ISSN 0961-9348

casg Computer Audit Specialist Group

JOURNAL

VOLUME 4 NUMBER 2 AUTUMN 93

The British Computer Society

Members' Meetings for 1993/94

Tuesday 9 November	**Automating software testing**	Mark Gillett Direct Technology Ltd
Tuesday 14 December	**Insuring computer-related risks**	David G Davies Hogg Insurance Brokers
1994		
Wednesday 12 January **IIA Joint Meeting** Contact: D Baker 0494 776188	**Legal aspects of document image processing** **Auditing aspects of document image processing**	Chris Reed Centre for Computer Law Studies Ken Tombs Independent Consultant
Tuesday 8 February	**Access control**	Dr Brian Collins PC Security Limited
Tuesday 22 February (Full Day)	**Discussion Group (Quality Issues)**	TBA
Tuesday 8 March	**Viruses**	Jan Hruska Sophos
Tuesday 12 April	**Annual Debate with the EDPAA**	TBA
Wednesday 11 May (Full Day)	**Annual Conference & AGM** (London Press Centre)	Outsourcing of I.T.

Meetings are usually held at the Royal Institute of Public Health & Hygiene, 28 Portland Place, London W1N 4DE (Ground floor, Lecture Room 1), except as noted above. For last minute confirmation, telephone 071-580 2731 or 071-636 1208. Meetings start at 4.00 for 4.30pm, unless otherwise stated. Tea and coffee are available before each meeting; sandwiches and refreshments afterwards.

Details of discussions groups are forwarded directly to members as part of the quarterly mailing. Please contact Bill Barton on 071 872 6720, or Steve Pooley on 0580 891036, for further information.

For details of the annual conference please contact Paul Howitt on 0992 644250.

SUBSCRIPTION REMINDER – See Page 2

LETTERS TO THE EDITOR

are welcome, write to:
Rob Melville

Centre for Internal Auditing
City University Business School
Frobisher Crescent
Barbican Centre
LONDON EC2B 2NU

Editorial

October promises to be a good month for the group, our meetings start with a very topical presentation on end user computing by my old friend John Silltow and a full day discussion group on LANS. It's not that long ago that auditors just did not consider PCs as entities to be audited: they were either no more than toys or they were potentially terrifyingly insecure. There can be few people in the profession who have done more to take the mystery out of auditing PCs than John, and there have been many occasions when I have been grateful for his capable and useful advice both at the Woolwich and since.

Another milestone has been achieved for your journal this month with the publication of our first 'refereed' paper. Refereed papers are significant because they extend the quality and quantity of our knowledge by developing ideas and practice and innovation. This entails a rigorous process of quality assurance, and it is a credit to our first refereed author Ed Hutt that he submitted to this. The process worked as follows: Ed Hutt wrote a paper which was initially reviewed by two committee members, to ensure it met basic criteria of readability and relevance. This review in itself would have satisfied many journals due to the professional status of the reviewers. We then sent the paper to be 'blindly' refereed by two academics with specialist knowledge of the field. (Anonymity ensures no favouritism or prejudice). Their comments and suggestions were passed to Ed, who then produced a final version for this edition. In all, the best part of a year's work. Our grateful thanks to Ed and to the reviewers who have made this huge contribution to our profession.

* * *

The editorial policy of the journal is to balance 'how to' articles with those that stretch the borders of our thinking. The rationale is that we must keep up with the leading edge of developments in information management and technology or we will be passively accepting the wisdom of industry. In the last two issues we have published two deliberately controversial articles (on information management and training) which attracted some interesting responses, not all in favour. These are covered elsewhere in this edition. As the editor and committee member for three years, I would like to encourage all members to respond to what they read, or would like to read in their journal. (No editor in their right mind would make unconditional promises though, so not all suggestions will be implemented. On the other hand, if you were in your right mind you would not be an editor . . .)

* * *

Any potential authors out there? We have had a lot of success with our monographs over the years but there are plenty of gaps to be filled. If you have an idea for a publishable 'how to' or 'what is' type book please write to me. We can arrange to have it published by the BCS and also provide you with a co-author and editorial advice if necessary. How about an auditor's guide to non-IBM operating systems, or retail point of sale systems? There are still so many gaps in our body of knowledge that one at least will tempt you.

ROB MELVILLE

The views expressed in the Journal are not necessarily shared by CASG. Articles are published without responsibility on the part of the publishers or authors for loss occasioned in any person acting, or refraining from action as a result of any view expressed therein.

EDP AUDIT

NATIONWIDE

TECHNICAL AUDITOR

Cheshire **To £27,000 + Bens**

Our client, a leading financial institution with a progressive EDP Audit department is currently seeking to recruit and expand its Technical Audit team. A degree, solid DP background, plus DEC VAX or IBM systems experience, and preferably Unix expertise will be of interest. The successful candidate should possess excellent communication skills.

COMPUTER AUDITOR

City **£25,000 + Bens**

International bank with an expanding Computer Audit department is recruiting for a graduate, Computer Auditor with a minimum of 18 months experience. Exposure to IBM mainframe and PC hardware platforms is of interest. Excellent opportunities plus overseas travel exist for the right candidate.

COMPUTER AUDITOR

Kent **£25,000 + Bens**

Our client, a leading financial organisation, is currently seeking to recruit newly qualified ACA with minimum of 12 months computer audit experience. IBM Mainframe and PC skills are of particular interest. Excellent career prospects are on offer to the successful applicant.

AS400 AUDITOR

London **To £35,000**

A Senior Computer Auditor with midrange (preferably AS400) skills to join an expanding team working for this internationally renowned blue chip corporation. Either an Accountancy or a DP background is required along with 2-3 years EDP audit experience. QiCA or CISA qualified would be an advantage.

SENIOR COMPUTER AUDITOR

W. Sussex **£26,000 + Bens**

Excellent opportunity with this blue chip company. The successful applicant will have 2-3 years experience, be QiCA or CISA qualified, and have had exposure to a variety of computer hardware and operating systems, primarily IBM, Tandem, Unisys and Dec. Effective communication skills and a professional approach to audits are essential.

INSURANCE

Surrey **To £30,000 + Bens**

This leading financial organisation with an excellent reputation for I.T. Audit and Security Controls throughout the industry is currently seeking to recruit a Senior Computer Auditor with a minimum of 2 years experience, particularly working on IBM mainframe systems. Excellent career prospects are on offer for the successful applicant.

BANKING

City **To £36,000 + Bens**

This leading international investment bank is currently seeking to recruit a Technical Auditor with exposure to Unix systems and networking. The successful applicant should be no older than 35, with 3 years EDP Audit skills within banking, educated to degree level and possess the ability to communicate effectively at all levels of management.

CUSTOMER BILLING SYSTEMS

1 year contract **Excellent Rate**

Based in the North of England, our client is currently seeking to recruit, on a contract basis, an EDP Auditor with extensive "CUSTOMER BILLING SYSTEMS" experience. The successful candidate will have preferably worked for a major utility and have exposure to ICL or IBM mainframe platforms. On top of excellent rates all expenses are paid.

COMPUTER AUDITORS

Move Into Consultancy

UK wide **To £35,000 + Car**

A number of the BIG 6 audit firms are expanding their EDP Audit teams. They are seeking to recruit qualified Chartered Accountants or DP professionals with a minimum of 18 months computer audit experience. Successful applicants must possess a degree, be under the age of 30, have the ability to communicate at all levels of management, plus the confidence to develop new business. Excellent career prospects are on offer.

INTERNATIONAL TRAVEL

London Base **To £45,000 + Bens**

This leading financial services organisation, with a first class international reputation, would be interested to hear from accomplished EDP Auditors. You must be keen to accept a challenging opportunity, providing an Internal Consultancy Service to IT operations throughout the world. This is one of the best positions at this level currently on the market.

MBA

The first step towards your next career move should be to contact Sean Farrell on 071-454 9010 (till 5.30 pm) or 081-318 4521 evenings/ weekends. Send a full cv to
Michael Bailey Associates Ltd,
Rococo House, 281 City Road,
London EC1V 1LA
Fax: 071-490 3361

MBA

Contents

Chairman's Corner

John Mitchell

In a previous edition of this Journal, I discussed the differences in the various computer audit related qualifications. This provoked a thoughtful response from Brian Selby in the shape of a letter to the editor. Well done Brian for taking the time to put pen to paper. We like to receive feedback from our membership and a letter to the editor is a sure way of informing us of your views.

I once wrote that one of the advantages of being chairman was that I could write what I liked in my 'corner' without much fear of editorial interference. However, your editor is not adverse to 'blue penning' the verbosity of your chairman, and he removed my comments on qualifications from this section into one of their own. So you were correct in your assumption Brian, that the article was not an unbiased opinion. I am indeed biased towards CISA, because it is an internationally recognised qualification and I still do not understand why the IIA-UK went to the trouble and expense of creating yet another qualification in this area. CISA also has a continuing further education requirement which ensures that its holders keep themselves up-to-date after qualifying. On the MBCS/FBCS debate Brian did not mention that you need to be MBCS before you can get the Fellowship. I own up Brian, I was once under thirty years old and do have an MBCS. My point in quoting Richard Sarson was that he is a well respected computer journalist and his point that you do not need to be a member of the BCS to practice in the IT arena touched a chord with me; in much the same way that you do not need to be MIIA to be an internal auditor.

Now this last point is important. A true 'profession' is one that you can only practice if you are qualified to the required standards of the appropriate professional institute. Typically, such institutes will have been granted the protection of a Royal Charter and you will only be able to practice if you become a member of the relevant 'club' (or closed shop!) and they will probably require you to pass their examinations first. You just try calling yourself an accountant, or a surgeon, without being a qualified member of the relevant trade association. It will not be long before you end up being hung, drawn and quartered.

