remedial action.

The system is unable to provide information showing the overall correct position of progressive balances in the absence of historical data, however, monthly deductions through payroll reconcile with the accounts.

The GP Fund Ledger (Broad Sheets) is being maintained in the System but it cannot be updated in the absence of historical data.

- Further, there are unusual breakdowns in the System that result in delayed extraction of data from the servers. Certain reports take days to complete and any breakdown results in loss of active reports resulting in loss of precious time.

Conclusion

Pension, GP Fund, Commitments, Banking and Fixed Assets modules in all the District Accounts Offices are not productive or partially productive due to technical reasons.

Historical data prior to inception of application SAP is not available in the system, therefore the System cannot provide reliable upto date Financial Reports.

Pursuant to the decision of the Auditor General of Pakistan, annual financial statements for the year 2006-07, which are the latest presented annual financial statement, have been prepared under the International Public Sector Accounting Standards (IPSAS)-Cash Basis issued by IFAC. The System, however, does not provide complete information for preparation of financial statements in the light of IPSAS.

The pace of transition from a manual approach of book keeping to system based approach needs to be increased, existing sites are required to be appropriately maintained. True assense of the SAP ERP can only be achieved through its complete implementation with respect to major modules and sub-modules and their effective interaction.

Further, proper migration from legacy system to SAP R/3 should be carried out through integration with the older system and importing data from that system to SAP R/3, so that the historical data prior to workflow can be extracted from the System.

Human resource is needed to be mobilized and equipped with the technical skills of operation of SAP ERP as effective implementation is only possible through trained staff, thus requiring the need for more training at the transactional level. Particulars of transactions are to be clearly mentioned and entered into the System.

IT Controls and Systems audit should be made part of the annual financial audit which shall include assessing the SAP Data Sufficiency. Proper procedures are to be designed in light of the new system and Audit Officers should be equipped with technical knowledge associated with IT Controls and Systems Audit.

Audit Objective 2: Assessment of General Computer Controls & Application Control in SAP/R3

Evaluation of Information in technology controls

During the audit of SAP/R3 system at three sites; Lahore, Peshawar and Islamabad, it was noticed that internal control structure relating to Information Technology was lacking some essential features which should have been implemented in order to increase efficiency, performance and security levels. An evaluation/overview of internal control structure is embodied in the following paragraphs.

Business Continuity / Disaster Recovery

Backup for Critical Hardware

Backup hardware for critical information assets such as servers, switches, routers etc is very important for the continuity of processing of data in the case of non availability of any of these information assets for any reason.

During the visit to the three AGPR offices, it was found that no such redundant hardware had been installed as a backup to cope with any disaster.

Disaster Recovery Site

The importance of the availability of servers for data processing compels the need for the arrangement of a Disaster Recovery Site where the system could be restored with the minimum possible amount of downtime in case of unavailability of primary server site. The Disaster Recovery site should be sufficiently distant and not be subject to the same natural/other disaster that could affect the primary site.

It was observed that no such arrangement had been made to counter the unavailability of central server site.

Auditor General of Pakistan, Islamabad



Business Continuity / Disaster Recovery Policy

The Business Continuity / Disaster Recovery Policy is a high level document and represents the strategic thinking of senior management regarding business continuity/disaster recovery. This document encompasses necessary preventive, detective and corrective controls. The policy formulation results in more detailed and dynamic documents such as procedures and guidelines which help and guide to tackle day to day problems faced.

It was found that no such policy had been finalized and approved.

Offsite Storage of backup files

The storage of backup files at physically secure offsite location is very important. This arrangement ensures the availability of data to restore the functioning of the system in case of any disruption.

During the visit of Lahore and Peshawar sites, it was noticed that there was no such practice of offsite storage of data. Recently a letter was written by Director FABS and addressed to various sites mentioning the respective offsite storage locations as well as the names of the responsible persons for handing over/taking over data.

Backup to Primary WAN / LAN Link

The PIFRA sites are connected to each other mainly through three types of WAN links such as DSL, DXX and Radio link. The need for reliability of data communication between these sites requires that there must be provision for alternative routing in case of failure of primary WAN link. Similarly, in case of LAN, redundant cable should be laid between critical hardware to ensure reliability of data communication if main cable is out of order for any reason.

