# AN EVALUATION OF INTEGRITY CONTROL FACILITIES IN AN AS/400 ENVIRONMENT

by

MICHAEL LOUIS BOSMAN

SHORT DISSERTATION

Submitted in partial fulfilment of the requirements for the degree

MASTER OF COMMERCE

in

COMPUTER AUDITING

in the

FACULTY OF ECONOMIC AND MANAGEMENT SCIENCES

at the

RAND AFRIKAANS UNIVERSITY

STUDY LEADER: PROF A. DU TOIT

JOHANNESBURG
SEPTEMBER 1991

## DECLARATION

I declare that this research essay is my own unaided work except to the extent acknowledged in the text and has not been submitted previously for any degree or examination at this or any other University.

MICHAEL LOUIS BOSMAN

CHAPTER INDEX PAGE

# OPSOMMING

'N EVALUASIE VAN

INTEGRITEITSKONTROLE IN 'N AS/400-OMGEWING

DEUR

MICHAEL LOUIS BOSMAN

OPSOMMING VAN SKRIPSIE INGEDIEN VIR DIE GRAAD

MAGISTER COMMERCII IN REKENAAROUDITERING

IN DIE FAKULTEIT EKONOMIESE EN BESTUURSWETENSKAPPE

AAN DIE RANDSE AFRIKAANSE UNIVERSITEIT

STUDIELEIER: PROF A. DU TOIT

JOHANNESBURG

SEPTEMBER 1991

## OPSOMMING

Die doel van die opsomming is om die agtergrond, metodiek en gevolgtrekkings van die navorsing oor toegangsbeheer risiko's in 'n AS/400 omgewing kortliks uiteen te sit.

Die volgende hoofde word vir hierdie doel gebruik:

1. PROBLEEMOMSKRYWING EN DOEL VAN HIERDIE NAVORSING

2. NAVORSINGSONTWERP EN METODIEK

3. GEVOLGTREKKINGS

### 1. PROBLEEMOMSKRYWING EN DOEL VAN HIERDIE NAVORSING

Die ouditeur, enersyds voor die taak gestel om 'n doeltreffende sowel as 'n doelmatige ouditbenadering te ontwerp, asook bestuur, wie se taak dit andersyds is om rekenaarsekuriteit ten uitvoer te bring en te monitor, moet integriteitskontroles evalueer.

Hierdie noodsaaklikheid om integriteitskontroles te evalueer, is aan die toeneem te wyte aan die toenemende kompleksiteit van rekenaaromgewingsfaktore sowel as die ineenstorting van die sogenaamde papierouditproses en die vervanging van toepassingskontroles met integriteitskontroles.

## 2. NAVORSINGSONTWERP EN METODIEK

Deur van die Roetekonteksmodel gebruik te maak, is 'n evaluasie van die integriteitskontroles en die risiko's aan 'n AS/400 -omgewing verbonde, gedoen. Die bedryfstelsel (OS/400) is in funksionele katogorieë afgebeeld ten einde met die evaluering behulpsaam te wees op 'n wyse wat ooreenstem met dié wat in die Roetekonteksmodel uitgestippel is.

## 3. GEVOLGTREKKINGS

Daar is tot die slotsom gekom dat die model deur beide ouditeurs en bestuur aangewend kan word om integriteitskontroles te evalueer. Daar is ook bevind dat nie alle risiko's deur integriteitskontroles die hoof gebied kan word nie, wat as 'n verdere aanduiding van die bruikbaarheid van die model dien.

Die doelmatigheid van die toegangsroete- en Roetekonteks-modelle in die evaluering van die integriteitskontroles in die AS/400-omgewing is derhalwe vasgestel.

## SYNOPSIS

Both the auditor, faced with the task of determining an effective and efficient audit approach, as well as management, charged with implementing and monitoring computer security, need to evaluate integrity controls.

This need to evaluate integrity controls is increasing, due to the growing complexity of computer environments, the breakdown of the paper audit trail, and the replacement of application controls by integrity controls.

By applying the Access Path and Path Context Models, an evaluation was performed of integrity controls and risks in an AS/400 environment. The operating system (OS/400) was delineated into functional categories to assist in the evaluation, in a manner consistent with that outlined in the Access Path Model.

It was found that sufficient integrity control facilities exist in an AS/400 environment to meet the control objectives, although several risks were identified which could only be addressed by application controls.

It was concluded that the model could be used by both auditors and management to evaluate integrity controls. It was also concluded that not all risks could be addressed by integrity controls, which is a further indication of the usefulness of the model.

The applicability of the Access Path and Path Context Models in the evaluation of integrity controls in the AS/400 environment has therefore been established. 

# CHAPTER 1. INTRODUCTION

CONTENTS PAGE

## 1. BACKGROUND AND PROBLEM DESCRIPTION

Trends in information technology such as the increasing complexity of operating systems, the proliferation of large networks and distributed processing, and the increasing lack of a paper audit trail have made the management and control of computer installations increasingly complex.

The increasing use of distributed data processing necessitates the implementation of the full range of communication controls, according to Kirk (1988:150). He adds that the distributed data processing environment is potentially the most complex the auditor will face, including all the problems of communications, data base, multiple machines and multiple operating systems.

Auditors have a duty in terms of statement AU 230 paragraph .08 issued by the South African Institute of Chartered Accountants (SAICA)(1986) to assess systems of internal control, with the objective of establishing whether such controls may be relied upon.

This duty is supported by the SAICA Guideline on auditing in a computer environment (1989: para .07). These controls are relevant as they are designed to ensure that the financial information produced is complete, accurate and valid.

Traditionally an audit approach distinguished between user controls and system controls. Due to the technology employed in modern computer systems this approach is no longer valid.

As Boshoff (1986:224) puts it "Trying to relate a general review of system software, physical and other controls to the audit objectives for specific applications in an on-line system is not efficient, nor is it always effective in modern systems as little audit comfort is obtained therefrom."

"The concept of interfacing application (user) controls and integrity (data processing) controls is necessary to control and audit modern computer systems ..." according to Boshoff (1986:225).

Studies by Boshoff (1985,1990) led to the development of the Access Path and the Path Context Model (PCM) as valid tools for the evaluation of complex computer systems and for addressing the evaluation of computer security.

The credibility and acceptance of Boshoff's models is supported by the publication of his findings in several prestigious international journals. A recent study found that the Access Model and PCM were applicable in evaluating controls in the MVS/XA environment (Damianides, 1991).

Management, who have the responsibility of ensuring computer security is adequate, can use the control model to determine whether computer security standards and procedures have been complied with, as well as whether the extent of application controls are appropriate, based on which integrity facilities are utilised.

The objectives of this essay are to identify internal control risks and software control facilities in an AS/400 environment using the Access Path and PCM, and to develop a model for analysing integrity controls which may be used by the auditor in determining an effective and efficient audit approach. Publications such as the guidelines for auditing in a computer environment (1989: para .07) and computer audit skill levels (1986:1) issued by the SAICA support the use of such a model.

## 2. SCOPE AND LIMITATIONS

### 2.1 The AS/400 environment

The AS/400 is a strategic development by IBM, as it is the first product to be Systems Application Architecture compliant, offers a migration path, programmer productivity aids, and supports many software products. Interest in the AS/400 is keen: by the end of 1989, 98 of IBM's top 100 accounts in the U.S. had an AS/400 evaluation project under way according to Stamps (1989:52).

Significant features of the AS/400 are that it has a Relational Data Base Management System (RDBMS), supports object orientation, and a single-level storage addressing architecture. The low operating costs of the AS/400 together with the ability to network AS/400's has led to large sites 'down' or 'right' sizing from other architectures, such as MVS and VM.

As far as connectivity is concerned, OS/400 supports a wide variety of protocols, including OSI, SNA LU 6.2 and PU2.1, token ring, and PC communication. One of the objectives IBM had in developing the AS/400 was to establish a product which provided market leadership in communications capabilities according to Clark et al (1989: 407).

## 2.2 Control objectives

The model includes certain control objectives, which need to be achieved to ensure that the AS/400 environment is appropriately controlled.

These control objectives have been derived from Boshoff's (1985) study on controls, research carried out by the author over the two years of formal study towards a masters degree, and various institutes governing auditing standards such as the South Africa Institute of Chartered Accountants, the American Institute of Certified Public Accountants, and the Canadian Institute of Chartered Accountants.

The control objectives according to Bosman et al (1988 : 2) are:

(i) Completeness of input, processing, updating of files and output.

(ii) Accuracy of input, processing, update of files and output.

(iii) Maintenance (integrity) of data while transient (being transmitted) and static (once data files have been updated).

(iv) Validity/authorisation of business processing. This includes division of duties.

(v) Appropriate programmed procedures or functionality. This describes the automated business procedures and whether they are in accordance with business practice and management's delegated expectations of what the system is supposed to do.

These control objectives and the Access Model are assumed to be valid, based on published research by Boshoff (1985,1990).

## 2.3 Integrity and Application Controls

Due to the fact that integrity (general) and application (user) controls are well documented by institutes governing auditing standards it would serve no useful purpose to further explore these concepts.

Due to the complexity of the AS/400 environment and the environments it may communicate with, the focus of this research essay will be on integrity controls. The need for application controls will be identified. The nature of these application controls will not be dealt with, as application controls will depend on each installation's circumstances.

Figure 1 below illustrates the relationship between integrity and application controls.