Now interestingly, the BCS has a Royal Charter, but you can still practice computing without being a BCS member, so I would argue that computing is not a true profession. Likewise, you can practice as an internal auditor without being a member of the IIA and without any other qualifications to boot, so I argue that internal auditing is not a true profession either. So where does this leave EDP audit? I see it as sitting in an uneasy halfway position between two non-professions. If you wish to be a professional EDP auditor, as based on my earlier rules, then you have to become TickIT qualified and be accepted by that particular club! Pretty depressing isn't it, but someone has to raise these issues and it may just as well be me, who as a member of the BCS, IIA and EDPAA has a toe-hold in three halfway professions!

Finishing on a brighter note however, South Bank University are offering a part-time MSc in internal auditing with electives in Information Technology and Quality Assurance. It may not make you a 'professional', but you will be able to put 'MSc' after your name, and those letters mean something to everyone!

Membership Renewal

Some of you reading this edition of our Journal will not have renewed your subscription for the current season (subscriptions are due in August of each year). Others of you may be unsure whether you have renewed, or not. If you are in this last category, please contact our membership secretary, Jacqui Race, at the Stock Exchange on 071 797 3551 to establish the current situation.

If you have not yet renewed your subscription, I urge you to use the renewal form that you will find elsewhere in this Journal otherwise you will lose out on the significant benefits of membership. These include:

- free attendance at our late afternoon meetings
- free quarterly journal
- 20% reduction in the subscription price of the *Computer Fraud and Security Bulletin*
- 20% reduction in the subscription price of *Computers and Security*
- a saving of at least £75 on our own Annual Conference
- 25% reduction in the subscription to the *Quality Software Report* newsletter
- discounts on attendances at many other conferences and training opportunities
- the opportunity to take part in our twice yearly Discussion Group

As Corporate membership costs only £75, you will realise that membership of the Group can actually save your organisation many hundreds of pounds each year.

Abstract

Stratus systems are often used to run critical business systems. However in many cases, these systems are treated as a separate unit from the remainder of the corporate IT strategy and management structure. For the purposes of this article, we call this the "small installation" and it is characterised by limited human resourcing, security policy implementation which is incompatible with that of the remainder of the installation, and often some quite gaping holes in system security.

This is unfortunate because the business applications running on these systems are often processing high value and/ or high volume customer focused transactions, and any management weaknesses can have a considerable impact in terms of adverse publicity.

In the following sections, we examine the principles of "continuous processing" and the reasons why an organisation will purchase systems which provide 100% up-time. From this, we examine some of the key weaknesses that are frequently present, and especially the importance of privileged users on a Stratus system

Fault Tolerant Auditing

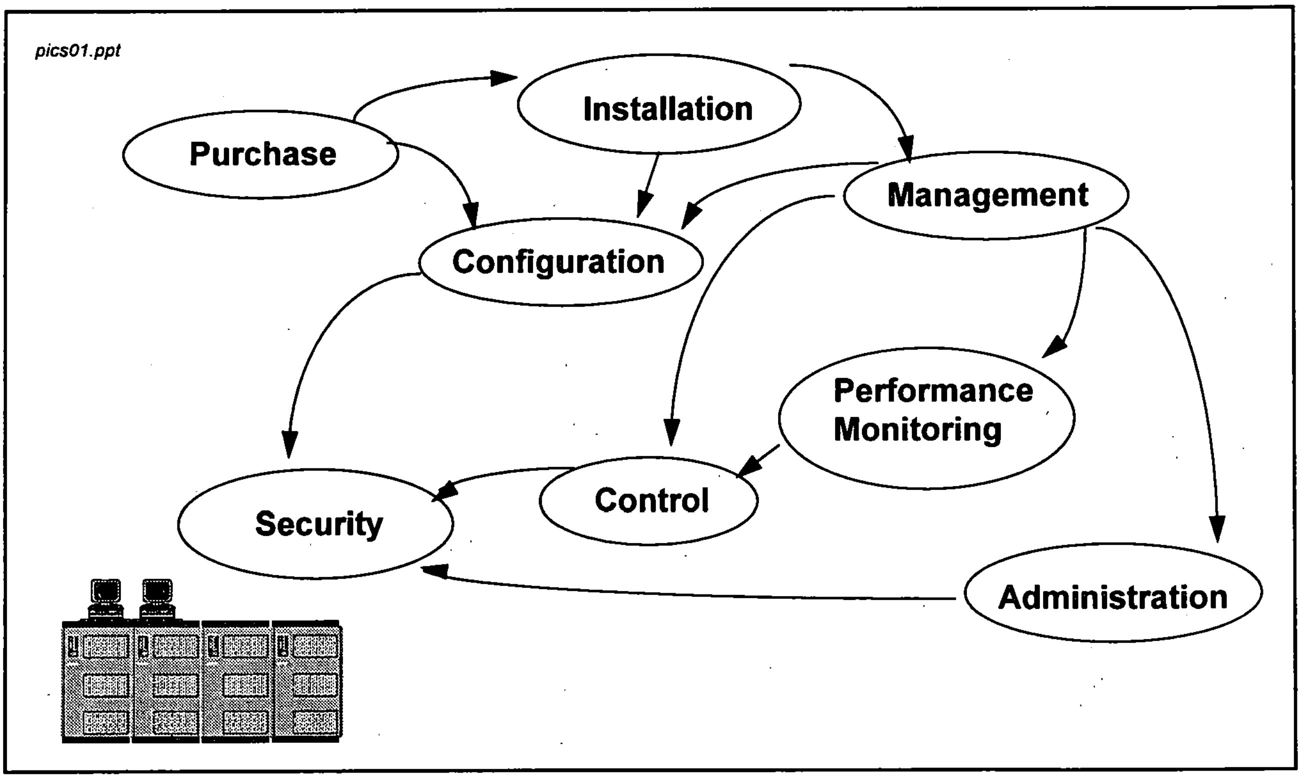
Ed Hutt

Coopers & Lybrand, West London

Ed Hutt is a manager in Coopers & Lybrand computer assurance services group, based in West London. He is a member of the Institute of Internal Auditors (QICA) and is a CISA.

Since 1991 he has been a member of the IIA Stratus audit and security group, focusing on management and technical issues relating to Stratus systems. If you would like further details of the activity of this group, please call Ed in the UK on 0895-274737.

This article is written as an up-to-date guide to the management, control and security features of Stratus XA and XA/R fault tolerant computers, and the proprietary Stratus/VOS operating system. It also examines some of the many issues (outlined below) which must be considered by auditors and security analysts in relation to systems running mission critical business systems and which require continuous availability. This forms a part of a larger audit and risk model for systems requiring continuous availability.



The scope of Stratus 'continuous' auditing

Overview of Stratus systems

STRATUS Computer inc. is an American producer of continuous processing (sometimes referred to as "fault tolerant") mini computers. The business applications that run on Stratus systems are those which usually require *complete* availability 100% of the time. For these business systems, *high* availability (perhaps 95% of the time, or even 99%) is not adequate to meet the *business objectives* of the organisation.

Stratus systems are commonly found in a number of different industry sectors.

Financial sector

Retail and investment banks, building societies (thrifts) and retail organisations use Stratus systems to drive On Line Transaction Processing Systems (OLTP), such as:-

- Electronic Banking Systems
- ATM (banking) systems
- Credit/ debit card processing and authorisation systems
- EFTPOS authorisation and transaction tracking systems
- Investment banks dealing systems

Manufacturing process control & automated warehousing

Stratus systems are also found in the manufacturing and process control environment. Examples of the types of uses to which these systems are put may include the following.

- Driving factory production flow lines (as in a tractor construction factory),
- The operation of automated machinery whose failure may be "safety critical" if it fails (ie: dangerous to human life - as in the case of nuclear power control systems or cranes used to transport heavy loads in a warehouse environment)

Travel & transport

Stratus systems are used in mission critical business processing system such as airline booking and reservation, where non availability may result in a considerable loss of income due to the tight margins under which airlines are forced to operate.

Leisure

The gambling industry is a major user of Stratus systems world-wide, where gambling machines are required by legislation to be monitored centrally or where a risk position has to be monitored centrally when issuing statistical odds on races or other probability driven activities.

Communications

Stratus systems are often found switching messages in a communications network. This may include telecommunications companies voice traffic and data traffic in a large communications network.

Fault tolerance

Stratus Computer Inc. began developing and selling continuous processing computer systems in the late 1970s. At this stage it was relatively inexpensive to perform programming work and relatively expensive to purchase hardware components. Stratus Computer took the strategic decision to base its fault tolerance on hardware rather than software. As computer systems have developed over the last fifteen years there has been a switch from hardware being inexpensive to hardware being less expensive, and from software being inexpensive to write, to it being very expensive indeed.

This contrasts with the approach taken by Tandem Computer Inc., another mid-range computer company, also from the United States, who took the view that fault tolerance should be built into not only hardware but also into software as well. This applies to applications software and the method in which it is programmed whilst being developed and subsequently maintained. Tandem Computers also have 'duplexed' parts. This means that they are similar to Stratus XA and XA/R computer range which are fully duplexed. However, the distinction lies in the processing power that is available to either system in the event of a failure. If a hardware part fails on a Stratus computer (say a processor board), then that computer carries on processing at the same throughput as if there were duplexed parts. With a Tandem computer transactions are processed through both duplexed processor streams. This means if there is a hardware failure, then only half the processing power is now available to that computer. This presents quite a strong contrast to the Stratus computer which carries on processing at full power. Tandem computers also contain software fault tolerance, where error correcting routines are written into the application software to correct errors which may be caused in processing.