It was observed that at all of the three sites, no arrangement for alternative/diverse routing had been made.

Environmental Controls

Water & Smoke Detectors

Water detectors are placed under raised floors and near drain holes and produce audible alarm on detecting the presence of water. Smoke detectors are placed near to the ceiling and below raised floors. Installation of both kinds of detectors in the server rooms as well as computer rooms is necessary for the safety of expensive information processing facilities.

It was found that no such detectors had been installed at any of the three sites.

Handheld Fire Extinguishers & Fire Suppression Systems

Placement of handheld fire extinguishers at visible locations is very important so that they can be used effectively in case of outbreak of fire. Similarly, the installation of fire suppression systems in server rooms and computer labs is necessary to control any outbreaks of fire.

While visiting the three sites, it was observed that not even a single handheld fire extinguisher had been placed at any of the server sites where expensive IT equipment has been installed. Likewise, no fire suppression system has been procured and installed at any of these sites.

Uninterruptible Power Supply

Uninterruptible Power Supply (UPS) installed with the servers, network devices and workstations typically ensures continued supply of power to the equipment in case of failure.

It was found that the UPS installed in the computer labs was not either functioning at all or working according to the specifications (standby time). Moreover, it is suggested that the UPS installed with the servers should be manageable so that the system does not all crash at once.

Network Management

LAN / WAN Policy

The LAN/WAN policy is a document which encompasses issues ranging from procurement and development of LAN/WAN to the maintenance, usage and change management of hardware/software. After formulation of this policy, standards, procedures and guidelines are developed for compliance and guidance in day to day working.

It was observed that no such policy had been finalized and promulgated.

Performance of Servers

The servers installed at AG NWFP and Punjab were not found to be meeting with the data processing needs i.e. their processing capability was not in line with the business requirements. This resulted in extra ordinary slow performance of the network. It is suggested that the processing capability (no of processors) of these servers may be enhanced immediately to avoid slow performance/downtime of the network.

Wiring Diagram of Network

The local area networks at various PIFRA sites have more than 100 computers connected and hence the architecture is complex. In such situations, the wiring diagram of the

network becomes very important as in its presence, it is easier and convenient to trace any fault that occurs.

During the audit, it was found that wiring diagrams had not been developed at any of the sites. This fact has made the network quite prone to failures lasting for long periods of time.

LAN & Transmission Cables

It was observed at the AG Punjab Server Site in particular that the LAN data cables within the server room had not been arranged and secured properly. This may result in difficulty in tracing problems if any.

It was also noticed that, in the case of AG Punjab and NWFP, the transmission cable from the server room to the AG site was also not found to be secure. This fact posed the threat of failure of the whole network if this primary cable was damaged (as there is no redundant/backup link).

Diverse / Alternative Routing

There is no arrangement for diverse/ alternative routing which may result in the failure of the network when the primary link is down. It is suggested that where the sites are connected through the DSL link, as an alternative (where possible), radio link may also be established in order to increase the reliability and availability of the network.

Provision of Fail-over Devices

An equipment or device is termed to be single point of failure if in case of its unavailability the whole network becomes unavailable for working. It is therefore necessary to provide fail-over devices (as backups) for equipment installed at single points of failure in the network.

It was observed that at all of the three sites, no fail-over devices had been provided to prevent single points of failure in the network.

Firewall Implementation

At various PIFRA sites, internet facilities have been provided to the users. Because of this openness to the internet, the workstations as well as the networks are vulnerable to internet attacks. These attacks may result in damage to important data and hardware. It is therefore mandatory to install firewalls as a means of perimeter security of the network. These devices control the network traffic flowing in and out.

It was found that these devices had not been installed in the networks. This fact may result in exposure of individual computers to internet attacks which in turn may damage/ destroy the whole network.