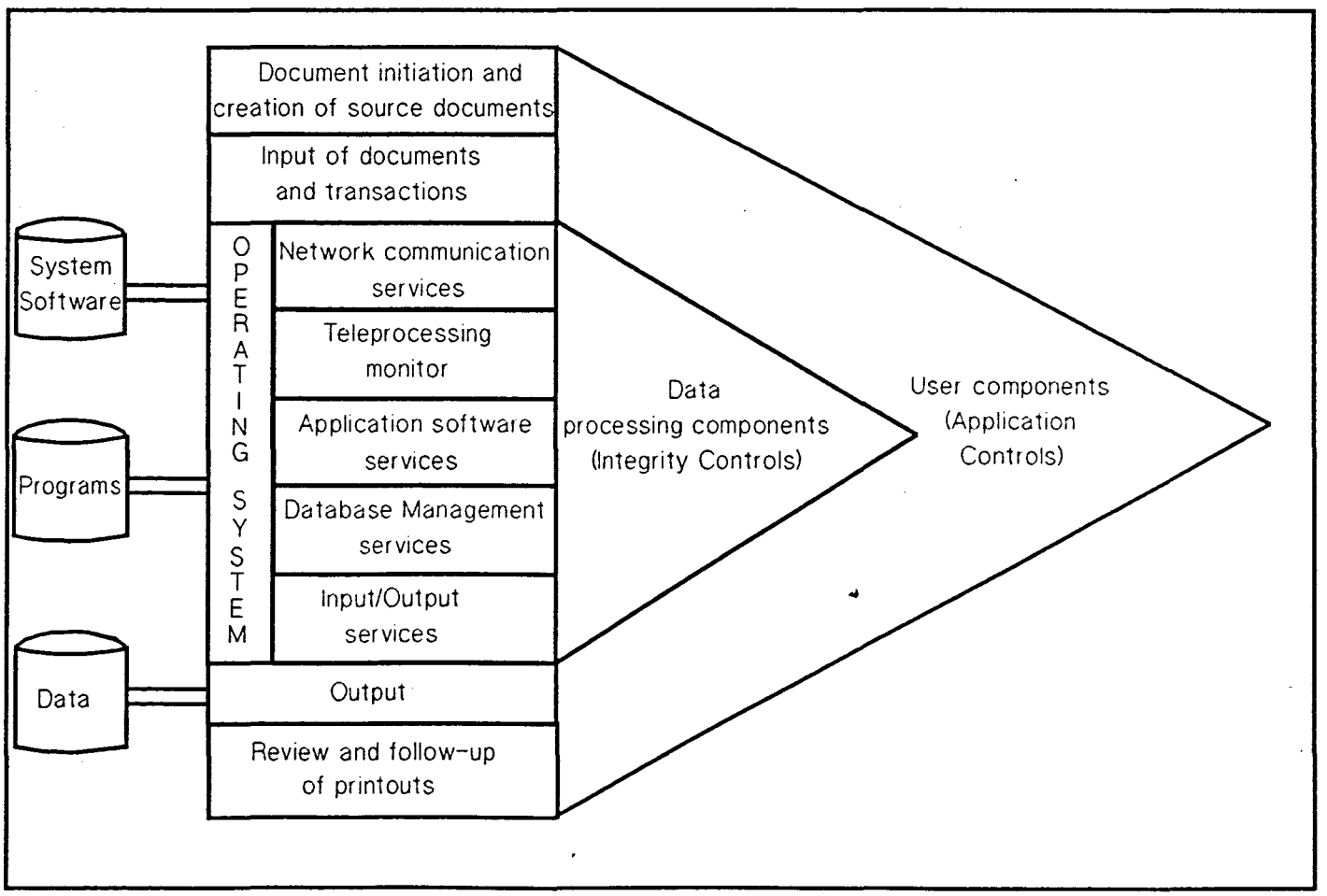


FIGURE 1. TYPICAL DATA FLOW IN A LARGE COMPUTER ENVIRONMENT
[SOURCE: BOSHOFF (1986:224)]

## 2.4 The Access Model

The Access model has, as its principal theme, the need to control technology by means of using technology. Using control objectives (referred to in Section 2.2 above), the model advocates the analysis of the use of software facilities. Each software component in a mainframe domain, for example VTAM, RACF, CICS, ADABAS, MVS, is seen as a net.

Using the model, management may determine which facilities in which component are to be used to achieve the control objectives, thereby using technology to control technology.

## 2.5 The Path Context Model

The PCM (Boshoff: 1990) is based on the premise that the need for computer security is paramount. In a multiple domain environment, the problem of identifying a user and ensuring appropriate access is enforced requires the use of complex mechanisms.

Any further discussion of the PCM is beyond the scope of this research essay.

## 2.6 Limitations

As the AS/400 environment covers a wide area, certain constraints and exclusions are essential to restrict the scope of this research study:

(1) Access control or security dealt with excludes physical security controls, as these are outside operating system and application software and are manually controlled.

(2) Certain controls which impact indirectly on integrity controls have been excluded.

These cover areas such as:

(i) documentation of system procedures and the operating environment

(ii) the organisation's IT strategies, policies and procedures

(iii) aspects of change control, other than authorisation and segregation of duties, over functions such as development, implementation and maintenance of software

(iv) AS/400 management, including such areas as installation, performance optimisation, problem diagnosis, and administering changes to the site

The reason for these exclusions is that each of these areas is large enough to warrant a separate research study.

(3) An appreciation and understanding of generally accepted auditing terminology and concepts has been assumed.

To the extent deemed necessary to present the model for use by auditors and management, certain terminology has been defined.

(4) A detailed discussion on OS/400 control facilities has been omitted, due to length constraints on this essay, and to provide focus. Technical manuals referred to in the bibliography can provide such detail if required.

Due to the size of OS/400 only the more significant components are discussed.

(5) This study is concerned with Version 1, Release 2.0 of OS/400.

## 3. METHODOLOGY

The approach followed in the essay was one of developing a model analysing control objectives and related control facilities to evaluate whether the PCM is applicable in an AS/400 environment.

The model was developed by the author drawing on research undertaken over the two years of formal study towards the M.Com. in Computer Auditing, together with the author's practical experience in several AS/400 sites. All control facilities were extracted from IBM AS/400 technical manuals. Acknowledged AS/400 experts were consulted where the technical manuals were deficient or incomplete.

The approach followed in developing the model was to link all risks to a specific control objective, and then to identify all integrity control facilities which could prevent or detect that risk from occurring.

## 4. LITERATURE SURVEY

An extensive literature survey was not performed as it would not have served a useful purpose. The justification for this is as follows :

(a) Definitions relating to the distinction between integrity and application controls are well known, and have been thoroughly dealt with in many texts including The American Institute of Certified Public Accountants (AICPA) (1977: 25,48; 1984:6), Boshoff (1985:37), Davis et al (1983:16), Halper et al (1985:16.8 - 16.11) Mair et al (1978:41), Perry (1986:143) and Roberts (1985:23).

(b) The validity of the control objectives used is supported by Boshoff's research essays (1985, 1990), Halper et al (1985:26-4, 32-3, CH16), a report commissioned by The Institute of Internal Auditors (1977:45), AICPA (1984:6; 1988:10) and a research essay on the application of the Access Path and Path Context Models in an MVS/XA environment by Damianides (1991:5).

The publication of Boshoff's works in prestigious international journals adds weight to the acceptance of the Access Path and Path Context Models.

(c) There is no known study covering the applicability of a Simple Path Context Model in an AS/400 environment. There is a risk that this may have been the subject of confidential or unpublished material. At the date of submission no such research was known which would have required acknowledgement in this research essay.

(d) The reference material used therefore consisted largely of IBM AS/400 technical manuals. Due to the fact that such manuals are very specific and contain numerous cross references between themselves, detailed page references to these manuals have not been included in this research essay.

All such manuals used by the author are included in the bibliography and have self-explanatory titles.

## 5. SUMMARY

The need for the model arises from an organisation's computer security standards and procedures, which are formulated by management. By applying the Access Path and Path Context Models, the model developed in this research essay may be used by management to evaluate:

(a) Whether the computer security requirements embodied in the computer security standards and procedures have been addressed.

(b) Whether risks which are not addressed by security procedures may be addressed by integrity and/or application controls.

(c) Risks which the organisation is exposed to, by not using integrity control facilities.

(d) Whether there are deficiencies in the organisation's computer security standards and procedures, i.e. where the model developed highlights a risk which is not addressed in the organisation's computer security standards and procedures.

An evaluation of control facilities was successfully carried out in the AS/400 environment. Certain risks were identified which could not be controlled by any OS/400 integrity facilities. The conclusion was reached that OS/400, in conjunction with certain application controls, can provide an adequately controlled secure environment. Where certain integrity facilities are not used, the AS/400 environment may not be considered secure.

A significant weakness in OS/400 Version 1 was identified, however this has been addressed in OS/400 Version 2. Only OS/400 Version 2, or later versions (Version 3 will shortly be released) may be considered secure.

The model has opened the door for research into other areas, for example the interfacing of the AS/400 environment with other environments such as an MVS/ESA domain, Local Area Networks, or architectures complying with OSI (Open System Interconnection) standards, as well as the areas described in section 2.4 above.

# CHAPTER 2. ESTABLISHING THE MODEL FRAMEWORK

# IN THE AS/400 ENVIRONMENT

CONTENTS PAGE

## 1. INTRODUCTION

This chapter outlines the context and relevance of the model to an organisation. The need for top management commitment to security is paramount. A survey conducted by the National Centre for Computer Crime Data in the U.S.A, on "Commitment to Security", ranked top management commitment to security the most important and valuable component of a general security strategy, according to Bloombecker (1989:72).

Following from the need for computer security, an organisational framework, showing the relationship between the organisation's computer security standards and procedures and the AS/400 environment, is described. The AS/400 environment is then broken down into its component parts, to illustrate the focus and scope of the model which was developed in Chapter 4.

Finally, a conclusion concerning the relevance of the model was drawn.

## 2. THE FRAMEWORK FOR COMPUTER SECURITY STANDARDS AND PROCEDURES

Conte (1990:36) states "security is the business function of protecting an enterprise's resources and operations; computer systems security should be designed within the context of the enterprise's overall security plan."

In describing trends in security in Europe, Attwell (1988:15) states "more and more organisations... aided by a number of highly publicized international EFT frauds... have radically improved their access control and network security."

Management often suffer from the misperception that the usage of certain security facilities, or an access control package, solve all computer security problems.

An organisation's computer security standards and procedures are developed by management to assist in achieving their responsibility to ensure that the computer environment within which perhaps the organisation's most important asset, its data, is secure.

What these standards and procedures should encompass, is the achievement of the control objectives outlined in Chapter 1, Section 2.2. It is important that these procedures address the use of technology to achieve control objectives.

Within, and supported by, these standards and procedures lies the AS/400 environment. As such the AS/400 environment should not be viewed in isolation.

The relationship between computer security standards, which provide guidance in terms of policies and principles, computer security procedures, which provide guidance on how to give effect to computer security standards, and the AS/400 environment is illustrated in Figure 2.

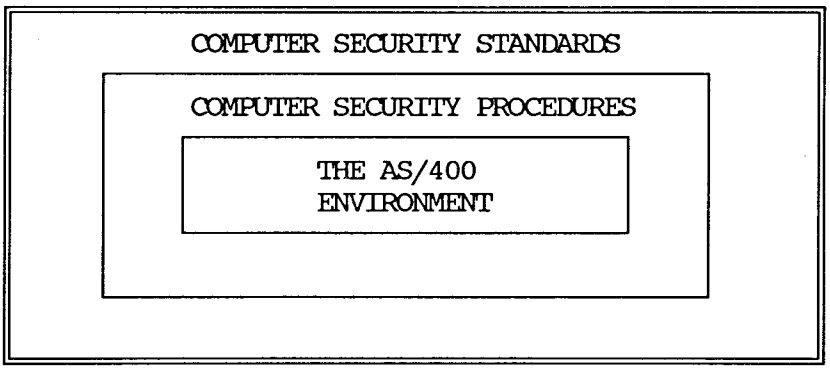


**FIGURE 2. COMPUTER SECURITY STANDARDS AND PROCEDURES**

## 3. THE AS/400 ENVIRONMENT FRAMEWORK

An appreciation of the components of the AS/400 environment is necessary to illustrate the framework on which the model is based.