Fault tolerance then comes in two forms:

- Hardware Fault Tolerance
- Software Fault Tolerance

Hardware fault tolerance is implemented through hardware design. All parts of the computer are duplexed (that is, there is two of everything). The processing units internally review each process and calculate numerical accuracy before release for further processing.

- Process instructions are passed along the bus (transmission channel) to the processor boards (one either side of the bus to provide a duplex architecture).
- The same process is performed by processor A and B, and the results compared.
- The same process is performed by both boards on either side of the bus.
- The results of processor A & B for both boards is compared, and the board with two identical results is accepted as the correct version.
- If both boards have identical results then there is no contention on results.
- If one board has a miss-match between processors, then the result from the other board is accepted.
- The board with the mismatch is taken out of service; an action known as a 'red light event' because of the red light illuminated on the front of the defective board.

In contrast, software fault tolerance is built into the software design by committing transactions only when they are completed and have been reviewed by software processes for accuracy and integrity. If an error in processing occurs then the transaction is rolled back and the initial start point prior to that transaction is established. A change to fault tolerant software will necessitate potentially expensive changes of the application to meet changes in the programs processing. Stratus system are based on hardware fault tolerance. This means that business applications written for Stratus systems only have to be integrated with the operating system processes. They do not have to be written in a fault tolerant way, but the systems running on these machines are then continuously available, 24 hours a day, 365 days of the year.

How continuous availability is achieved

The Stratus platform is used for critical applications where the assurance of continuous availability of applications that generate revenue or provide customer service is required. For these operations, a high availability - the ability of the application to run for the majority of the time, but with certain periods of down time - is inadequate. To provide this continuous availability, Stratus computers combine hardware fault tolerance with on-line system administration and maintenance provided by a remote service network (RSN). Stratus computers "phone home" to the customer assistance centre (RSN) to report hardware faults. This stimulates (subject to contract) the dispatch and installation of replacement parts and so allows the processing of data to continue even during system upgrades and major maintenance work. In addition, there is a third "leg" to continuous availability which is the existence of a tested and fully functional disaster recovery plan, which supports the business systems in the times (such as in St Mary's Axe in1992) when even hardware fault tolerance and the rapid delivery of spare parts was not enough to save a number of sites from an IRA bomb.

Continuous contingency

There is a common fallacy that, because Stratus modules are "fault tolerant" and have a duplex architecture, there is no need for additional disaster recovery planning. The obvious error in this argument is that disasters of a global nature (the bomb, falling airliner, flood, network outage.) will affect both the "sites" in one go and so result in the system being unavailable until it can be replaced at source. Some organisations are also taking the view that possession of a "basic" module, consisting of only the minimum component set required to operate a live system is sufficient. This may include the module being equipped as a simplex system (boards not duplicated) with the view to equipping the module with additional boards and disk packs in the event of a contingency. The advantages and disadvantages of this approach are considered below.

Advantages

- Lowers cost of the contingency system, which otherwise may be a significant cost if run as a fully duplexed system. This may be a considerable issue in some organisations where the Stratus system is seen as being peripheral to core accounting systems.
- Ease of upgrade to a duplex system based on the existing RSN supplies network
- The basic processing infrastructure is in place and is capable of being tested even in the simplex environment.

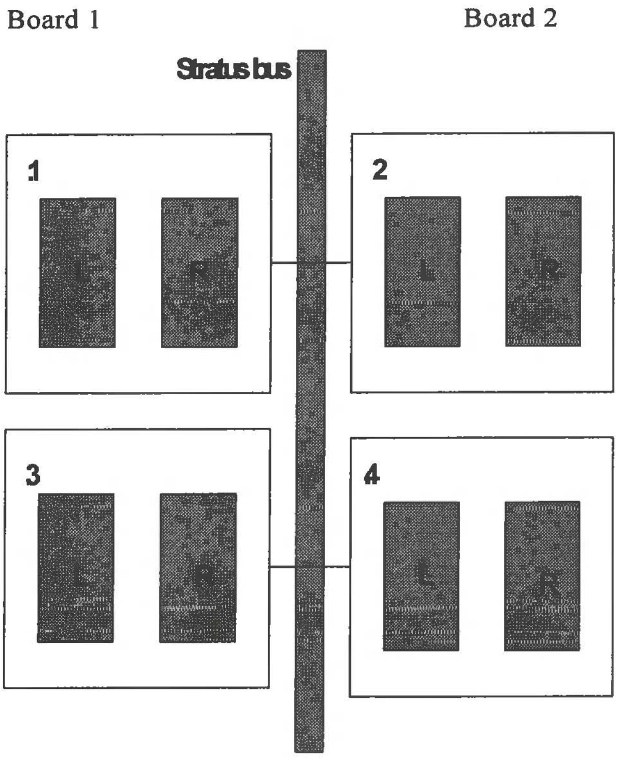
Disadvantages

- Increased risk in the event of a "global" disaster in a small geographical area. (ie: St Mary's Axe bomb in 1992 which was within range of at least 20 Stratus sites)
- Lag time between declaration of disaster and ability to commence operations at the second site. This may be critical in certain systems which require continuous availability.
- Performance testing may be ignored.
- Testing (especially the switch over from site A to site B) may be difficult in the event of the B site being simplex. During the transfer from A to B (and in reverse) there is the risk of the live site being simplex and so the original continuous availability objective will not be achieved.

Disaster recovery is one of the "three pillars of wisdom" of continuous availability along with hardware fault tolerance and the remote service network. In many cases it is the Achilles heel of a business system that requires continuous availability, because continuous availability means 24 hours and 365 days, and this requires adequate contingency planning. Without computer contingency planning that is effective and tested, an organisation's investment in fault tolerant hardware may be wasted in the event of a minor disaster.

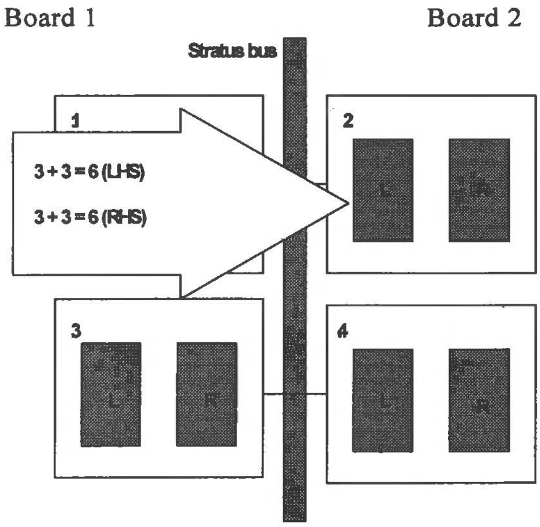
Stratus systems are built to be hardware fault tolerant. This means that:-

- All component boards have a common layout which provides self checking of all processes. This is shown in the diagram below.



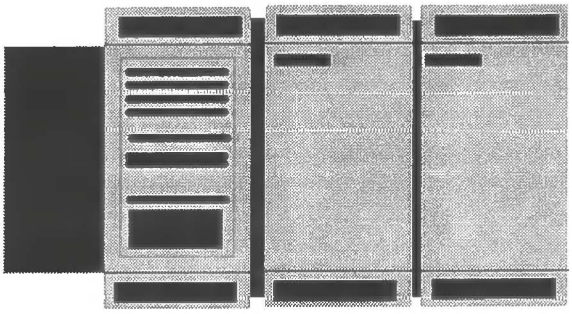
Duplex boards in a Stratus module

In this example, the two processor boards are shown. The two boards exist either side of the "Stratus bus" which is the communications channel by which all components receive and pass data and instructions. In the next stage of the process, a transaction is introduced and processed by both of the processor boards. In this case it is an arithmetic calculation (3+3). The calculation is carried out by both boards at the same time and the results matched. Within each processor board, the calculation is also carried out twice, by different internal components. Consequently, any error will be detected within the individual component, and this will result in the whole board being taken out of service by the operating system. This is termed a "red light event".



Application of a transaction to a duplexed processor pair

Critical components are duplexed (paired) to provide resilience. This includes disk packs, power units, memory boards, and I/O units. The only parts that are "simplex" are the back plane board (the cabinet unit connection to the component parts) and the tape deck unit.



Opening the modules cabinet.

Hardware failures are automatically reported to the Customer Assistance centre over the remote service network. Replacement parts may arrive for fitting before an installation is aware of having a 'red light event' (a fault on a duplex component). In addition to the fault tolerance provided by duplicate boards and disk pack configuration management, there are also duplicate power packs which allow the system to be either run from UPS sources or to be shut down in a controlled manner.

Stratus systems and the "small installation".

The types of organisations that use Stratus systems are currently very diverse. They vary from small to medium software houses and financial institutions through to extremely large organisations who have a total IT spend of many millions of pounds every year. Some of these organisations use only Stratus systems for core processing while others use Stratus systems for peripheral processing. This concept is explained further below.

Core processing

This means that the organisation's central accounting, management information, production control or control systems are based on the Stratus platform. This is generally not a common situation.

Peripheral processing

This refers to organisations which have one application or one application type running on the Stratus platform. It may perhaps be an ATM system in a financial institution or a production control system in a manufacturing and warehouse system. This is a much more common situation at present.

There is an issue relating to 'peripheral processors' that do not allocate resources to their Stratus systems and tend to have weak control and security implementations. This is the concept of the "small installation" where the applications that are loaded on the Stratus systems are treated as potentially less important than those running on the corporate mainframe, and have very limited organisational segregation of duties between the security administrator, programmers and in some cases, users. An outline survey in the UK in 1993 revealed the following trends in respect of "small installations".

Small Installations	Total sites
14	28

In other words, half of the key UK Stratus sites are treated in this way by their IT management, and so have potentially serious management and security issues that are not being addressed.