Virus Protection

The term virus is a generic term applied to a variety of malicious computer programmes that send out requests to the operating system of the host system under attack to append the virus to other programmes. In this way, viruses are self-propagating to other programmes. A virus may alter computer files or fill computer memory with junk to a point where the computer can no longer function. Anti-virus software can be implemented at the network as well as the workstation level. The network based anti-virus software installation enables to detect viruses as they enter the network whereas the workstation based software screens the software and data for viruses as they enter the machine. During the audit it was observed that:

- No network based anti virus software was procured and installed at any one of the three sites rendering the respective networks vulnerable to the virus attacks from outside or from within the network.
- There was no formal procedure in place to update workstation based anti virus software through live updates provided at the time of procurement of hardware.
- There was no formal procedure in place at AG Punjab to install operating systems (windows) from original licensed master copies.
- The flash and CD ROM drives of workstations at AG Punjab and AGPR Islamabad had not been disabled. This fact has increased the chances of spreading viruses.
- No arrangement had been made at AG NWFP and Punjab Local Area Networks to restrict installation of software at workstations. Moreover, there was no practice of scanning software before installation.

- At all of the three sites there was no practice of checking workstations for virus and worms on a periodic basis.
- No training had been imparted to create awareness among the users in this regard.

Protection of Information Assets

Security Policy and Procedures

The information systems security policy provides framework for designing and developing logical and physical access controls. The basic purpose of this policy is to protect the information assets from all types of risks-accidental or intentional. The responsibility for implementation of security policy to an appropriate level of management is also fixed. After finalization of the security policy, necessary standards, procedures and guidelines are developed for compliance in day to day working.

It was observed that no such policies, standards and procedures had been developed as yet. This situation implies that the users still do not have any benchmarks or guidelines to follow for implementing security of information assets under their custody resulting in high vulnerability against security threats.

Security Awareness and Education

In order to have effective security management of information assets, it is necessary that the users should be given appropriate training to foster security awareness among them.

During the audit of the three sites, it was found that no such training programme had been developed as yet.

Authorizations Award / Revocation Process

System access permissions are typically privileges given to a user to read, create, modify or delete a file or data or execute a programme etc. At PIFRA sites, authorizations are awarded to the users in order to do their work on computerized systems. The award of authorizations to the users should be documented and on need to do/need to know basis.

At all of the three sites, it was found that the records in this area were not kept and the written authorized user creation requests were mostly not found. Moreover, it was observed at AG NWFP & Punjab that the authorizations were not revoked or changed in a timely manner upon transfer or status change of the employee.