### Background

The AS/400 supports IBM's Systems Applications Architecture which is graphically illustrated below (figure 3) :

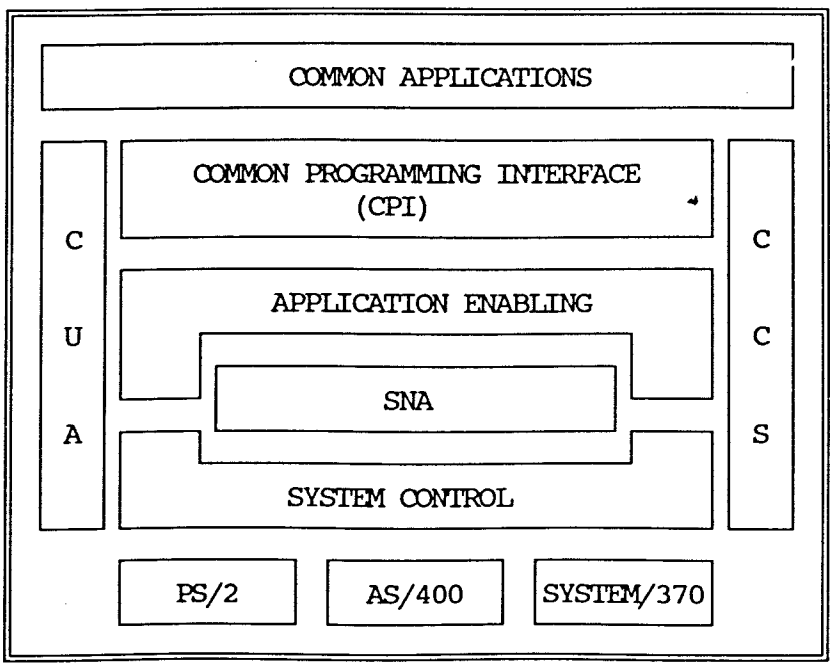


**FIGURE 3. IBM'S SAA (Systems Application Architecture)**
**[Source: IBM reprinted in Systems Integration (1990:37)]**

SAA consists of four related elements establishing interfaces, conventions and protocols, which are briefly outlined below by Schleicher and Taylor (1989 : 362):

(a) Common User Access (CUA) defines the design rules for user inter- face elements and interaction techniques.

(b) Common Programming Interface (CPI) specifies the languages and services used to develop applications that are portable across SAA environments.

(c) Common Communication Support (CCS) designates the communication architectures which, when implemented, allow interconnection of SAA applications, systems, networks, and devices.

(d) The Applications element consists of Common Applications developed to execute across all SAA environments.

The relevance of this background is to explain references made to SAA, and more importantly, highlight the effects the above have on control issues which are taken into account in providing focus to this research essay. The major effects are:

(a) The wide communications capabilities present additional potential security exposures for an organisation. OS/400 communication integrity facilities are addressed; however communication exposures relating to architectures other than the AS/400 are outside the scope of this research essay.

(b) The other elements do not have an impact on control issues, other than to provide standards which may be supported by those of the organisation.

## 3.1 Structure of the AS/400

The nature and structure of the AS/400 components are illustrated in figure 4.

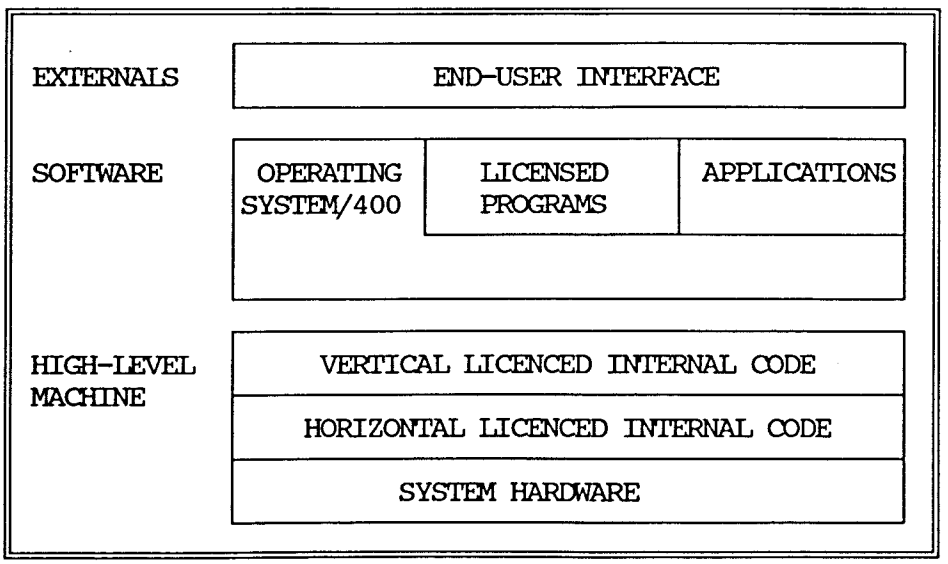


**FIGURE 4. AS/400 LAYERED ARCHITECTURE**
**[Adapted from: Schleicher et al (1989:365)]**

## 3.2 End-User Interface

The end-user interface provides menus, prompts, help facilities, etc. supported by the User Interface Manager (UIM) which enforces SAA interface standards. These standards are mandatory on the AS/400.

## 3.3 Licensed Programs

Licensed programs consist of all IBM supplied software, other than the operating system. These include IBM -supplied programs such as Office/400, Query/400, Compilers, and SQL. Third party vendor-supplied programs such as Robot (job scheduler) and CASE products such as LANSA and GENESIS, would reside in this area as well.

IBM-supplied utilities include:

DFU (Data File Utility)
SEU (Source Edit Utility)
IDDU (Interactive Data Definition Utility)
SDA (Screen Design Aid)
PDM (Program Development Manager)
RLU (Report Layout Utility)
APF (Advanced Printer Function)
BGU (Business Graphics Utility)

## 3.4 Applications

These comprise software developed or purchased to meet a business need, and could be coded in COBOL, RPG/400, Fortran, PL1, C, or Pascal.

## 3.5 Operating System /400

The operating system provides the means whereby all the components in Figure 2 communicate and interact. OS/400 includes all application and communication security facilities, the RDBMS file handler, I/O management and communications support.

## 3.6 Machine Interface (MI) and Licenced Internal Code (Microcode)

The MI consists of Vertical licensed code, Horizontal licensed code, and the solid state hardware. Microcode consists of the first two components.

As there is only one version of Microcode in main storage, which is not modifiable, assurance as to Microcode integrity is provided. This is supported by the many installed sites where the functioning and integrity of the Microcode is in evidence.

The Microcode, together with the MI, supports the following constructs according to Clark et al (1989:420):

User profile.

Process Access Group.

Program variable storage [program automatic storage areas (PASA) and program static storage areas (PSSA)].

MI exception - handling support.

Event - handling support.

Object - locking support.

A discussion of these components is beyond the scope of this research essay. The relevance of such features is that they provide, together with MI and OS/400 interaction, a transaction processing model based on each user's job.

## 3.8 System Hardware

This consists of processors, storage devices, I/O devices, media and networking devices. Control procedures relating to system hardware should be addressed by the organisation's computer security standards and procedures, and are outside the scope of this research essay.

## 3.9 Focus of this research essay - the AS/400 environment

Following the above discussion of the AS/400 environment, and the access paths graphically illustrated by the author in Figure 5 (overleaf), the focus of this research essay is on communications security, application security, licensed programs and OS/400 operations. Facilities discussed are those which are relevant to the achievement of the control objectives outlined in section 2.2 of Chapter 1.

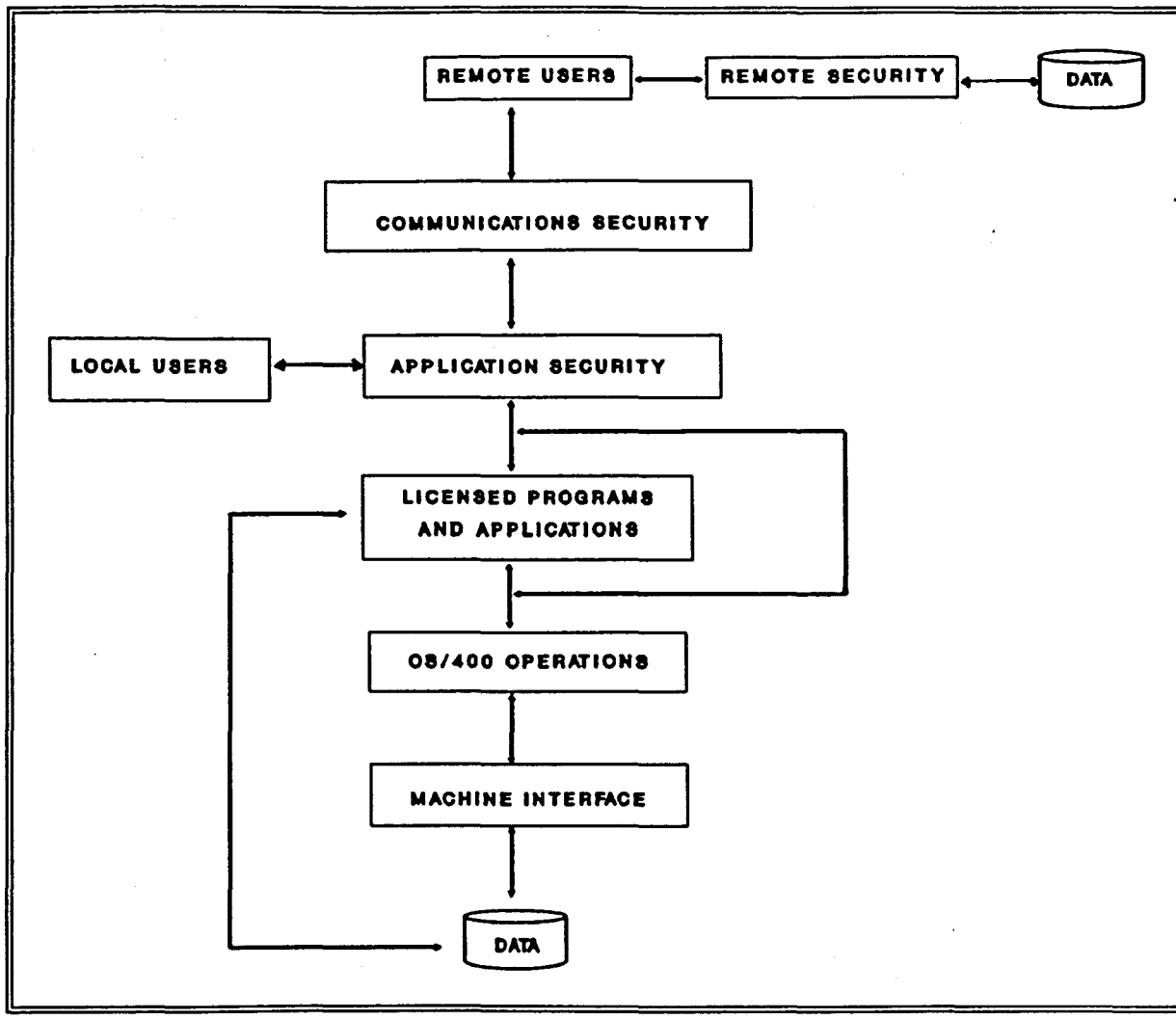


**FIGURE 5. AS/400 ACCESS PATHS**

The justification for the focus of this research essay is as follows :

a) The usage of Licensed programs and Applications may be controlled by integrity facilities in OS/400. Whilst there may be exposures through the use of utilities other than those supplied by IBM, a discussion of these issues is beyond the scope of this research essay.