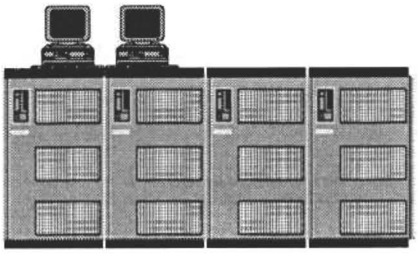
Implementation planning

Stratus systems, being hardware fault tolerant, are expensive to purchase as we have already discussed. This means that it is vital that the systems that are purchased are correctly sized and subsequently implemented in order to maximise the benefit to the purchasing organisation. It is in this process that an internal auditor or security analyst involved in the early stages of the selection and development project can make significant contributions to the quality of the delivered system and to the value for money received by his or her organisation from this system.

The Stratus Hardware Architecture

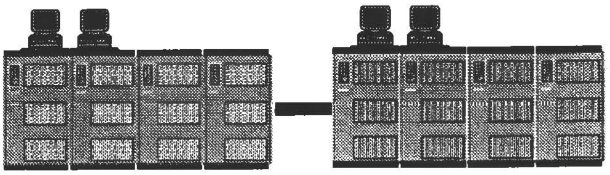
An important concept in the audit and security of Stratus systems is the distinction between Module, System, and Network.

A module is a single self contained processing unit. It contains a single logical CPU board (dual physical boards for fault tolerance); memory boards; disk packs; an IOP and tape subsystems. These are linked by a common back plane board. A module has a single copy of VOS running on it.



A single module may typically represent a production control unit or a small ATM/POS card authorisation system. Because each module has fully duplexed parts, it has built in contingency, and so there is no need to maintain a separate machine for operational purposes (although the need for a separate machine for disaster recovery purposes may still be present).

A system consists of between 2 and 32 Modules, connected by the networking protocols and systems of **Stratalink**™ or **Stratanet**™.



Each module on the system has its own copy of the VOS operating system. It is possible that two modules on a system may be running different operating systems. For instance:-

- %VGC#m1 runs VOS Version 10 Release 1
- %VGC#m2 runs VOS Version 8 Release 2
- %VGC#m3 runs FTX Version 1

A **system** may typically represent a large credit card authorisation unit, or a large banking and broking unit. A **system** may be split between a number of sites and used for different purposes. For instance an ATM system may have a live module with a separate development module at a separate location for two site contingency purposes.

A network contains (at VOS version 11) up to 8000 modules linked by Stratalink™ or Stratanet™. The distinction between a system and a network is that a system is going to be owned by a distinct business unit (such as a legal company). A network may be split between related organisations, or between companies and the Customer Assistance Centre (CAC).

A Stratus module must consist of at least:-

- A single back plane board with a multi slot chassis for:
  - Processor
  - Memory component boards.
- A separate IOP (communications subsystems).
- One physical disk pack attached to the back plane board

The module may additionally have:-

- Tape subsystems for input and output
- Optical disk storage
- Additional disk packs
- Additional processor and memory boards up to the capacity for that chassis
- Additional communications hardware added (to address other network architectures)

Each Stratus module comprises a number of physically similar hardware parts. There are a number of different chassis types ranging from the ten to the forty slot chassis models, but generally most models of Stratus computer comprise similar components. The actual differences between Stratus modules occur in the technical specification of certain components. The importance of this information to the auditor lies primarily in assessing the systems sizing during a selection exercise, or in the assessment of costs for future operation.

Auditors are often involved in the selection process, and it may be necessary for them to assess the implications to their organisation of choosing a chassis that will require upgrade (or is too large) if actual transaction volumes increase beyond the capacity of that system at the time of sizing.

All Stratus hardware modules consist of at least two cabinets joined by an air plenum. (An air plenum is a part of the cooling system and allows air to circulate around the hardware parts). Access to the innards can be gained from either side of the cabinet, and parts fitted to either side. There is no distinct "back" or "front". The disk packs on a Stratus module may be distributed between front and back cabinet frames and there is no physical or logical restriction as to their location in the chassis. The processor boards are always located in the first chassis cabinet, with the IOP units in the second. A number of cabinets may be used where a large number of disks are used in conjunction with a forty slot chassis module. This allows for expandability (and reduction) of components over time in conjunction with changes in business requirements.

XA model computers are based on CISC (Complex Instruction Set Computer) processors. The XA/R modules are available under VOS version 11 as the model XA/R 20. This is based on RISC (Reduced Instruction Set Computing) processors and may become more popular in the short run as more speed is required from existing configurations.

Applications and programs compiled for an XA module type must be recompiled in order to run under the RISC architecture. The RISC processor units are now becoming more common and should produce a more rapid throughput of transactions in situations such as ATM processing where the volume of throughput may be a constraint on the use of other systems. In this case, both fault tolerance and performance are critical issues and must be included in the scope of audit work relating to selection and implementation planning.

On all models, single component boards can be decommissioned or removed without affecting system performance. This is, after all, how the RSN is able to load and remove components so fast. No down time is required during this operation and the machine does not have to be switched off, although earthing precautions should be taken. This shows us the advantages of fully duplexed fault tolerant hardware system. It also reveals an added risk of theft and error because components can be decommissioned (either with or without authorisation) and subsequently left unreplaced.

Logical file and directory naming conventions

The naming convention applied to modules is **% (name of system) # (name of module)** where:-

- **%(name of system)** is the name of the system often reflecting the company name (ie. **%VGC**) and prefixed by a % sign
- **#(name of module)** is the module name prefixed by a # sign (ie. **#m1**)

Each module consists of a number of disk packs. The naming convention for disk packs follows on from the system and module where:-

%VGC#m1_d01 is system		**VGC**
	module	**#m1**
	disk pack	**_d01**

There may be a number of disk packs on any module. These will be numbered consecutively **_d01**, **_d02**, **_d03** etc. Each disk pack is declared to the VOS operating system as a separate entry in the **devices.tin** file. This entry is made by a member of the **SysAdmin** group.

Audit issues

It is necessary to identify all of the disks in order to include all of the disk packs within the scope of an audit. Applications are generally spread across a number of disk packs to enhance system resilience and this presents another audit issue in that the spread of data and programs must be such that critical items are not "bunched" as result of this policy being misinterpreted by the implementation planning team. Therefore, the operating system may be on **_d01**, the applications on **_d02**, and data spread across **_d02** and **_d03**.

Each ***module*** has one disk pack that is designated as the ***pack master disk***. This is the boot disk that is used by VOS to:-

- Load the operating system into memory during module start-up
- Resolve the path name of the user's default home directory (home_dir)

On multi module ***systems*** a ***principal_master_disk*** may be established. This is the pack master disk of one module in the system, and this is used to store the configuration directory. This is done to:-

- Eliminate redundancy between system modules
- Centralise system files
- Ease system administration

Audit issues

This has the associated audit issue of scoping, and whether the disk contents (such as module_start_up.cm) that is reviewed as a part of the audit is actually the macro that is used to start the system.

This configuration is achieved by way of **links** that are created within the VOS operating system. Links are commonly used on multi-module Stratus systems and must be considered as a part of the audit planning and review process. Multiple modules can share a common configuration file *(configuration.sys)*. This allows for a much higher degree of control over the configuration of the individual Stratus modules because the security administrator has only one file to manage, and the auditor has only one to audit. This situation will also reduce the risk of changes being made to the configuration file which do not fit in with the site's security policy, or which are inconsistent between different modules, so leading to additional file maintenance costs.

Changes to hardware configuration

The data definition (**.dd**), table input (**.tin**) and final files (**.table**) of board, disk and device configurations are stored in the *>system>configuration* directory. There are five basic steps in the update and installation of change to this directory:

- **change_current_directory** to the configuration directory on the principal master disk
- use the **edit** command to modify the .tin file for the appropriate disk, board, or device
- use the **create_table** command
- install the table file into the directory **(master_disk) > system** using the command **broadcast_file**. This places the request in a queue serviced by the Overseer. The path name of the queue is:-

%VGC#m1_d01>system>broadcast_queue.message_queue

- configure the board, disk or device using the commands:

  configure_disks
  configure_boards
  configure_devices

Audit issues

This tells VOS to recognise these components at once. This does have an audit impact in that the start_up.cm macro settings can be changed interactively by the use of these commands. Extra terminals (devices) can be added to a module or system, and subsequently removed without any reference to the action appearing on the start up program settings.

All parts (other than boards and disks) in the Stratus cabinets and attached to the communications lines have an entry in the devices file. This is a powerful networking control, as all external and internal devices (login terminals, ATM's, & POS terminals) must be declared in this file in order to be used. Only privileged users may access these files, therefore ultimate control is achieved by control of privilege.

Audit issues

As all terminals and routes by which data can be extracted (and in some cases input) must be in the devices file, you can see that this is a very important file on any Stratus system. This is especially important in relation to business critical systems such as card processing systems where there may be many terminals to a system spread around the world.

VOS Operating System

VOS is the "Virtual Operating System" and is the current proprietary operating system for Stratus computers. VOS has approximately one major release per year, with a number of sub releases to provide corrections to new problems which may arise, or in response to operational issues which have been identified in design. Stratus users are not forced to follow an annual upgrade migration path and there are currently many different variants of the VOS operating system in circulation. As a result, Stratus users are now running a wide range of VOS versions world-wide. In some cases, a given site may be running different versions of VOS on different modules within the same data centre. This has the advantage of allowing organisations to plan their system technical architectures over a longer period of time, but has the obvious disadvantage for auditors who may be faced with a variety of disparate operating system versions, all with their own particular security, operational, performance and management issues to consider and review. In many cases, they will not have the advantage of having the technical support from their systems programmers because the provision of training for that version of the operating system will no longer be available.