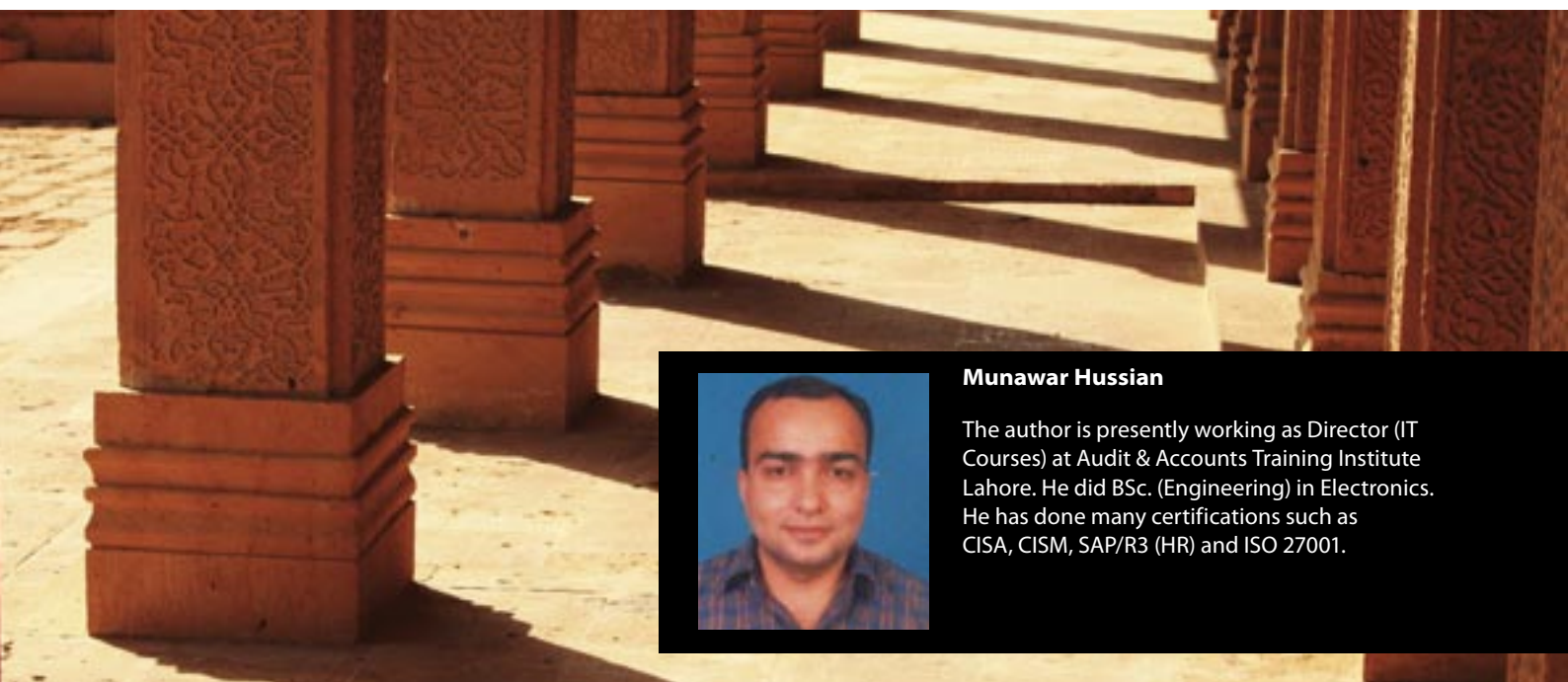
Audit Logging

The data stored through the SAP/R3 software at PIFRA sites is very critical and of utmost importance and hence needs high security measures to be taken accordingly. In addition to the restrictions imposed through user access permissions, it is also important to monitor other activities of a suspicious nature so that access violation may not occur. The SAP/R3 system has security features that log and report all levels of access attempts – successes and failures.

At all of the three sites, the important feature of audit logging is not turned on.

Physical Controls

While conducting audits, it was observed that the server sites at AG NWFP and Punjab were not located at physically secure places. Moreover, no arrangements in the form of security guards or any biometric recognition systems were there to restrict people from server room access where equipment worth millions of rupees is housed.



Munawar Hussian

The author is presently working as Director (IT Courses) at Audit & Accounts Training Institute Lahore. He did BSc. (Engineering) in Electronics. He has done many certifications such as CISA, CISM, SAP/R3 (HR) and ISO 27001.



SWITZERLAND

The Swiss ICT project management method

HERMES is an open method for the uniform and structured management of projects in Information and Communication Technologies (ICT). The method is mandatory within the Federal Administration for all ICT projects. HERMES is also used by other public administrations, universities and businesses.

HERMES describes a concrete process using a phase based model and specifies for each phase the required results and the specific roles. HERMES improves transparency and eases planning and execution of projects.

The Federal Administration, represented by the Federal Strategy Unit for IT (FSUIT), is the owner of the rights to the HERMES method. FSUIT designs and determines for the federal administration the ICT strategy, architectures, standards and methods and enforces their implementation using appropriate controlling measures.

The HERMES Method

HERMES is a method of managing, developing and executing projects in Information and Communication Technologies (ICT).

The advantages of HERMES

HERMES describes a concrete process using a phase based model, specifying for each phase the required results and the specific roles. HERMES improves transparency, eases planning and execution of projects.

The phase model

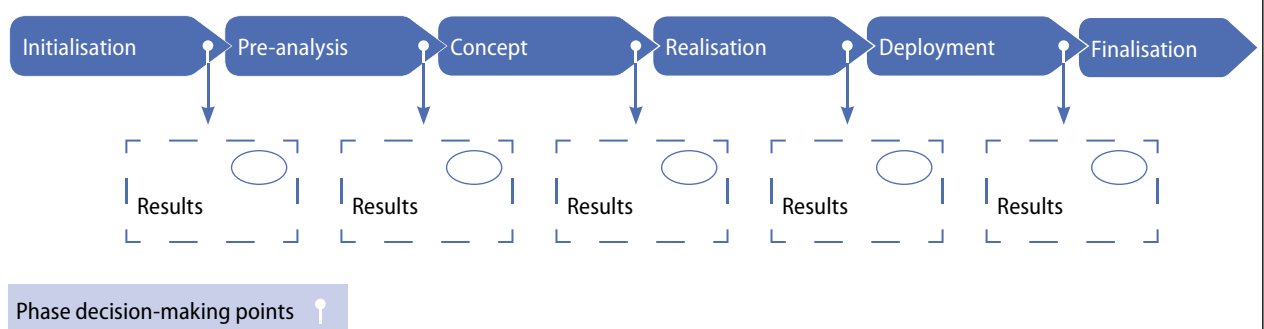
- To enforce a well structured project HERMES divides the process into 6 phases: Initialisation, Pre-analysis, Concept, Realisation, Deployment and Finalisation.
- These phases are defined in function of the required results and the decision-making points which are derived from them. The running of a project is structured by the decision-making points. At the end of a phase it has to be decided on the basis of the results, if the next phase should be started or not.