The reasons for this are that third party programs and applications have very wide-ranging uses and exposures, and the organisation's computer security standards and procedures should address these possible issues.

b) The Microcode is generally not accessible by users or programmers, and, as such, does not have many control ramifications.

It is possible for high level MI calls to be made by a program. This exposure is dealt with (refer Section 3.2.12). Other than this there are no MI and Microcode control issues.

## 4. CONCLUSION

Due to the long-term commitment by IBM to the AS/400 and SAA, there will be increasing interest in the AS/400 as a strategic hardware platform. The connectivity with OSI architectures indicates that the control model developed can be viewed as a 'building block', which, together with models of other architectures, can be used by auditors and management for the evaluation of integrity controls and risks across a multi-architectural platform.

# CHAPTER 3. APPLICATION OF THE MODEL IN THE AS/400 ENVIRONMENT

CONTENTS PAGE

# 1. INTRODUCTION

To assist in the identification of potential risks and controls in OS/400, the functions performed by OS/400 have been divided into the areas of communications, processing, operations, maintenance and office services and support products.

The installation's options in each of these areas will be examined, together with the risks the installation would face depending on which option was chosen. The control and security implications will be reviewed.

This approach is consistent with the Access Path Model, which views each mainframe software component as a "net", through which the user must pass to gain access to data and other system resources.

A knowledge of how OS/400 works is assumed, and the discussion of key parameters and options will concentrate on their effect on controls and risks.

This chapter does not detail all possible control concerns and the possible combinations of control facilities. Possible combinations in the usage of control facilities are discussed in the IBM manuals, such as IBM:AS/400 Security and Auditing considerations.

## 2. COMMUNICATIONS

### 2.1 Introduction

Communications facilities are the means by which sessions between devices are established and controlled. Communication facilities are generally part of OS/400 and are not a separate software product.

The focus of this section is on communications facilities which may be utilised to achieve the control objectives outlined in Chapter 1.

IBM has announced the Advanced Peer-to-Peer Networking (APPN) architecture as an extension to SNA and SAA. Documentation of the open architecture for the APPN End Node has been made available to software developers by IBM. (The End Node supports OSI standards).

Companies which have advised IBM they intend producing products which implement the APPN End Node architecture are Apple Computer Inc., Novell Inc., Systems Strategies Inc., and Siemens/Nixdorf Informationssysteme AG.

APPN products are the AS/400, IBM SAA Networking Services/2 Version 1,0, 3174 APPN, Teleprocessing Network Simulator (TPN's) and DPPX/370.

According to IBM (Communications: Advanced Program-to-Program Communications and Advanced Peer-to-Peer Networking User's Guide: 2-1) an APPN network "is a communications network where any system can control the establishment and ending of sessions and application program transactions without a controlling host system".

APPN utilises the SNA PU2.1 protocol. Advanced Program-to-Program Communications (APPC) utilises the SNA LU6.2 protocol, and controls the interface between application programs and APPN networking support.

OS/400 uses Distributed Systems Node Executive (DSNX) support, which may be configured to run as an application program, and which uses Systems Network Architecture Upline Facility (SNUF), for communications with a Netview DM host system.

OS/400 DSNX acting as an intermediate node requires an object distribution/Systems Network Architecture Distribution Service (SNADS) connection to other AS/400 systems and System/36s (IBM:Communications:Communications and Systems Management User's Guide:1-1).

Alert Support (refer Section 2.6), and SNADS logging and error detection (refer Section 2.3), are DSNX components.

## 2.2 Network Security

The source system APPC will connect a remote system to the network as non-secure if Security level 10 is used. APPC can provide session and transaction level security when security levels 20 or 30 are used.

### 2.2.1 Session level security

This is available when the use of a password (which is specified on the LOCPWD parameter) is used to validate session establishment with a remote system. The EXCHID parameter may also be used to validate such a remote system.

### 2.2.2 Transaction level security

Application Program Security may be used to provide security at transaction level, whether session level security is used or not. Security parameters of user profile, password or user ID are available, which the remote system can use to verify that the user ID is defined on the remote system.

A DDS (data description specification) Security Keyword may be set to *USER (the user's profile on the local AS/400 system must be used), or * NONE (the default user profile must be used) to provide security at file and record level.

### 2.2.3 Distributed Data Management

#### Introduction

Distributed Data Management (DDM) controls processing of data resident on a remote system. The remote system must also support DDM. DDM uses APPC or APPN to enable communication between two remote systems. DDM can be used to communicate between systems that are architecturally different (Communications:Distributed Data Management User Guide:1-3).

#### Control Facilities

Remote access is controlled by the Change Network Attribute (CHGNETA) command. The DDMACC parameter may prevent all remote access, or control access to files using standard authority to files. A user exit may be used to restrict the types of operations allowed on files for particular users.

To provide security, additional user profiles may be set up on the target system. A default user profile may be used for multiple source system users. The communications entry used in the subsystem in which the target jobs are run determines the default user profile which will be used.

### 2.2.4 System related security

DDM Source and Target System Security

When a DDM file is created, the AUT parameter is used to control the rights all users on the source system have for that DDM file. The Grant Objects Authority (GRTOBJAUT) or Revoke Object Authority (RVKOBJAUT) command can be used to control users' rights to a DDM file.

The source system does not send a password when communicating with a TDDM on the target system. The target system may request a userid, and if so, the userid will be sent by the source system. The SECURELOC parameter on the target system controls access rights by the source system.

If SECURELOC (*YES) is specified, the source system userid is sent to the target system, which verifies the userid and uses user profiles on the target system to determine the source system user's access rights. If SECURELOC (*NO) is used, a default userid must be set up on the target system to control access rights.

A user exit program may be used on the target system to restrict source system user access to objects via commands submitted on the Submit Remote Command (SBMRMTCMD).

Various location lists (both local and remote) for different communication protocols are used before a session between controllers is established.

DDM target system security consists of user-related security elements using the SECURELOC parameter as discussed above, and object-related security via the DDMACC parameter and an optional user exit program to supplement normal object authority controls.

The DDMACC parameter may be set to *SAME, (which specifies that the current value of the DDMACC parameter remains unchanged), *REJECT (will not allow any DDM requests from remote systems), or *OBJAUT which allows remote access subject to target system object authorities (which requires the use of Security level 30 in the target system).

## 2.3 SNADS logging and error detection

On an AS/400 system, SNADS (System Network Architecture Distribution System) is a set of closed-protocol boundary-only IBM-supplied programs that have direct access to SNADS distribution functions.

SNADS functions that support logging are:

(a) SNADS receiver jobs (via APPC/APPN from another system)

(b) SNADS router jobs (to local users)

(c) SNADS sender jobs (via APPC/APPN to another system).

All functions in SNADS are entered in the log after they are performed.

## 2.4 System Distribution Directory

The System distribution directory contains the userID, address and description for local users authorised to send and receive distributions on the SNADS network. The same information is on the directory for remote users if default values are not used.

The system distribution directory is an IBM-supplied object, which has three parameters with control implications:

(a) QSECOFR - this entry should be changed and kept in the directory to enable the security officer to receive distributions. It may be used to prevent the security officer from receiving distributions.

(b) QDFTOWN - this is a default owner entry, and denotes the user who owns the directory. It may be used to prevent the default owner from receiving distributions for security reasons.

(c) QSYS - this is an internal system entry which owns IBM-supplied folders and documents (shipped with the system). It may be used to prevent this user from receiving distributions for security reasons.

The AS/400 security officer or a user with security administrator (*SECADM) authority can add or remove users from receiving objects via Document Interchange Architecture (DIA) (used for document exchange) or object distribution (used for exchanging objects other than documents).

### 2.4.1 Object distribution

Users may utilise object distribution and the system distribution directory (for local users), or a SNADS network and the system distribution directory (for remote users), to send objects and messages to another user.

Object distribution will allow users to:

(a) Backup and restore objects to and from a remote system respectively.

(b) Send data files, messages and spooled files to remote sites.

(c) Submit job streams to run on a remote site.

To ensure that object distribution, which is available to all users, is used appropriately, all sensitive resources must be defined, i.e. security level 30 should be used.

Object distribution may be used as a control mechanism to backup a system to a remote site, keep remote sites unmanned, send either source or object code or maintain compilers at remote sites.

To control the submission of jobs on a system via a remote system the Change Network Attributes (CHGNETA) command may be used.

The JOBACN parameter may be used to either file (*FILE) or reject (*REJECT) all incoming jobs. The value *SEARCH allows the network job table to control incoming jobs by using values in the table.

The actions supported by the network job table include the *SUMBIT parameter, which submits the job stream to a job queue, as well as the *FILE and *REJECT parameters. The *FILE command files the incoming job stream on the queue of network files for the receiving user, who may cancel or submit the job.

## 2.5 Remote Spooling Communications Subsystem/Professional Office System (RSCS/PROFS) Bridge

RSCS/PROFS is an application (which is not part of OS/400) and which provides:

(a) Distribution services between an AS/400 SNADS network and a System/370 VM/RSCS network.

(b) Distribution services between an AS/400 system and an MVS/JES2 or MVS/JES3 network (MVS/XA or MVS/ESA).

(c) Sending or receiving of files and messages between System/370 users and object distribution users.

(d) Distribution of documents created by a document interchange session.

(e) Distribution of files, notes and messages between users on AS/400 Office, DISOSS, or any DIA/SNADS node connected to the bridge and RSCS/PROFS.

Where any of the above facilities are used the principal control concern is that all access is valid and authorised. Keeping authorities in step across the various architectures and applications is an important task, vital to the maintenance of computer security.

## 2.6 Alert Support

The AS/400 uses alert support for network problem management using SNA alerts. Alerts may be used for :

- Monitoring systems and devices that operate unattended

- Managing situations where the local operator cannot handle the problem
- Maintaining control of system resources and expenses

(IBM:Communications:Communications and Systems Management User's Guide:7-1)

## 2.7 Securing a communications line

### 2.7.1 Data transmission

There is a risk that data transmitted on a communications line will be viewed. The System Service Tools (SST) has a protocol analyser which may be utilised to view data received and data transmitted.