VOS is a self contained operating system that has no "add on" security package in the way MVS needs RACF or similar security package to be added onto it. Program and data security is provided by operating system features while system integrity is provided by the applications running under the operating system. VOS is written in the high level language PL/1, with some communications routines written in C. This means that all files and table appear in source format in a language and style that can easily be understood by computer auditors. This is in marked contrast to other operating systems that are written in assembler format and cannot be easily understood.

The operating systems currently supported by Stratus areas are:

●	VOS	Virtual Operating System
●	FTX™	Fault tolerant UNIX (V5.4 UNIX)
●	PICK	The PICK operating system running under a VOS host.

Although VOS is the current proprietary operating system for Stratus systems (1993) with industry moves towards open systems, this situation is likely to change over the next few years. Stratus have declared (Stratus Computer inc. Annual Report 1991) this change as inevitable, however a large number of VOS sites will certainly remain beyond any strategic transition from supplying VOS to supplying only UNIX by Stratus. VOS is heavily biased towards on-line transaction processing and this is where it is most commonly found. FTX™ is biased towards communications, and is now commonly found in many parts of the world as the operating system that is used for message switching systems. This is a situation which is going to become more common as the industry trend towards using UNIX for message switching becomes better developed. FTX (Fault tolerant UNIX) the fault tolerance Stratus platform provides continuous availability for critical switching and communications systems. However, this does raise the question of how "continuously available" a message switching system has to be. What is the business impact of somebody dialling a telephone number and instead of getting the ringing tone they get the dial tone again? The natural reaction in this situation is to dial the number again so the actual business impact is slight. How many organisations will be willing or able to pay for this level of continuous availability? This situation would apply to modems and communication links as well. Perhaps the business impact is in fact not sufficient to warrant the cost of a fully duplexed message switching system.

The internal structure of VOS binds the applications to the operating system, and consequently restricts the range of application that can be run to those which have been optimised for this particular environment. The software architecture of VOS applications uses the ***Requester - Server*** model and is process based, rather in the same way as that of the UNIX operating system.

VOS command structure

VOS is a command driven operating system. That is, it does not have "Utility Programs" attached to the operating system in the same way as a large mainframe operating system like MVS. All functions (including **login**) are called by the use of commands, or strings of commands, on the command line.

VOS commands are classified into two categories:

- **Internal (operating system commands)**
  Part of the operating system and residing in memory
- **External (application system commands**
  Executable programs or command macros that are on the hard disk as part of the system. They are read into memory in order to be executed.

Privileged commands

Privileged commands are a subset of internal commands. They all have a global effect on the system (such as "shutdown") and can only be executed by privileged users. They are all operating system commands.

Audit issues

Privilege is one of the most important issues in Stratus installations world-wide. This is an area that is frequently mis-understood and it may result in the allocation of inappropriate or unauthorised levels of privilege to users who may then be able to change their own access rights to suit their own wishes rather than meeting the needs of the organisation's security policy.

Under VOS, the allocation of privilege is key to the security of the operating system, and because of the close architectural relationship between the application and the operating system, it will also affect the security of data and programs. As auditors, if we can successfully recommend that the allocation of privilege is adequately controlled (ie it is allocated to only a very limited number of users in the production environment) then we have made a significant contribution to system security.

VOS Directory Structures

All data, programs, macros, boards, disks, and users, are contained within files. (rather like in the UNIX operating system) All files belong to directories, and directories are arranged in a hierarchical structure under each disk pack. The naming convention for directories applied in VOS follows on from the naming convention of systems, modules and disks. Directories and files in a hierarchy are divided by the > sign. VOS is supplied with certain default directories. Most of these will remain on the live system once it has been installed. Each site is able to configure its own directories and files. These will vary from site to site depending on the number of users and the applications in use. Each user has at least one directory and may have a number of files. Each application may have a number of directories and files. These may be split over more than one disk pack.

All users are assigned a home directory (home_dir). This is the location in the directory structure at which they will arrive when executing **login**, or when changing back to their default pack master disk from another disk. A group is a set of users, and a user must be a member of at least one, but not more than five, groups when being registered on the system by system administration. A group directory is a set of users' directories grouped together for the purpose of allocating access to system resources. All users are assigned a home directory (home_dir) within the directory structure. This is the location in the directory structure at which the user is placed:

- when executing the command, **login**, or
- when changing back to their default pack master disk from another disk, or
- when using the command **change_current_dir (ccd)** without a declared path as part of the command.

A group is a set of users, and a user must be a member of at least one, but not more than five, group(s) when being registered on the system by the system administrator. A group directory is a set of user directories grouped together for the purpose of allocating access to system resources.

Installation Planning & privilege

An important aspect of installing a Stratus system is the planning of which users, programs and processes will have access to which files and directories. Access control is based on specific permissions (primarily) and also inherited default permissions. These default permissions are derived from a position in the hierarchical structure of the systems directory tree. If the arrangement of a system's directory's and files are incorrectly planned at installation, then the control of the complete system becomes harder for the systems administration team in the future. This applies both to the logical access control to specific directories and files, and to the physical administration of individual access rights, where group access would have been appropriate.

Installation planning also requires the integration of the Stratus system(s) with the site security policy, although this is an area that is often very difficult because of the need to have a specially trained Stratus team who perform all administration and maintenance work. The Stratus systems should not be treated as a separate entity to other processing facilities within the organisation, although where Stratus modules occur as part of a much larger installation involving one or more mainframes they are sometimes perceived as an unimportant part of the complete information systems environment.

The installation planning stage is also used to define user and group naming conventions, and the administrative saving associated with the use of links. An important area for the system administrator to plan is the allocation of users to groups. Generally, only groups should be granted access to files and high level directories because of the concept associated with the default access control list and inherited access rights. Individual users should generally only appear in home directors, or perhaps as named processes if it is necessary to segregate the duties of a group. If named individuals begin to appear on access lists, then the system maintenance effort becomes much greater.

Audit Issues

It is important that only authorised users have privilege granted to them by the systems administrator. The granting of privilege is planned by the systems administrator during the installation planning stage of the system.

Prior to registering any users, the structure of the group directories must be planned by the system administrator and agreed with the site security officer. In many cases this planning is never performed and the system (which may be security critical) is inherently weak from the start. This planning should include the following areas:

- How many groups are required, now and in the future
- Group naming conventions
- Where the group will be located (by disk, by module)
- What access each group will be allocated and to which directories and with which permissions, rights and authorities.

Where new systems are being established, a production test and a development environment may exist. It is frequently the case that a development environment is established on the intended production machine during this phase, as the various terminals are brought on line and the system is configured. Once the system goes live in this situation, the controls associated with the production environment may have inherited a number of characteristics of the development environment. These may include:

- **Write** access for all users to the source libraries of the application system
- **Login** users in the system directory
- Many systems administrators all with privilege
- Development staff as members of group SysAdmin (also with privilege)
- Many users with privilege
- Ability of users to change privilege or default privilege status

Based on the previous comments made on the security exposures associated with **privilege**, the situation in many Stratus sites may appear quite bleak! Another result of the change between environments during initial configuration and implementation may be tight control over the development machine, but limited control in the production environment. This may only be manifest during the early stages of a systems life, and should not exist after any sustained audit or security reviews.

Stratus systems are supplied with the following groups as a default:

●	SysAdmin	Systems administration group
●	system	For system processes
●	Guest	For initial users
●	stratus_service	For the RSN (remote service network) dial in.

Three of these groups have supplied group directories. The exception is **system** which must have *no physical login users* registered to it. It (the system process) is a non_login processes. This is because a user can potentially become a part of the operating system if signing on as a member of the system group. Group directories can be stored on any of the disk packs on a module. If a group directory is stored on a disk other than the pack master, then it must be connected to the master disk by a **link** so that the information contained on this pack master disk can be shared by other disks attached to it. This situation will also apply to the principal master disk used in the networking environment.

An important aspect of installing a Stratus system is the planning of which users, programs and processes will have access to which files and directories. A separate section explains the method of registering users by the command **registration_admin**, and the allocation of access to directories and files. Access control is based on specific permissions (primarily) and inherited default permissions. If the arrangement of a systems directorys and files are incorrectly planned at installation, then the control of the complete system becomes harder for the systems administration team in the future. This applies both the logical access control to specific directories and files, and to the physical administration of individual access rights, where group access would have been appropriate.

Installation planning also requires the integration of the Stratus system(s) with the site security policy. The Stratus systems must not be treated as a separate entity to other processing facilities within the organisation. The installation planning stage is also used to define naming conventions for users and groups, and the administrative saving associated with the use of links. An important area to plan is the allocation of users to groups. Prior to registering any users, the structure of the group directories must be planned as described earlier.

Generally, only groups should be granted access to files and high level directories because of the default access control list concept. Individual users should generally only appear in home directories, or perhaps as named processes if it is necessary to segregate the duties of a group. If named individuals begin to appear on access lists, then the system maintenance effort becomes much greater.

The importance of privilege

It is important that only authorised users have privilege granted by the systems administrator. The granting of privilege is planned by the systems administrator during the installation planning stage of the system.

There are two privileged switches which have to be set within registration_admin.

- **Privilege**

  If the privilege field is set to **YES** during **registration_admin**, then the user with the attribute allocated can login as privileged by issuing the -privileged argument at login, or by cycling the privilege field to **YES** (login **(user_name) -privilege**). The **-privilege** argument can be replaced by using function key F21 cycled to **privilege=yes**.

- **Default Privilege**

  If this field is set to **YES at registration_admin**, then the user concerned is automatically logged in as privileged unless the -no_privilege argument is issued at (login **[user_name] -no_privilege**). This value must be **NO** if the value in the privilege field is **NO**. This is because **default_privilege** will over-ride **privilege**.