Two project types

HERMES distinguishes two types of projects:

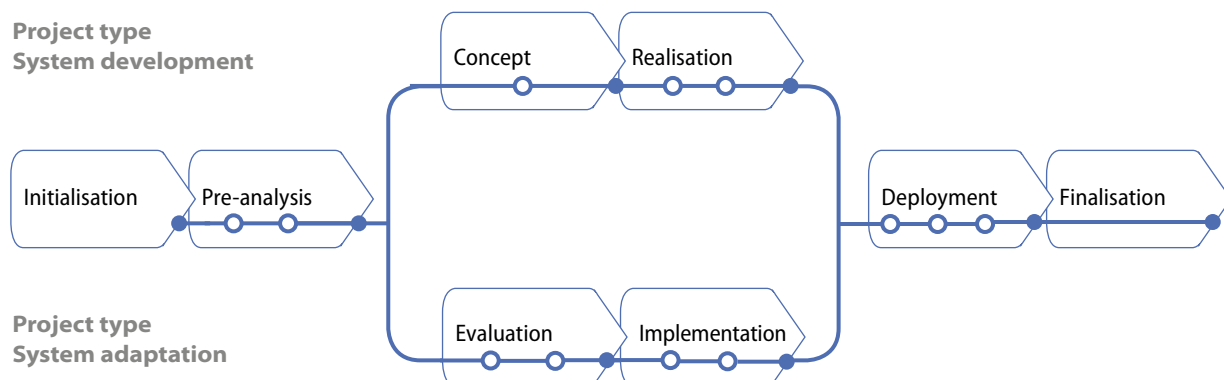
- System development – implementing a solution from scratch
- System adaptation – implementing a purchased solution

The phase model





The phase model is different in each case



Sub models for the transverse functions

The transverse functions and processes are described in the form of sub models. They are the same independent of the project type. They apply to most Information and Communication Technologies projects:

- Project management
- Quality assurance
- Risk management
- Configuration management
- Project marketing

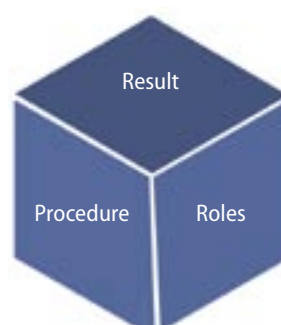
Result
Project Proposal
Report Concept
Report Pre-analysis
...
Operating Handbook
System design

Three views

In a project, the agreed results must be produced, the process must be evident and the roles have to be lived. For these reasons, a HERMES project is considered from three perspectives (views):

- View to procedures: How is the work performed?
- View to the obtained results: What is produced?
- View to the various roles: Who is doing what?

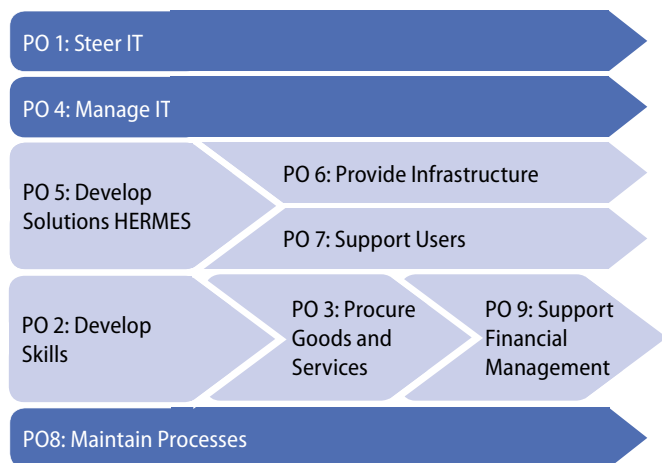
Procedure
Activity 1
Workstep 1
Workstep 2
Activity 2
Workstep 3
Workstep 4
Workstep 5
Activity 3



Roles
Project Leader
Purchaser
Designer of Solutions
User Representative
QA Expert
Risk Assessor
...