Stansbury (1990:82) points out that to ensure that the SST protocol analyser is not used to view data received or transmitted the ability of users to run SST should be revoked.

Data encyption (using Cryptographic support) may be used to ensure the privacy of data whilst being transmitted. Various software products are available to encrypt data transmitted and received by OS/400.

### 2.7.2 Dial-in access

The ability to allow dial-in access may be controlled by using the AUTOANS parameter. The AUTOANS parameter may be set to *NO, which ensures that the ANSLIN command is entered before a session is established by APPC.

# 3. PROCESSING

## 3.1 Introduction

This section considers facilities which may be used to control the accessing and/or processing of data.

Due to the amount and complexity of these facilities, it is not possible to include a detailed discussion of facilities (and the possible combinations of facilities).

## 3.2 Application Security

Application security consists of integrity facilities in OS/400 which may be used to control access to data on an AS/400 system.

### 3.2.1 Security Levels

Three levels of system security are available, the features of which are summarised below. The default is minimal security i.e. level 10 is active. The significant facilities available in each level are summarised in Figure 6 below, and then briefly discussed.

| | Level 10 | Level 20 | Level 30 |
|---|---|---|---|
| 1. Userid required | Yes | Yes | Yes |
| 2. Password security active | No | Yes | Yes |
| 3. User profile aut. created | Yes | No | No |
| 4. Resource security active | No | No | Yes |
| 5. Menu and initial pgm security active | No | Yes | Yes |
| 6. Access to all objects | Yes | Yes | No |
| 7. Enrolled in System Distribution Directory | No | Yes | Yes |

**FIGURE 6. OS/400 SECURITY LEVELS (Ver 1, Rel 2.0) (Source: Adapted from IBM, "Programming:Security concepts and planning": 1 - 4)**

Level 10 offers no security, level 20 password, menu and initial program security, and level 30 full resource object-level security with many other facilities discussed below. (An object may be a file, program, library,user profile, in fact, almost anything stored on the AS/400).

The existence of these levels is not, in itself, a control.

### 3.2.2 Userids and Passwords

A userid is required to allow access to the AS/400, for any level of security. Password security is available in security levels 20 or 30.

### 3.2.3 User profiles

For security levels 20 and 30 a user profile must have been created before a user may gain access to the AS/400.

User profiles (profiles for use by a group may be created) can be used to control the functions available to a user as follows:

special authority
display station security
sign-on security
initial program security
initial menu security
limited capability

### 3.2.4 Menu security

IBM-menus and displays may be used to allow a user access only to a command option on a menu i.e. excluding other menu options. The user must be authorised to use the original menu program and any options that directly operate commands. System authority checking includes authorisation from group profiles or from the program adopt function.

### 3.2.5 Initial Program Security and Limited Capability

Initial Program Security may be used to specify which program must run when a user signs onto the system. A user may be assigned Limited Capability, which will restrict the functions the user may perform.

### 3.2.6 Resource Level Security and Library security

Resource Level Security allows security to be implemented at object level i.e. allows programs, devices, libraries, databases, users and files to be defined as objects. A user must have access to both the object and the library the object resides in before that object may be accessed.

### 3.2.7 Logical Views

Logical views of data fields may be defined to restrict access to sensitive data to authorised users. This facility may only be used if Data Management (which is the RDBMS contained in the microcode of OS/400) is used to store and manage data. Logical views should be used to provide security at field level, as using object authority secures access at file level.

### 3.2.8 Sign on Security

Sign on security provides the ability to define the maximum number of unsuccessful logon attempts. The workstation concerned is automatically de-activated once the defined number of unsuccessful logon attempts is reached.

Ensure the LMTCPB parameter is set to *YES. This prevents the user from changing his initial menu, initial program or current library values, or invoking commands usually restricted at a menu. Note that the LMTCPB parameter is only available at security levels 20 and 30.

### 3.2.9 Authorisation lists

An authorisation list may be used to control a list of users and the authority each user in the list has to all objects the list secures (Security level 30 only). These may be used to grant a user access to an object (other than the owner of that object, who automatically has access to it).

### 3.2.10 User Classes

Users are divided into the following classes:

| | |
|---|---|
| Security officer | (*SECOFR) |
| Security administrator | (*SECADM) |
| Programmer | (*PGMR) |
| System Operator | (*SYSOPR) |
| User | (*USER) |

User classes are hierarchical in authority and may be used to implement segregation of duties amongst IS staff functions.

### 3.2.11 System Authority

System authority is broken down into Special authority, to perform system control functions, and Specific authority, to perform operations on an object and the data contained in that object. This is depicted diagrammatically in Figure 7 below.

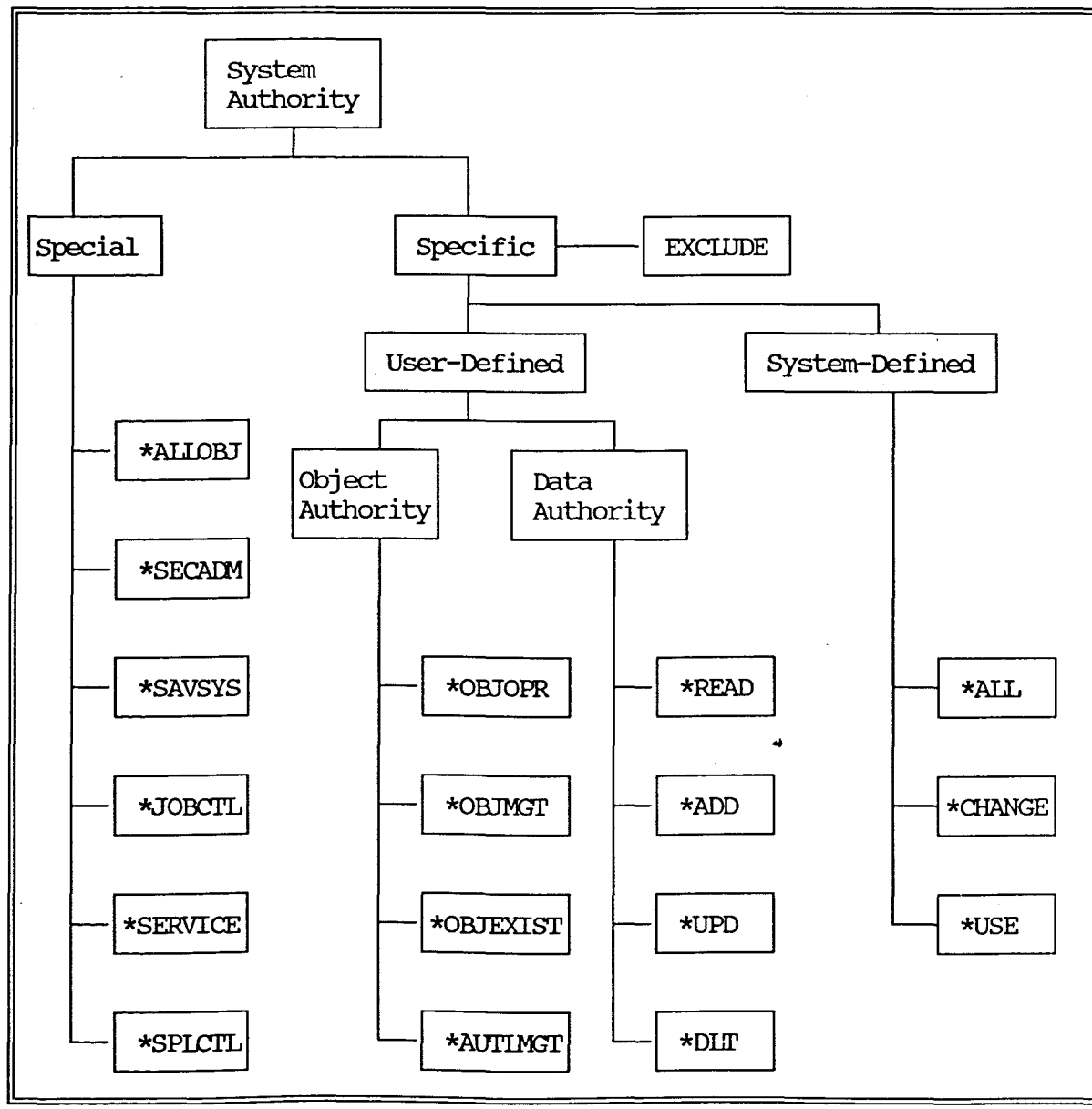


**FIGURE 7. OS/400 SYSTEM AUTHORITY**
**(Source: IBM, "Programming: Security concepts and planning": 1-9).**

### 3.2.12 OS/400 Security Exposures

There are certain exposures relating to MI, which is the foundation of AS/400 security. Conte (1990:74) describes these exposures, which revolve around the obtaining of improper authorities by an MI program.

Relatively few people have the technical skill to use the necessary MI-level techniques to exploit the gaps in AS/400 security. IBM have supplied Version 1 release 3.0 of OS/400 which contains security level 40, which closes the security gaps. This is achieved by forcing all applications to use API's (Application Program Interfaces) which control MI calls.

## 3.2 Data Management

Data Management (IBM: Data Management Guide: xxiii) "provides the functions that an application uses in creating and accessing data on the system and ensures the integrity of the data according to the definitions of the application".

Data Management supports the use of four types of files:

(a) Database files - which provide access to data stored on the database. Database files may only be created by use of the Interactive Data Definition Utility (IDDU), which creates data dictionary definitions, as well as a file description.

(b) Distributed Data Management (DDM) files - which provide access to data residing on another system.

(c) Device files - which provide access to externally attached devices such as printers, and tape and diskette drives.

(d) Save files - which are used for preparing data to be saved or moved to another system.

To control access to these files, object authority should be used. As far as DDM files are concerned, DDM security facilities should be used ( refer Section 2.2.3).

# 4. OPERATIONS

## 4.1 Introduction

Operations deals with the operating of the AS/400 machine/s. There are facilities used in the operating of the AS/400 which are relevant to the achievement of certain of the control objectives outlined in Section 2.2 of Chapter 2. These facilities are briefly outlined and discussed.

Aspects addressed include facilities which may have an impact on the continuity and reliability aspects of the AS/400, such as system initialisation, and backup and recovery facilities.

## 4.2 System Initialisation

The AS/400 has a system keylock. This is a physical key which can be used to control the AS/400 IPL (Initial Program Load) options. Although access to the key should be physically controlled, as use of the key affects the operations of the AS/400 and the achievement of the control objectives referred to, it is of relevance.

There are four keylock positions as follows :

- SECURE only allows the system to be powered down from a display station.

- AUTO allows the system to be IPL'd remotely as well.