Privileged commands are those commands which have a global effect on the system. These include the following important command which are of interest to auditors and security analysts.

Registration_admin

This is used by the security administrator to:

- Register users on the system.
- To grant privilege.
- To change user passwords.

It forms a user-friendly interface which calls VOS commands such as **register_user** and **change_password**. These individual sub commands are commands in their own right and are also defined to VOS as **privileged** commands. It is used to revise the following two files in VOS and to display information to privileged users about the contents of these files.

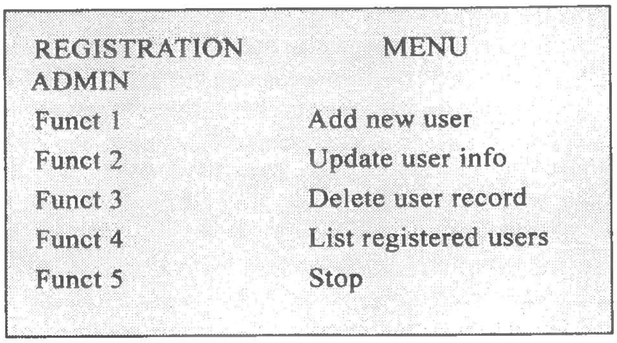
- **user_registration.sysdb**
- **change_password.sysdb**

Registration_admin is a subsystem of VOS. That means that when a privileged user executes the command, the prompt **RA> (registration_admin)** replaces the **ready**: prompt, indicating that the user may now execute commands in that sub-system area only. If the privileged user wishes to issue another VOS command outside of this sub-system, then **RA>** must be exited and the command issued on the VOS command line. The commands available for use in this subsystem from which an authorised user may choose are as follows.

- **add_user**
- **update_user_info**
- **delete_user**
- **list_registered_user**

When an action has been selected from this command menu, the system administrator may return to the above menu and make many alterations to these system files during one execution of **registration_admin**. There is another command within this set called **process_table**. This is used for batch processing of information in the **registration_admin** subsystem. It does not appear on the menu list of the **RA>** subsystem, but can be executed through the **registration_table** argument attached to this command. The command can only be used if the registration files **user_registration.sysdb** and **change_password.sysdb** have already been created by the system administrator. This action is privileged and can be executed by the command **create_user.sysdb**. Before modification to these files occurs by **RA>** subsystem commands, VOS makes additional copies of the registration and password files, naming them as **user_registration.sysdb.backup** and **change_password.sysdb.backup**. If an error is encountered during execution of the **RA>** subsystem, VOS renames the corrupt files as **(name).error** and reverts to the backup files that were previously copied. These now adopt the original file names of the files, before the initial error.

The figure below is a screen display of the **registration_admin** subsystem menu page. This appears on execution of the command **registration_admin**. The alternative is to execute the command **set_registration_info** <F21>.



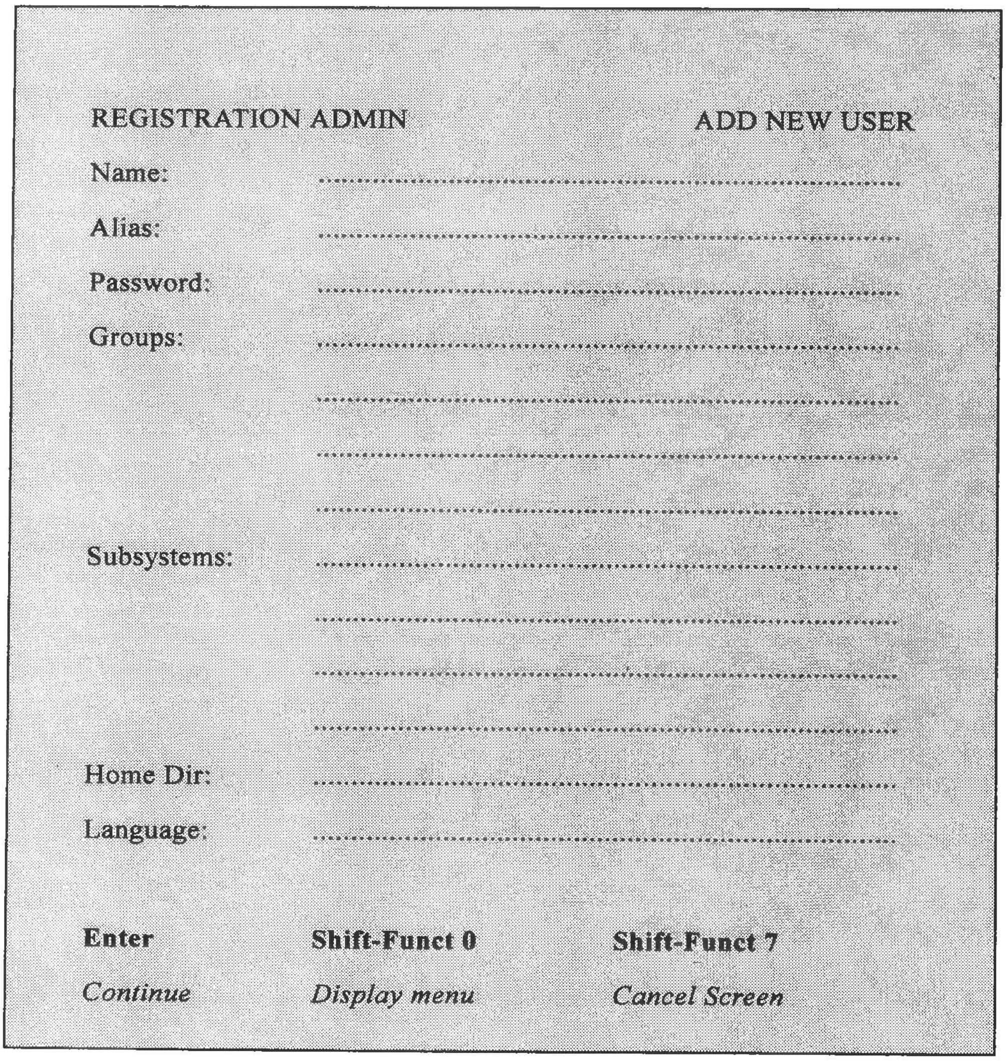
```
REGISTRATION          MENU
ADMIN
Funct 1               Add new user
Funct 2               Update user info
Funct 3               Delete user record
Funct 4               List registered users
Funct 5               Stop
```

Add New User produces a two page form which is completed by the system administrator (or any other privileged user with membership of group .SysAdmin) to register users on the system for the first time. This is distinct from update users, which is a separate command and a separate set of forms.

The first screen (of two) which are used to add new users is illustrated below.

There are a number of points arising from screen one.

- The fields **<name>** and **<group>** are mandatory and must be filled in when completing this form. It is impossible to create a user without a name of some sort.
- Groups need to be created as directories before this form is completed. This requires prior planning of group structures to meet the organisation's current and/ or planned structure.
- Subsystems are run at the login point, and may be used as a control tool for certain users. This may include operators, who can have their access restricted to certain site written menu functions only. This is especially important where operators have to execute privileged commands in order to perform their duties. When a sub system is used, they have access to restricted processes, but can execute them through a menu system only, and so are prevented from accessing the privileged area of VOS.
- At least one group must be completed on this form. Up to five can be added. This can be used to give granularity to specific access groups within an organisation and to manage access rights more effectively. In many cases, the use and membership of groups is not planned in advance and so a system may be built which has sub optimal security designed from the start.



REGISTRATION ADMIN ADD NEW USER

Name: ....

Alias: ....

Password: ....

Groups: ....

....

....

....

Subsystems: ....

....

....

....

Home Dir: ....

Language: ....

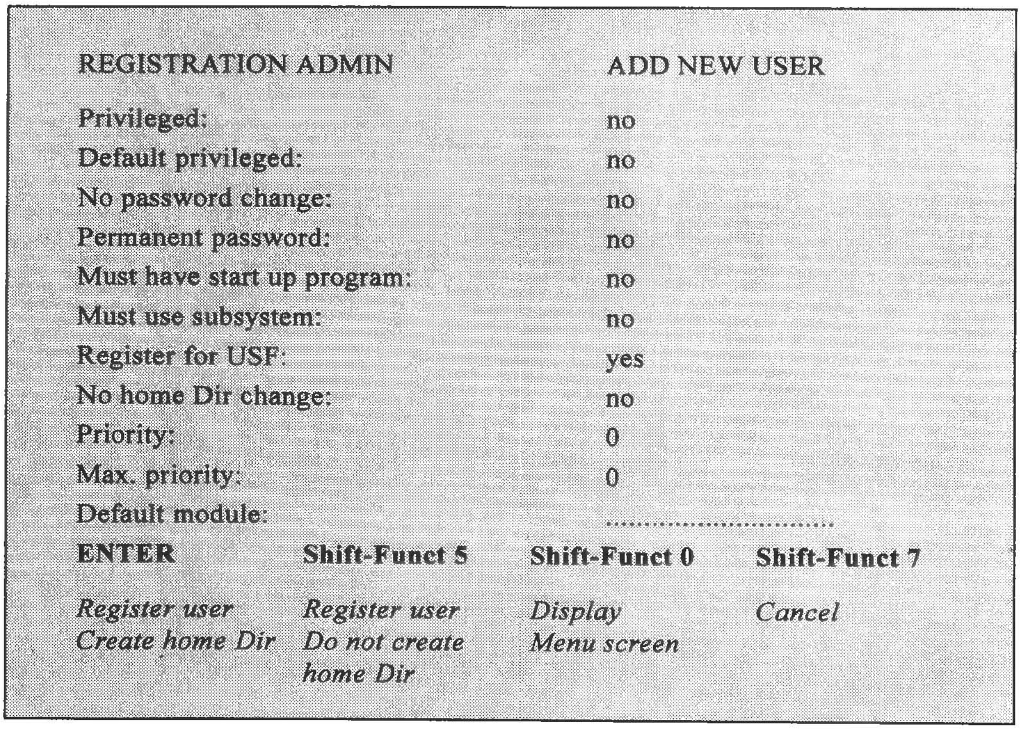
Enter	**Shift-Funct 0**	**Shift-Funct 7**
Continue	*Display menu*	*Cancel Screen*

Screen 1.