HERMES in the Federal Administration

The diagram illustrates the organisation of IT processes in the Swiss Federal Administration. The HERMES project management method is the core instrument of IT process P05, Develop Solutions.



Quality Assurance (QA)

The task of **quality assurance (QA)** in a project is to guarantee that the project results, i.e. the documented demands, correspond to the required level of quality. QA is a component of **total quality management (TQM)**, to which belong all those activities that relate to the establishment and implementation of quality planning, quality monitoring and quality assurance. Total quality management also covers the description of all processes and results of an organisation and the guaranteeing of the quality of those processes and results.

TQM is a task for management which forms the framework for the meaningful deployment of QA in a project.

QA in projects guarantees that all the necessary audits and tests are planned, prepared, effectively and comprehensibly carried out and adequately documented, based on the specifications of the TQM, or quality management system as the case may be. Beyond this, reporting on the implementation of QA activities and their results and trends is also one of the tasks of QA.

A foundation for planning QA is provided by project planning. The necessary audits and tests required for the assurance of quality will have been planned and agreed upon in project planning, keeping in alignment with the scheduled termination deadlines of the final and interim results, as well as with the **quality objectives** of the project.

Role responsibilities, the procedures for audits or tests (e.g. review of documentation and blackbox testing in the case of software), the audit and test criteria to be applied, deadlines, resources and other further organisational details are established each time. The purpose of the audits and tests is to demonstrate that demands are met, or to reveal possible deviations from the target specifications. In order to avoid a conflict of interest, the tasks of design and examination of a result must be taken on by different people.

Tests serve to verify the quality (requirements, shortcomings) of products or results. **Audits** serve the purpose of supervision and maintenance of the quality requirements in the project process in order to achieve quality in products or results.

Key aids to ensuring quality assurance in projects are:

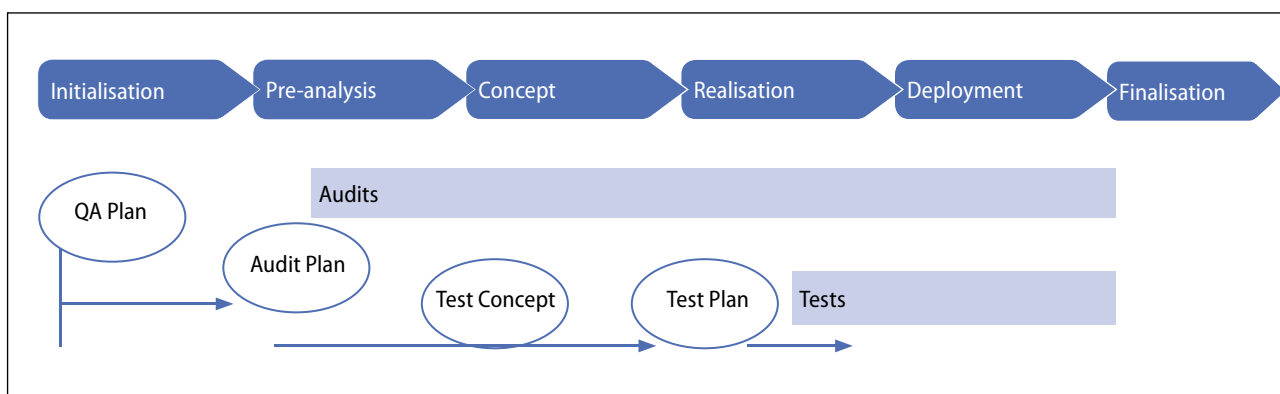
- The QA plan in which quality assurance for the concrete project is defined (with regard to the project results to be examined, guaranteeing adequate audit methods etc.)
- The audit plan which contains the planning dates for the individual audits together with the relevant details on implementing them
- The test concept which contains the technical framework and the test procedures
- The test plan which provides the organisation and time frame for the tests
- The audit and test notes and records that form the documentation for implementation and the results of the audits and tests performed