- NORMAL in addition to the above functions allows the system to be turned on using the power switch.

- MANUAL allows manual IPL, power off and control of functions, as well as a different version of OS/400 to be IPL'd, and Dedicated Service Tools to be used.

## 4.3 Backup and Recovery

OS/400 has several facilities which together provide a backup and recovery capability. These facilities are, briefly:

### 4.3.1 Save and Restore Processing

This allows for the saving of objects (generally programs and data files) and the ability to restore them. Access paths may be saved and/or restored, at the operator's option. It is generally faster to restore access paths using the Journal.

To restore data in the event of a system failure, the Journal may be used.

### 4.3.2 Journal Management and History Log

Journal management allows for database files to be recovered, as well as providing an audit trail, activity report and job accounting information. Two objects are used for journal management, a journal and a journal receiver.

The journal identifies the journalled files, the current journal receiver, and all journal receivers that are on the system for the journal. The journal receiver records activity type for a specific record (e.g. added or deleted) as well as file and file member operations performed.

The journal data in conjunction with the history log provides a comprehensive audit trail. Data supplied by the history log includes userid, physical device used, and session logon and logoff times.

Access to commands which allow the journal to be copied should be restricted, possibly by storing such commands in a library, and restricting all access to this library to the security officer (QSECOFR).

### 4.3.3 Commitment control

This is an extension of the journalling function, which caters for uncompleted transaction update interrupted by a system or job abend, to ensure that incomplete transaction update is removed, or removing changes made by a transaction. These are called commit and rollback operations respectively. Commitment is invoked by a program instruction. Rollback is optional, and is invoked by the user.

Commitment control may only be used on files which make use of Journalling.

There is a risk that programmers may make inappropriate use of commitment control commands. This should be controlled by development standards.

### 4.3.4 Auxilliary Storage Pools (ASP)

This facility controls storage, where certain types of objects are stored on auxilliary storage devices, protecting the objects from losing data because of disk media failures occurring on other disk units not included in the ASP.

### 4.3.5 Checksum Protection

Checksum protects data stored in the system ASP from failure of a single disk. (The system ASP is always configured and created by the system and contains licensed internal code, licensed programs and systems libraries. User ASP's may be created and assigned a number 2 to 16.)

The Checksum facility takes data residing on several disks and combines that data onto one disk in such a way that, if any one disk should fail, its contents may be recovered by recombining the data on the remaining units.

The disadvantage of Checksum protection according to Clarke et al (1989:442) "is that the system cannot continue to run when a DASD fails, as the portions of temporary objects stored on that device are no longer available and cannot be recovered". Until the DASD is repaired system operation cannot be resumed.

To assist in minimising the risk of DASD failure, DASD mirroring may be used. This facility is only available in OS/400 Version 1 Release 3,0 and subsequent releases.

# 5. MAINTENANCE

## 5.1 Introduction

This section addresses concerns relating to the maintenance of objects residing on OS/400 by the use of utilities, as well as maintenance of OS/400.

## 5.2 Utilities

### 5.2.1 Data File Utility (DFU)

DFU is a program generator which creates programs to enter data, update files and make file enquiries. DFU creates a program based on your answers to displays. It provides a quick way of updating a file using a temporary program which does not have to be defined first. DFU also allows the creation of database maintenance programs faster than one could by using a programming language.

To ensure adequate data security, file controls must be introduced over DFU functions.

Object authority should be used to control access to objects using DFU. Similarly, data authority should be used to control the functions carried out by using DFU, such as update or delete.

As the audit report option in DFU may be set to "NO" (i.e. use of DFU will not be logged), it is important to journal use of DFU (refer Section 4.3.2).

### 5.2.2 Source Entry Utility (SEU)

SEU is a full-screen editor that allows you to enter and update source file members. Starting an edit session with SEU enables the user to:

a) insert new records
b) change existing records
c) delete records
d) move records from one location to another within a member
e) find a specified character string within the member.

As with DFU, object and data authority should be used to ensure that all use of the SEU is authorised, and all access to members is authorised.

### 5.2.3 Interactive Data Definition Utility (IDDU)

This utility works with Data Description Specifications (DDS), which are used to define physical files. It allows changes to be made to fields or files. Access to IDDU should be restricted via object authority.

Users of IDDU should backup physical files before using IDDU, as data may be corrupted when the physical file and logical views are maintained.

### 5.2.4 Dedicated Service Tools (DST) and System Service Tools (SST)

Access to DST should be restricted via a DST password. It is good security policy to let only the Security Officer and ISM staff know this password. This is important as DST are very powerful, and can perform tasks such as configuring ASP's.

Access to SST, which may be used for diagnosing error conditions, should be controlled, perhaps via system authority.

### 5.2.5 Programming Development Manager (PDM) and other utilities

PDM is basically an interface from which all utilities may be invoked. Access to PDM may be restricted. If this is not done, user authority for the utility called using PDM is checked.

The other utilities do not have any security ramifications, other than that access to them should be restricted, perhaps by using object authority.

## 5.3 Maintenance of OS/400

Maintenance of OS/400 may only be achieved via an IBM-supplied PTF. AS/400 PTF's which have been supplied per ISM Inform (1991:12) are:

a) AS/400 Ver 1 Rel 2; C0180120

b) AS/400 Ver 1 Rel 3; C1010130

c) AS/400 Ver 2 Rel 1; C1164210

Integrity of operations may be compromised if PTF's are not appropriately run. There should be standards governing the application of PTF's, as well as ensuring that only the most current version of OS/400 is IPL'd.

Maintenance of OS/400 is well controlled, OS/400 keeps a backup of the operating system software in machine area A, and any PTF's and manual operations run off a separate version of operating system software in machine area B.

This allows the usage of OS/400 to revert to a re-IPL version of OS/400 if a problem is encountered.

## 6. OFFICE SERVICES AND SUPPORT PRODUCTS

### 6.1 Introduction

AS/400 Office is a licensed program that supports the use of calendar, mail, word processing and office administration capabilities. AS/400 Office may be utilised together with other licensed programs like AS/400 PC Support and AS/400 Query.

OS/400 has an office services function which encompasses directory, document distribution, document library, security and word processing services. Application Program Interfaces (API's) can be used by application programmers to integrate AS/400 Office with business applications (IBM:Office Services Concepts and Programmers Guide :iii).

The focus of this section is on security services and backup and recovery procedures, with security aspects of PC Support and Query also being dealt with.

## 6.2 Office Security

Access to documents and folders may be controlled by using "specific user authorisation, group authorisation, object ownership, public authorisation, special authorities, working on behalf of others, authorisation lists, and access codes" (IBM:Office Services Concepts and Programmers Guide:5.2).

Access codes are the only method to secure documents stored remotely on S38 or S370 DISOSS, and are supported by OS/400 for co-existence with these systems.

The above authorisation functions are identical for other OS/400 objects, except for the following which relate only to document library objects :

(i) Document and folder authority levels. Four authority levels are supported, *ALL (all authority for operations on document library objects), *CHANGE (update authority), * USE (enquiry authority), and *EXCLUDE (no access at all).

(ii) Remotely filed documents. Office supports the authority levels in (i) for remotely filed documents.

Office ignores adopted authority when checking for authority to access a document library object.

## 6.3 PC Support

PC Support is a licensed program which allows a user to combine the ease of use of a PC, with the resources on the AS/400. PC Support may work in conjunction with DOS or OS/2. As Anderson (1990:60) puts it, the PC Support function "runs on the PC under the control of DOS".

The PC may be stand-alone, or access the AS/400 via a Token-ring LAN. (Token-ring is the only topology supported by the AS/400). Communications between the PC (whether stand-alone or via a LAN) are supported by APPC. Where the PC communicates with a remote AS/400 (or other architecture supporting APPN), such communication is supported by APPN.

PC Support has a router which allows communications across a multiple machine multiple architecture APPN network.

### 6.3.1 PC Support security

The ADRS parameter may be used to control communications between the PC and the host system using the following :

(i) System name - This is the system name to which the PC wishes to link.

(ii) Name of link - This is the name of any intermediary system.

(iii) User ID - This is the normal user ID used to sign on to a system. A default user ID will be used if not specified. The user will be prompted for the associated password where this default user ID is used.

AS/400 Application security will control the user's ability to sign on to the AS/400 using a PC running PC Support. (This is illustrated in Figure 5 in Chapter 2.).

Facilities outlined in Section 2. on Communication security may also be used to control PC access. The PCSACC parameter can be set to *OBJAUT to prevent access to a system by independent work station requests from other systems.

Due to the flexibility offered by PC Support, application security together with Office security should be used to control access to objects.

## 6.4 Query

Query is a report generator. Query may be used to add records to an existing file. Access to Query should be restricted, and it should not be run in interactive mode. Batch mode should be used, as if Query is running in interactive mode adding records, and the session is interrupted, the record being added at the time of the interrupt may be corrupted.

## 7. CONCLUSION

The more significant integrity control facilities in OS/400 were briefly listed. Many integrity facilities have been incorporated into the AS/400, the most significant, perhaps, being the ability to implement object-level security. The auditor should obtain an appreciation of how significant AS/400 integrity facilities operate and interact.

The timing, nature and extent of audit procedures must be determined by the auditor. The technical manuals in the references provide details including which commands the auditor may use to access data on these integrity facilities he wishes to audit.

Due to the extent and complexity of AS/400 integrity facilities, it is apparent that security should be planned prior to the commencement of operations. To attempt the planning and implementation of computer security subsequent to the commencement of operations is generally significantly more difficult.

The implementation of control over computer security requires, as a starting point, organisational computer security standards, procedures and guidelines.

# CHAPTER 4. DETAILED APPLICATION OF THE MODEL

CONTENTS PAGE

## 1. INTRODUCTION

This chapter describes how the analysis tables, used to present the model, have been constructed. A section on how the model should be interpreted is followed by a table for each area discussed in Chapter 3, i.e. Communications, Processing, Operations, Maintenance, and Office Services and Support Products.

## 2. ANALYSIS TABLES - CONSTRUCTION

Analysis tables are used to link control objectives achieved to the integrity control facilities. Risks which are prevented or detected by the utilisation of the control facilities have been identified.

The control objectives correspond to those detailed in Chapter 2 Section 2.2. Abbreviations have been used as follows:

COMP = Completeness of input, processing, updating of files and output

ACC = Accuracy of input, processing, update of files and output

INT = Maintenance (integrity) of data while transient (being transmitted) and static (once data files have been updated)

VAL = Validity/authorisation of business processing. This includes division of duties.

CONT = Appropriate programmed procedures or functionality. This describes the automated business procedures and whether they are in accordance with business practice and management's delegated expectations of what the system is supposed to do.

Integrity facilities are those discussed in Chapter 3. References to the applicable section in Chapter 3 have been included. The control objectives achieved by these integrity facilities and the manner in which the control objective is achieved are indicated as follows:

P = denotes a preventative control, and

D = denotes a detective control.