The second screen in **registration_admin** is illustrated below.

There are a number of issues which are of audit significance in the registering of new users using **registration_admin**.

- The users name may be changed other than when first registered, but if this is done, then it is necessary to use the command **propagate_access** to update all access lists in all directories and links. This applies especially to systems where a principal master disk is used to contain all start up information for a number of modules.
- Privilege access should be available to members of group .SysAdmin only. (See earlier audit issues box on privilege)
- If **Default Privilege** is set to "yes" and privilege is also "yes" then the user is registered as automatically privileged.
- A **Permanent Password** indicates that the password used will never expire. This may be used for an emergency password for recovery purposes, or if there is only one systems administrator. An audit of **registration_admin** that reveals many permanent passwords may result in an unsatisfactory audit report.
- The **Must Have Start Up Programs** flags the need for a start_up.cm to VOS. If this is set to "yes" then the users home_dir will contain the macro. The operating system will deny access if the required start_up.cm is not present. This can be used to control the access of certain groups or individual users.
- **Must Use Subsystem** indicates that the user must have a subsystem in his/her library path. This subsystem may be used to control the actions of certain classes of user who are not permitted access to the VOS ready prompt. Their access is restricted to a menu which is site defined. If a required sub-system is not present then access will be denied. This flag can be used to control certain groups and individuals by forcing them to use a subsystem.
- **No Home Dir Change** indicates that the user may not change the home_dir of his/her directory path. This does not have a significant audit or security implication.
- **Priority** indicates the operating system priority assigned by VOS to the users processes. The range is from 0-9, with 7-9 being reserved for VOS. Users should not have priority in the VOS range.
- **Maximum Processes** indicate the number of processes between 1 and 235 that a user may execute at one time. 0 = no limit in this case. This can be used to control users who attempt to flood the operating system with process requests in order to obtain execution time. This may have an impact on the management of development staff who wish to achieve a faster execution time for their programs.



REGISTRATION ADMIN	ADD NEW USER
Privileged:	no
Default privileged:	no
No password change:	no
Permanent password:	no
Must have start up program:	no
Must use subsystem:	no
Register for USF:	yes
No home Dir change:	no
Priority:	0
Max. priority:	0
Default module:	....

ENTER	Shift-Funct 5	Shift-Funct 0	Shift-Funct 7
Register user *Create home Dir*	*Register user* *Do not create* *home Dir*	*Display* *Menu screen*	*Cancel*

Screen 2.

- When users are deleted, the entry in the **registration_admin.tin** file is removed, but the home directory is unaffected. The removal of the home_dir can be achieved by moving the contents to another user's directory, removing the directory to tape for backout purposes, and then executing a **delete** command for the home_dir in question. Removal of a home_dir without moving any objects to another directory is not recommended,

> **Audit issues**
>
> The **registration_admin** subsystem updates the **registration_admin.tin** file. This is located in the library path **%VGC#m1_d01>system>configuration** in this example. There is a separate **registration_admin.tin** file for each module, and these may be joined by links for economy and ease of administration. The scope of the audit must be carefully defined to ensure that all of the modules within scope are addressed within the scope of the review. The role of the principal master disk is of special importance in this context.

The following diagram shows how the **registration_admin.tin** file appears on the system when displayed.

The **registration_admin.tin** file contains only the information registered for the user outside of defaults. Therefore if a user is not privileged then no negative entry is recorded on file. An abbreviated version of the above record will therefore exist. The password field is not displayed on this file and is shown for completeness only in this example.

Login_admin

This command will set login parameters for a module, and is one of the methods of implementing site security policy. The command **login_admin** contains the following parameter setting when displayed using key F21:

```
ready: login_admin -form
-------------------login_admin---------------------
    max_logins:
    -module:
    -password:
    -restrict:
    -unrestrict:
    -list_restricted:                  no
    -delay_prelogins:                  yes
    -password_exp_time:                0
    -min_password_len:                 1
    -max_access_attempts:              0
    -max_bad_logins:                   no
    -subproc_logout_message:           no
    -password_grace_time:              0
    -password_format:                  any
    -terminal_as_process_name:         no
```

```
    /*  %VGC#m1_d01>system>configuration>registration_admin.tin

    /   =action                    add
  =person                     Ed_Hutt      /*required*/
  =alias                      eh
  =password                   secret
  =group1                     Audit        /*required*/
  =group2                     SysAdmin
  =home_dir                   %VGC#m1_d01>guest>Ed_Hutt
  =privileged                 1
  =default_priviledged        1
  =no_password_change         0
  =permanant_password         0
  =must_have_start_up         0
  =no_home_dir_change         1
  =create_home_dir            1            /*add new user only*/
  =priority                   5
  =max_priority               6
  =max_procs                  4
  =default_module             m1           /*add new user only*/
```

The following points from the **login_admin** form are of audit significance in **login_admin**.

- **Max_logins** gives the maximum number of users allowed onto a module at any one time. This can be used to control performance by restricting logins to a certain number. This may be important for certain on line systems where an excessive number of accounts can cause service degradation and reduced business impact.

- **Password** gives the option for a **special session password**. This may be used to restrict additional user logins during a session. A second (unknown to the user) password will be requested and this will be known only to the administrator. This command is commonly used where a system has to be shutdown during working hours for a re-boot.

- **-restrict** is an option to specify a user name to be added to the list of those who are restricted from logging into the module directly, but not through a sub-processes. In conjunction with other parts of **registration_admin** this can be used to control operator access to a module or system.

- **Password_exp_time** sets the password expiration time for the module, in days. A value of zero turns off the expiration check so that there is no limit on how long a password remains valid. The initial (default) value for this is zero and should be changed to reflect the site security policy prior to live running.

- **Min_password_len** sets the length for passwords. This is the minimum length permissible unless no_password_change is set in **registration_admin** for a given user. The default value is 1. This should also be changed to reflect the site security policy prior to live running.

- **Max_access_attempts** gives the maximum number of consecutive unsuccessful login attempts that can be made on a terminal. When the maximum number is reached, the Overseer processes disconnects the terminal. A zero value in this field turns off the checking for login violations for each pre-login process. The initial default value is zero. This has obvious audit and security analysis implications and should be reviewed as a part of an implementation audit.

- **Max_bad_logins** is the number of consecutive login failures permitted before a users account is terminated. A non zero value terminates the account after the specified number of consecutive violations for each user account. This has obvious audit and security implications and should be reviewed as a part of an implementation audit.

- **Password_grace_time** is the option to change the number of days a user has, after the passwords expiration point has been exceeded, to change passwords. During the grace period, the user must change their password before a login process can complete.

- **Password_format** is the format which a login user must follow when specifying a new password. The options available are **any**, or **two_words**. If this argument is omitted then the current value is used. The default value supplied is **any**. This is an instrument of site security policy and can be used to control the format of passwords to be used on a module or system. Where links are put in place to connect many modules to a principal master disk, this, and many of the above, arguments can be controlled from a single start_up macro and set of **registration_admin** forms so ensuring consistency of site policy.

The command **login_admin** sets login parameters for a module for the current bootload only. When a module is rebooted, the parameters will revert to the initial values supplied with VOS, unless changes have been recorded in the **module_start_up.cm**.

Summary of default values in login_admin

Max logins	255
Password	-
Restrict	-
Delay prelogins	yes
Password expire time	never
Minimum password length	1 character
Maximum access attempts	no limit
Maximum bad logins	no limit
Sub process logout message	no issued
Password grace time	none
Password format	any
Terminal as login name	login

The details contained in **login_admin** are also contained in the **module_start_up.cm**. This macro contains the start up parameters for the module and is read by VOS during a start processes. This is delivered as a standard with VOS, but may be changed by an installation to meet its local site requirements and procedures. This is done by altering arguments and executing commands as command lines within the macro. The system parameters can be reset interactively and subsequently changed without affecting the details on the **module_start_up.cm**. This obviously has audit implications, as a site security policy that is enforced through the **start_up.cm** but not through interactive command control will be inherently insecure. Uncomment the command string **login_admin** in the **module_start_up.cm** if values other than the default parameter values are to apply on rebooting the module. **Login_admin** must be activated in the **module_start_up.cm** if you have to set password expiration as a command argument.

Site specific commands and parameters can be added at the end of the macro. These will include the following issues:

- Connections to external networks.
- The establishing of processing priorities.
- Mode setting.

Audit issues - audit access

Beware, that the module_start_up.cm details will only apply at start up. The settings can be changed interactively using login admin so on balance it is necessary to review the start up macro and the current login admin settings using the login admin command.