Information security and data protection

Current and consistent information is of great importance for the seamless functioning of processes of all types. Furthermore, in using Information and Communication Technologies respecting legal obligations and requirements for secure processing, saving and transmission of data is important. The notion that security costs money but generates no direct utility, together with the 'ostrich/head-in-the-sand' mentality and the hope that no security infringements will occur, leaves many projects close to a precipice without anyone realising.

The goal of information security is to recognise and protect the value of the task performed by data and service providers, with respect to **confidentiality, integrity and availability**. To determine such requirements a security policy can give guidance. Tasks are for example:

- Establishment of security requirements
- Development and maintenance of a security consciousness
- Implementation of security measures
- Review of the effectiveness of the security measures



- Continual improvement of the security theme in projects
- Information dissemination to management and the project team

By using defined **measurement categories** projects can become more efficient and effective in the area of security matters. Measurement categories can contain the following themes:

- The degree of coverage of the recognised risks
- The exposed security loopholes
- The exposed security infringements (viruses, penetration attempts, password usage and so on)
- The degree of effectiveness of measures introduced after discovery of security loopholes or infringements

The advanced state of today's Information and Communication Technologies offers a wide variety of increasingly powerful

possibilities for data management and utilisation. This conceals a particular danger for individuals or legal entities relating to data held on named or unnamed individuals. For this reason it is necessary to give due attention to the issue of data protection at the project conception stage of future ICT solutions.

Data protection legislation defines the permitted dealings concerning personal data in particular with respect to the creation, retention, application, alteration, release, filing or deletion of data. This should therefore be kept in mind during project work.

At the same time the coverage of the information concerning individuals plays a decisive role in its compilation of a data collection. **Personal data** together with personal profiles are to be particularly protected when they contain information on such things as:

- Religious viewpoint, world view, political or trade union views and activities

- The health, the private sphere or the person's race
- Social security claims
- Administrative or punitive legal sanctions or pursuit

If it can be established that the personal data is not sensitive but the intended use or the context of data processing is, then protective measures are still to be applied.

In considering rules for handling data from a technical viewpoint, one can differentiate between the following four levels which should be kept in mind in data protection:

- Application (ICT procedures)
- Transmission
- Data collection
- Operating system and hardware

Data protection measures have to be aimed at the lowest level in order to guarantee uniformity, integrity and effectiveness.

Risk assessment checklist

Area

Potential risks for the project

Project management, organisation

Planning

Is the planning up-to-date, adopted and active (is it being put into practice)?
Are the milestones suitable as measurements of the project's progress?
Are the deadlines and the number of milestones appropriate? Has the planning been communicated to the service providers and service procurers concerned?
Has the planning been communicated to the service providers and the service procurers concerned?

Decisions, implementation mandate and performance verification

Do the project committees, service providers and service procurers reach decisions promptly?
Are the decisions followed by a clear implementation mandate (including clear responsibilities), and does a verification of performance take place?

Information

Are the project participants well informed (promptly and in relation to their tasks)?

Resources: cost-effectiveness

Financial resources

Have the financial resources been agreed in writing with the competent authorities? Are the financial resources available?

Human resources

Have the human resources been agreed in writing with the competent authorities?
Are the human resources available, with the necessary qualifications, in the necessary numbers?

Unforeseen resource needs

Is there, for any reason, a potential for unforeseen resource needs?

Results: solution

Requirements

Are the service procurer's requirements complete and qualitatively practical?
Are the requirements sufficiently stable?
Is there a clear change management concept?

Application complexity; breaking down the task

Is the IT solution to be developed complex?
Is it practical to break down the task of implementing the requirements?

Interfaces to other systems in the environment

Are the interfaces to other systems in the environment well defined?
Are they compatible in content and timing?



User integration: acceptance

User integration	Have the future users been integrated in the project?
User acceptance	Is the user's acceptance verified regularly?