Risks denoted in the model are those exposures identified in Chapter 3, and have been referenced as such. Where a risk or exposure cannot be controlled by an integrity facility, an "R" has been used to denote the control exposure, under the appropriate control objective/s which is/are not achieved.

## 3. ANALYSIS TABLES - INTERPRETATION

The premise the model is built on is the need for an analysis of integrity controls, both by the auditors (internal and external) and management. Supporting this need is the importance of computer security, which is expressed in an organisation's computer security standards and procedures.

The primary focus of the model is to assess whether integrity facilities are appropriately used. This, in turn, depends on the application controls in place. Whether it is possible to replace integrity facilities by application controls will be decided on the practicalities involved, and effectiveness and efficiency considerations in achieving the control objectives.

The model also provides guidance on what control objectives should be addressed as a minimum, if integrity facilities in OS/400 are replaced by another software product.

The need for certain application controls is indicated where a risk factor is identified which cannot be addressed by an integrity facility. By specifying which control objectives are affected, some guidance is provided as to what procedure/s are appropriate.

Finally, the application of the model should be tested against the organisation's computer security standards and procedures, to ascertain whether management's delegated expectations are indeed being carried out. Possible deficiencies in these computer security standards and procedures could be highlighted by using the model.

Whilst both the internal auditor and management would perform all the above, usage of the model by external auditors would focus on an understanding of the control facilities used in determining whether a compliance or substantive audit approach would be appropriate.

## 4. COMMUNICATIONS TABLE

| CONTROL OBJECTIVES | | | | | INTEGRITY FACILITY | RISK |
|---|---|---|---|---|---|---|
| COMP | ACC | INT | VAL | CONT | | |
| | | | P | | 1. EXCHID parameter (2.2.1). | Remote unauthorised access to the AS/400 is gained. |
| | | | P | | 2. LOCPWD (2.2.1). | |
| | | | P | | 3. SECURELOC (2.2.4). | |
| | | | P | | 4. Local and remote location lists (2.2.4). | |
| | | | P | | 5. DDMACC parameter may be used to reject or restrict access by a remote system (2.2.3). | |
| | | | P | | 6. DDMACC parameter could invoke a user exit program which could validate the remote access request and which objects such request may access (2.2.3/4). | |
| | | | P | | 7. The PCSACC parameter may be used to prevent access by independent work station from other systems (6.3.1). | |
| | | | P | | 8. DDS Security Keyword used to invoke user profile (2.2.2). | |
| | | | P | | 9. System Distribution Directory (2.4). | |

4. COMMUNICATIONS TABLE (continued)

| CONTROL OBJECTIVES | | | | | INTEGRITY FACILITY | RISK |
|---|---|---|---|---|---|---|
| COMP | ACC | INT | VAL | CONT | | |
| D | D | | | D | 10. SNADS logging (2.3). | Data transmitted is lost |
| R | R | R | | | | Data is intentionally corrupted whilst being transmitted. |
| | | | P | | 11. Object authority over SST restricts access to SST (3.2.6). | Dumps are used to determine password or data content. |
| | | | R | | [Org S+P needed] | Non - AS/400 target system has inappropriate security set up, allowing access to unauthorised data. |
| | | | P | | 12. The SECURELOC parameter may be used to verify the user profile exists in the Target system (2.2.4). | User profiles in source and target systems are not in step, allowing inappropriate access. |
| | | | P | | 13. AUTOANS parameter (2.7.2). | |
| D | D | | | D | 14. Alert Support (2.6). | |
| | | | P | | 15. Object distribution (2.4.1). | |

5. PROCESSING TABLE

| CONTROL OBJECTIVES | | | | | INTEGRITY FACILITY | RISK |
|---|---|---|---|---|---|---|
| COMP | ACC | INT | VAL | CONT | | |
| | | | P | P | 1. Three levels of system security are available (3.2.1). | The security level used is not appropriate allowing unauthorised access to system resources. |
| | | | P | | 2. Password security is available in security levels 20 or 30 (3.2.2). | Unauthorised access is gained to the AS/400. |
| | | | P | | 3. A user profile must be created before a user may access the AS/400 (levels 20 and 30) (3.2.3). | |
| | | | P | | 4. Menu security (3.2.4). | |
| | | | P | | 5. Initial program and limited capability (3.2.5). | |
| | | | P | | 6. Sign on security defines maximum no. of unsuccessful logon attempts (3.2.8). | |
| | | | P | | 7. Authorisation lists (3.2.9). | Authorised user accesses unauthorised resources. |
| | | | P | | 8. Object oriented security (in security level 30) (3.2.6). | |
| | | | P | | 9. Logical views (3.2.7). | |
| | | | P | | 10. User classes (3.2.10). | |

5. PROCESSING TABLE (continued)

| CONTROL OBJECTIVES | | | | | INTEGRITY FACILITY | RISK |
|---|---|---|---|---|---|---|
| COMP | ACC | INT | VAL | CONT | | |
| | | | P | | 11. System authority (3.2.11). | |
| | | | R | | [Org. S+P needed] | Ineffective use is made of OS/400 security facilities. |
| | | | | | 12. ALLOBJ* special authority (3.2.11). | Unauthorised change made to system security level. |
| P | | P | | | 13. Commitment control (4.3.3). | Lockout of records during processing results in data loss. |
| | | | R | | (Version 1 Release 2.1 of OS/400 has a facility for enforcing the regular changing of passwords. | Access security is compromised by not enforcing regular changes to passwords. |
| | | | R | | [Org S+P needed] | By using the Adopted Security feature, users obtain an inappropriate level of access to data files and programs. |
| R | R | R | | | [Org S+P needed] | Field overflow error causes loss of data accuracy. |
| | R | R | | | [Org S+P needed] | Valid invalid data is accepted for processing, compromising data accuracy. |

5. PROCESSING TABLE (continued)

| CONTROL OBJECTIVES | | | | | INTEGRITY FACILITY | RISK |
|---|---|---|---|---|---|---|
| COMP | ACC | INT | VAL | CONT | | |
| R | R | R | | | 14. System authority and library security used to restrict access to commands (3.2.11). | There is unauthorised maintenance and/or duplication of records. |
| | | | R | | 15. Object authority and library security restrict access to Journal commands (3.2.6). | Before and after images used to determine sensitive data. |
| R | R | R | R | R | [Org S+P needed] | Intentional or unintentional changes are made to the DBMS and/or the data dictionary. |
| R | R | R | R | R | (Version 1 Release 3,0 of OS/400 enforces use of API's to control MI calls). | Inappropriate MI pointer authority is obtained (3.2.12). |
| D | D | | | D | 16. Journalling (4.3.4). | Complete and accurate update of files does not occur. |

## 6. OPERATIONS TABLE

| CONTROL OBJECTIVES | | | | | INTEGRITY FACILITY | RISK |
|---|---|---|---|---|---|---|
| COMP | ACC | INT | VAL | CONT | | |
| P | P | P | P | P | 1. System Keylock (4.2). | Unauthorised version of OS/400 is initialised. |
| R | R | R | R | R | [Org S+P needed] | System keylock is set to manual i.e. users may select a different IPL or use service tools which bypass resource security. |
| | | | P | | 2. Object authority used to control access to JOBCTL and SPLCTL commands (3.2.6). | Use is made of JOBCTL* special authority to spool confidential reports to an unauthorised user.<br><br>Spooled files containing sensitive information are viewed by unauthorised users. |
| R | R | R | R | R | [Org S+P needed] | Access to the operating system command line is not restricted, which may allow access to sensitive system commands or other objects not otherwise restricted. |
| | | | P | | 3. Restrict access to CRTDUPOBJ command via library and object authority (3.2.6). | Unauthorised objects are defined. |
| | | | P | | 4. JOBACN parameter can be set to *REJECT to prevent jobs being initiated from a remote system (2.4.1). | Unauthorised jobs are started in a remote system. |
| | | | D | D | 5. Job accounting (4.3.2). | Unaccounted for usage is not detected. |

6. OPERATIONS TABLE (continued)

| CONTROL OBJECTIVES | | | | | INTEGRITY FACILITY | RISK |
|---|---|---|---|---|---|---|
| COMP | ACC | INT | VAL | CONT | | |
| | | | R | | 6. QSECOFR and QSECADM user classes (3.2.10) | Access rights are dynamically re-defined by an unauthorised user. |
| | | | R | | [Org S+P needed] | The public authority parameter is not set to *EXCLUDE. As a result of objects not being in step with new user profiles created unauthorised access to objects is obtained. |
| R | R | R | | | [Org S+P needed] | Data is lost through the incorrect setup of the database. |
| P/D | P/D | P/D | | P/D | 7. Save and Restore, Journalling, Commitment control, ASP's, Checksum (4.3.1/2/3/4/5). | Inadequate backup and recovery procedures cause loss of data compromising data accuracy and/or completeness. |
| D | D | D | | D | 8. SNADS logging and Alert Support (2.3/5). | System errors are not followed up compromising data accuracy and error handling. |
| | | | R | | [Org S+P needed] | User profiles of MRT jobs or prestart jobs logged are those of the user starting the job. User profiles of jobs updating database files which are journalled may therefore not be valid. |
| R | R | R | | | [Org S+P needed] | No/inappropriate use of commitment control causes data loss. |
| R | R | R | | R | (DASD mirroring is available in Version 1,0 , Release 3,0). | Multiple disk failure causes data loss (checksum protection not effective). |

## 7. MAINTENANCE TABLE

| CONTROL OBJECTIVES | | | | | INTEGRITY FACILITY | RISK |
|---|---|---|---|---|---|---|
| COMP | ACC | INT | VAL | CONT | | |
| | | | P | | 1. User profile (3.2.3). | Access to production libraries does not provide appropriate segregation of duties between programmers, operators and users. |
| | | | P | | 2. Separate libraries may be used for development and production objects (3.2.6). | Segregation of duties between production and development staff is not enforced. |
| R | R | R | R | R | [Org S+P needed] | Default public authorities for data files and programs are set too low, allowing all users to read, add to, delete from and update such files and programs. |
| R | R | R | R | R | [Org S+P needed] | Programmers still have *ALL access right to production programs via ownership i.e. ownership is not transferred and all accesses except READ revoked on transfer of the program to a production library. |
| P | P | P | P | P | 3. File controls may be implemented over DFU functions (3.2.6). | Unauthorised access and/or changes are made to data files using the Data File Utility (DFU). |
| R | R | R | | | [Org S+P needed] | Inadequate maintenance procedures corrupt data. |
| | | | | R | [Org S+P needed] | Backup data is corrupted |

7. MAINTENANCE TABLE (continued)

| CONTROL OBJECTIVES | | | | | INTEGRITY FACILITY | RISK |
|---|---|---|---|---|---|---|
| COMP | ACC | INT | VAL | CONT | | |
| | | | P | | 4. System authority (3.2.11). | System Service Tool(SST) utilities are used to achieve unauthorised access to passwords or data. |
| P | P | P | P | P | 5. DST password (5.2.4). | Unauthorised use of DST compromises continuity and integrity of operations. |

## 8. OFFICE SERVICES AND SUPPORT PRODUCTS TABLE

| CONTROL OBJECTIVES | | | | | INTEGRITY FACILITY | RISK |
|---|---|---|---|---|---|---|
| COMP | ACC | INT | VAL | CONT | | |
| | | | P | | 1. Various application security facilities (6.2). | Unauthorised access is gained to documents, files or programs. |
| | | | P | | 2. Document and folder authority levels (6.2(i)). | |
| | | | P | | 3. ADRS parameter (6.3.1). | Unauthorised PC accesses the AS/400. |
| | | | P | | 4. PCSACC parameter (6.3.1). | |
| | | | P | | 5. Various application security facilities (refer processing table). | Support products are used to gain unauth. access to objects. |
| | | | R | | [Org S+P needed] | Inappropriate use of facilities allows unauthorised access to objects. |

## 9. CONCLUSION

The tables developed have highlighted potential computer security exposures where integrity facilities are not used, or are used inappropriately. These tables may be used by the auditor to evaluate controls.

Management, in discharging their responsibility to ensure computer security is addressed, may use the tables to assist in deciding which integrity control facilities should be used.

The need for computer security standards and procedures is clearly indicated by the model. The auditor should review these standards and procedures and their implementation, in conjunction with a review of integrity controls.

# CHAPTER 5. CONCLUSION

CONTENTS PAGE

## 1. INTRODUCTION

This chapter evaluates the success of the model developed in analysing the use of integrity control facilities, and establishes the relevance of the model in terms of:

- o use by Internal and External auditors,
- o use by Management, and
- o the organisation's computer security standards and procedures in the implementation of computer security.

## 2. COMPUTER SECURITY STANDARDS AND PROCEDURES

The organisation's computer security standards and procedures must be sanctioned and supported by senior management. Operational management, in implementing these standards, must institute business processes and procedures.

These processes and procedures encompass the work flow around an application program. An internal control analysis should be performed, to identify whether the internal controls contained in these processes and procedures are effective and efficient.

Both the auditor and management should such an internal control analysis.

The model developed provides a methodology for analysing whether the implementation of integrity facilities complies with these standards, and assists in the identification of possible omissions and inconsistencies in these standards and procedures.

Compliance with standards should result in the achievement of the control objectives outlined in Chapter 1, Section 2.2.

## 3. IMPLEMENTATION OF COMPUTER SECURITY

The implementation of computer security will depend on the business circumstances. Factors such as processing volumes, business exposures, employee skill levels, and the complexity of applications all play a role in determining how computer security should be implemented.

Efficiency considerations may dictate that application control procedures are replaced by integrity control facilities. Similarly, certain AS/400 integrity control facilities may be replaced by application program procedures and controls.

It is important that a control review be performed of all significant transaction cycles, both by the auditor and management, to evaluate whether computer security has been correctly and completely implemented.

## 4. EVALUATION OF THE MODEL

The model is useful in evaluating the usage of integrity facilities. Internal and External auditors would benefit from the use of the model. Internal auditors may use the model to review the effectiveness and efficiency of controls in an AS/400 environment, as well as the review of application programs, where both integrity controls, programmed controls and manual procedures and controls are included.

External auditors may use the model to evaluate the usage of AS/400 integrity facilities, in conducting both a General control review or a review of an application program.

The model would provide input on the nature and extent of internal controls, which the auditor could use to determine whether a substantive or compliance audit approach is appropriate.

## 5. CONCLUSION

The model has demonstrated the applicability of the Access Path and Path Context Models in the evaluation of integrity facilities in an AS/400 environment. An evaluation of control facilities was successfully carried out. Certain risks were identified which could not be controlled by any OS/400 integrity facilities.

The conclusion was reached that OS/400, in conjunction with certain application controls, can provide an adequately controlled secure environment. Where certain integrity facilities are not used, the AS/400 environment may not be considered secure.

Several weaknesses in OS/400 Version 1 were identified, however these have been addressed in OS/400 Version 2. Only OS/400 Version 2 or later versions (version 3 will be released shortly) may be considered secure.

The model has opened the door for research into other areas, for example the interfacing of the AS/400 environment with other environments such as an MVS/ESA domain, Local Area Networks, or architectures complying with OSI standards.

## BIBLIOGRAPHY


1. **Anderson, R.** 1990. Really understanding PC Support. News 3X/400, 1990, May.

2. **Attwell, B.** 1988. European trends in information systems. (In Ford, J., ed. 1988. Management of Information into the 90's. Cape Town: Juta). (Proceedings of the third NACCA Conference, September, 1988).

3. **Bloombecker, J.J.** 1989. Short-circuiting computer crime. Datamation, 1989, October.

4. **Boshoff, W.H.** 1990. A Path Context Model for Computer Security Phenomena in Potentially Non-secure Environments. Dissertation in fulfillment of a Doctors Degree in Natural Sciences, Rand Afrikaans University.

5. **Boshoff, W.H.** 1986. Computer auditing - taking care of technology. Accountancy SA, 1986, May.

6. **Boshoff, W.H.** 1985. The interface between application controls & integrity controls in modern computer systems. Dissertation in fulfillment of a Masters Degree in Economic Sciences, Rand Afrikaans University.

7. **Bosman, M.L., Damianides, M.A., Henson, D., Wadsworth, E.D., Wilson, H.J.** 1988. A control model for the analysis of control facilities and audit issues in a predefined mainframe environment - Part 1 - Advanced Communications Function for the Virtual Telecommunications Access Method (ACF/VTAM). A study done in partial fulfillment of the requirement for a Masters Degree in Commerce, Rand Afrikaans University.

8. **Clark, B.E., Corrigan, M.J.** 1989. Application System /400 performance characteristics. IBM Systems Journal, Vol 28 No 3, 1989.

9. **Conte, P.** 1990. A principled approach to security. News 3X/400, 1990, January.

10. **Conte, P.** 1990. OS/400 Level 30 Security Exposures. News 3X/400, 1990, January.

11. **Damianides, M.A.** 1991. A control model for the evaluation and analysis of control facilities in a simple path context model in a MVS/XA environment. Research essay in partial fulfillment of the requirements of a Masters Degree in Commerce, Rand Afrikaans University.

12. **Halper, S.D., Davis, G.C., O'Neil - Dunne, P.J., Pfau, P.R.** 1985. Handbook of EDP Auditing. Boston: Warren, Gorham & Lamont.

13. **IBM,** "Advantage AS/400", SA 21-9540-0

14. IBM, "Application Development Tools: Data File Utility User's Guide and Reference", SC09-1169.

15. IBM, "Application Development Tools: Programming Development Manager User's Guide and Reference", SC09-1173.

16. IBM, "Application Development Tools: Screen Design Aid User's Guide and Reference", SC09-1171.

17. IBM, "Application Development Tools: Source Entry Utility User's Guide and Reference", SC09-1172.

18. IBM, "Communications: Advanced Program-to-Program Communications and Advanced Peer-to-Peer Networking User's Guide", SC21-9598.

19. IBM, "Communications: Communications and Systems Management User's Guide", SC21-9661.

20. IBM, "Communications: Distributed Data Management User's Guide", SC21-9600.

21. IBM, "Communications: Distribution Services Network Administrator's Guide", SC21/9588.

22. IBM, "Communications: Programmers Guide", SC21-9590.

23. IBM, "Communications: Remote Job Entry Facility User's Guide and Reference", SC09-1168.

24. IBM, "Communications: User's Guide", SC21-9601.

25. IBM, "Office: Planning Guide", SC21-9626

26. IBM, "Office: Services Concepts and Programmers Guide", SC21-9758

27. IBM, "Office: Setting Up and Administering Guide", SC21-9627

28. IBM, "Office: User's Guide", SC21-9616

29. IBM, "PC Support: Operations Reference", SC21-8090

30. IBM, "PC Support: Technical Reference", SC21-8091

31. IBM, "PC Support: User's Guide", SC21-8092

32. IBM, "Programming: Backup and Recovery Guide", SC21-8079

33. IBM, "Programming: Control Language Programmer's Guide", SC21-8077

34. IBM, "Programming: Data Base Guide", SC21-9659

35. IBM, "Programming: Data Management Guide", SC21-9658

36. IBM, "Programming: Security Concepts and Planning", SC21-8083

37. IBM, "Programming: Work Management Guide", SC21-8078

38. **IBM,** "Security and Auditing Considerations", GG24-3322

39. **ISM,** 1991. Latest AS/400 and AIX PTF's. ISM Inform, 1991, July.

40. **Kirk, I.** 1988. Risks and controls in a distributed data base environment. (In Ford ed. 1988. Management of Information into the 90's. Cape Town: Juta). (Proceedings of the third NACCA Conference, September, 1988).

41. **Mair, C.M., Wood, D.R., Davis, K.W.** 1978. Computer Control and Audit. The Institute of Internal Auditors.

42. **Perry, W.E.** 1986. A Standard for Auditing Computer Applications: Selected Audit Areas. Auerbach Publishers Inc.

43. **Roberts, M.B.** 1985. EDP Controls. John Wiley and Sons.

44. **Schleicher, D.L, Taylor, R.L.** 1989. System overview of the AS/400. IBM System Journal, Vol 28 No 3, 1989.

45. **Stamps, D.** 1989. The AS/400's Surprise Role. Datamation, 1989, May.

46. **Stansbury, D.** 1990. Network security. News 3x/400, February.

47. **Systems Integration,** 1990. "Company: IBM. Architecture: SAA", Systems Integration, June, 1990.

48. **The American Institute of Certified Public Accountants.** 1977. The Auditor's Study and Evaluation of Internal Controls in EDP Systems. Audit and Accounting Guide.

49. **The American Institute of Certified Public Accountants.** 1984. The effect of Computer Processing on Examination of Financial Statements. SAS48.

50. **The American Institute of Certified Public Accountants.** 1988. Consideration of the Internal Control Structure in a Financial Statement Audit. SAS55.

51. **The Canadian Institute of Chartered Accountants.** 1984. Audit Strategy and Reliance on Internal Control.

52. **The Institute of Internal Auditors.** 1977. Data Processing Control Practices Report, Part II of the Systems Auditability and Control Study.

53. **The South African Institute of Chartered Accountants.** 1986. Accounting Systems and Internal Controls. Statement AU230.

54. **The South African Institute of Chartered Accountants.** 1989. Auditing in a Computer environment.

55. **The South African Institute of Chartered Accountants.** 1986. Guideline on Computer Audit skill levels.