Service provider: company

Company stability	Are there signs that the company's existence is threatened, or that its ownership may change?
Ownership of results and work in progress	Are there signs that the company's existence is threatened, or that its ownership may change?
Technology transfer	Has the desired degree of technology transfer been assured?

The Development of HERMES

Next steps

Starting 2010	An Expert Committee on project management methods will be formed. Its purpose will be to evaluate current trends and requirements for project management methods. The evaluation should drive the development of the next version of HERMES.
2008-2010	Optimisation of the tools supporting the application of HERMES The highlights are: <ul style="list-style-type: none">● The electronic support of the project manager with HERMES PowerUser 2.0● Integration of the method in the enterprise● Analysis of different subjects in collaboration with the HERMES specialised groups of eCH● Electronic management of the HERMES manual content.

History

2008	Foundation of the specialised group HERMES in eCH (an association). HERMES PowerUser Release 2.0 is available in German and in French.
2007	The certification for HERMES project collaborator and project manager is available. SAQ is mandated to perform the certification. HERMES PowerUser (Release 1.0) is available.
2006	HERMES is a eCH standard .
2005	HERMES Systemadaption (SA) is published. It deals mainly with the "buy" part of system development (only in D and F). The rest of the manual is basically identical to the SE manual (see below).
2003	Revision of HERMES. Tailoring has been methodologically documented. A first manual covers HERMES Systementwicklung (SE) (essentially the "make" part of system development – in German and French – with all aspects of project management being covered). Publication of HERMES Manager in 4 languages. It provides useful guidance for the manager (the line manager responsible for the project manager) overall accountable for the whole project. HERMES is recognised as an open Standard . HERMES is more and more widely applied in the Swiss administration and in industry.
1995	HERMES 1995 is published in German. It is based on the German V model
1986	HERMES 1986 is published in German.
1975	First HERMES version. It is recognised as well as a standard outside the Swiss Administration.
1970	The Swiss Administration starts its own development of a project management method for ICT projects. The project is named HERMES.



The Fundamentals behind HERMES

Organisations develop projects in order to realize their defined goals, strategies and processes. For this reason, a project is always embedded in a specific environment which must be taken into consideration.

A **project** is a unique plan aimed at reaching a defined goal, at a defined level of quality, with limited time and resources. Projects can be of different types and categories.

The **project type** describes the kind of end result intended, the necessary intermediate or partial results, procedures and roles (such as system development, preventive maintenance, infrastructure, etc.).

The **project category** describes the project with reference to the three key project characteristics, importance (in relation to the corporate strategy), size (finances and resources) and risk.

HERMES can be **tailored** both to smaller and to large, high-risk projects. Such tailoring defines the key results and a procedure for the success of the project according to the given situation.

The **project manual** or project plan documents the specific application of HERMES and the decisions which follow from that application with regard to the results to be obtained, the decision points (milestones) to be reached, and the time planning.

Expert exchanges

The project management method HERMES is used in many administrations (cities, cantons, federal) and companies. In order to collect the needs and the modification proposals from the user community, a specialised eCH group has been created.

The eCH association encourages and approves eGovernment Standards in Switzerland. Members are authorities, private companies, organisations, academia and research institutes.

The board of directors has accepted the HERMES specialised group on 20 June 2008.

Want to learn more?

All the HERMES manuals in PDF format and further information on the Hermes project management method are available at <http://www.hermes.admin.ch/>

Hermes manuals are available and freely downloadable in German and French, with some also available in English.



For questions please contact Mrs Hélène Mourgue d'Algue, Responsible for HERMES at FSUIT, helene.mourguedalgue@isb.admin.ch



Massimo Magnini

Mr Massimo Magnini CISA, CISM, CIA is responsible for the Competence Centre IT Audits at the Swiss Federal Audit Office in Bern. He is also member of several national working groups and international associations like ISACA, IFACI, EUROSAT IT Working Group. Furthermore, he represents Switzerland at the INTOSAI Working Group on IT Audit.

intoit

The INTOSAI information
technology journal

© National Audit Office 2010 | Design
and production by NAO Marketing &
Communications Centre | DG Ref: 9078 |
Printed by Precision Printing

Printed on Greencoat paper. Greencoat is
produced using 80% recycled fibre and 20%
virgin TCF pulp from sustainable forests.

www.intosaiitaudit.org