Accounting_admin

The accounting_admin command enables or disables the logging of statistics for a module and specifies the information that is to be collected. Using this command it is also possible to log transactions (although this may degrade system performance). The use of this command lies mostly in recording when particular files or commands have been used. This can be used to record when commands such as **create_new_users** and **analyze_system** have been used. The disadvantage of this approach is that it is used primarily to record the use of privileged commands. However, privileged users can issue a **stop_logging** command and so suppress the use of the logging facility. This would mean that no audit trail of command or file use exists for the period that we will most wish to log and review.

```
Ready: Accounting admin form
...................accounting admin.......................
module:                         %VGC#m1
- disable accounting:           no
- port accounting:              no
- log commands:                 no
- no log proc stats records:    yes
- no log proc user records:     yes
- log transactions              no
```

- When the **-disable_accounting** switch is on, the module will disable accounting on the named module.
- When **-port_accounting** is activated, VOS will record statistics about I/O traffic on each port of the selected module. This will result in a degradation of system performance.
- The argument **-log_commands** will record start and stop records to the log for each command executed. (Command logging)
- **-log_files** forces VOS to record a file close record whenever a file is closed. (File logging)
- The argument **-no_log_proc_stats_records** will record statistics on VOS process calls every time a **s$log_resource_usage** call executes. The **no_log_proc_user_records** records details of every **s$slog_process_record** call.
- VOS writes a transaction log for every start, commit or abort performed. This is transaction logging, and can cause a major degradation in performance.
- The records written using this command are recorded in the system directory and have the suffix of **(date)** to distinguish the day of recording.

Analyze_system

Analyze_system is a privileged command which was originally designed for engineer use only by RSN staff. It has subsequently been included in the technical manuals in later releases of VOS. As a privileged command, its implication is that any user that has **analyze_system** has privilege and so access to commands of a key nature from a security perspective. It is commonly requested by programmers who wish to perform core memory dumps during the programming of new system in order to analyse problems as they occur. It can also be used to review the contents of files and directories that have Null (no access) access list access. In other words, files and directories that have all access barred other than to the systems administrator or other privileged users can be opened through the use of this command. So, even if a site plans and implements a system that restricts the programmer from the use of other privileged commands through the use of **start_up.cm** sub system macros and menus, access to **analyze_system** can still allow that programmer to view restricted data.

The main solution to this issue lies in implementation planning, and where an existing system is being reviewed, in whether a particular set of system users (such as the programming team) need permanent access to this command (and as privileged users) on the production, or the development machine for their work. The allocation of this command to programmers working in the development environment in some cases presents a lower risk than the command's use in the production environment. However, instances have occurred where the development and production environments have been interchanged for contingency and system implementation purposes, and the security net that previously surrounded the initial production system is lost. The use (or abuse!) or **analyze_system** is one which must be resolved by each individual organisation in accordance with its security policy.

Shutdown

This will close a system down. The re-boot of a large module or system can take up to 45 minutes. In critical business systems which must operate during the business day, or in some cases 24 hours a day (such as ATM's, EFTPOS, or dealing systems requiring 24 hour operation), an outage of this nature and magnitude can be fundamental to the business. At the end of the day, organisations have purchased continuous processing systems to combat this risk, and so allowing many staff access to such a key command defeats the purpose of having such an expensive system at all.

Access control

Each directory and file has an access control list attributed to it. This is the mechanism that VOS uses to determine a users access rights to files and directories. Programs (and VOS operating system processes) run as system processes, and are attributed to group **.system**. This is the reason why no login users must be permitted to have membership of the **.system** group. Access to files and directories is defined by entries in **access_control_lists (ACL)** and **default_access_control_lists (DACL)**.

Access lists generically contain two components.

- The users name, comprising of the user_name and group (ie Ed_Hutt.SysAdmin)
- The type of access allowed. (This is different for files and directories)

The user_name and/or group name may be substituted by the wild card character of *. This represents the following:

● User name	=	*	=	Any users
● Group name	=	*	=	Any group

There is a hierarchy of acceptance in the access lists which is applied in all situations. This is a VOS rule which is built into the operating system logic.

name.group	***VOS accepts this first***
***.group**	***VOS accepts this next of all***
name.*	***VOS then accepts this next***
.	***VOS accepts this last***

For example:

An access list in VOS contains the following example entries:

Ian_Whelan. audit	**READ**
Ian_Whelan.*	**WRITE**

The permission associated with **Ian_Whelan.audit**, which is READ, will take precedence over the WRITE permission of **Ian_Whelan.*** (any group). This situation makes use of the facility that a user can be connected to up to five groups. This hierarchy allows the system administrator to plan the security administration of an installation based on group and user naming conventions.

The same user is referred to in both cases, as the **user names** on a module **must be unique**. The access rights associated with **Ian_Whelan.audit, (READ)** takes precedence over the rights of the user with only a .* (dot. wild card) group name. **registration_admin** allows a user to be connected to up to five (and at least one) groups, so this hierarchy of access rights allows the systems administrator to plan security administration within a Stratus site based on the rule shown in the box above.

Directory permissions

The permissions associated with a directory are:

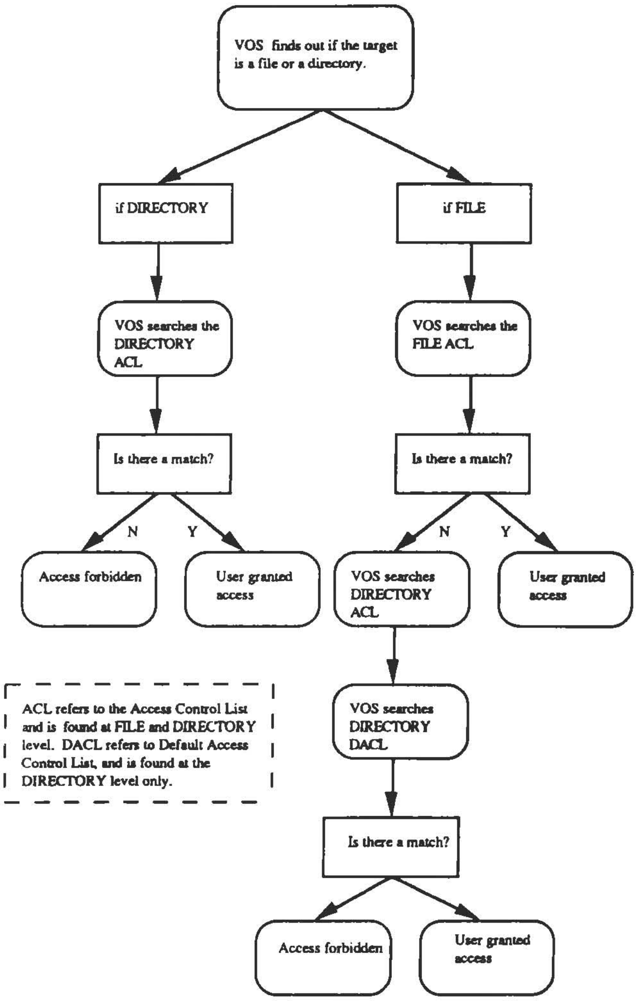
M	**Modify**	Full access to the content of the directory
S	**Status**	User can list the directory contents and see other information, but can make no changes to the contents.
N	**Null**	No acces is permitted by the user.
-	**Unspecified**	No permission is specified. This is the negative case of the access control lists on directories, and can have a material impact on access control.

File permissions

The permissions associated with a file are:

W	Write	The file can be written to and executed by the user
R	read	The file contents can be read by the user only
E	Execute	The file can be executed only
N	Null	No access is granted to the user
-	Unspecified	No access rights are specified. (Comment as for directory).

When new directories are created, the initial contents of its default access list will be the same as that of the parent directory (ie the directory above it in the hierarchy of directories). This is a case of the child directory inheriting the rights of the immediate parent directory



ACL refers to the Access Control List and is found at FILE and DIRECTORY level. DACL refers to Default Access Control List, and is found at the DIRECTORY level only.

It is necessary for an auditor to be able to move between directories, disks, modules and systems in order to effectively review access lists and the activities of the System Administrator, and to assess the implementation planning of a client installation. The default position for any user is their home Directory. A user can move down a directory structure using the command **change_current_directory** (abbreviation **ccd**) followed by the character >. A user can move from dir_new to dir_old using the command **ccd**> or the full command string:

change_current_directory
%system#m1_d01>pack_master>dir_new>dir_old

This will move the user down the directory tree to the position in which he desires to be for audit review purposes. It is possible to move down many layers at once by extending the command. In the example diagram above, to move from pack_master (the home dir of the user) to new_dir, the command **ccd>dir_1>new_dir** is typed on the command line. The alternative is to use the full command:

%system#m1_d01>pack_master>dir_1>new_dir
as before

To move up a directory hierarchy, the less than key "<" is used. This can only be used to move a user back to the position of the home directory. It cannot overrun into directories above the home directory. Many levels can be navigated in the same way as for the move down a hierarchy. For instance, the command "<<" will move up two levels. A quick way to return to the home directory is to use the command **change_current_directory (ccd)**. This will automatically take the user or auditor to their current home_directory if no path is specified.

Site specific reporting and audit trails

VOS allows organisations to write site specific logging and recording routines. This is done by way of:-

- Command macros, using the command macro language.
- Programs, using one of the VOS supported complied languages (such as, PL/1 or COBOL).
- A third party product such as Rose Bud.

These reports may include recording:

- The accesses of the group **.SysAdmin**.
- Accesses by certain specified named individuals.
- Programmer access.

Any VOS command that can be executed

Any VOS command that can be executed individually on the command line, and any logical syntax that can be written in the **.cm** language can be built into a reporting routine.

Audit issue

The control weakness in the use of recording techniques like this is, in common with all other VOS logging methods, that any user with **privilege** can gain access to the files that contain the reports, and execute commands that will change, add to or delete the contents of the file.

Conclusion

Stratus systems are often misunderstood by auditors, and often (rather unfortunately) by those who manage these systems, usually on a part time basis in the "small installations" of this world. Many key issues, such as access to privileged commands and users being attached to system processes, are common resulting in critical weaknesses in security at Stratus/ VOS sites.

Remember

- ☛ **Network risk**
- ☛ **E *.***
- ☛ **s$ commands**
- ☛ **No DR planning**
- ☛ **N *.* access block**
- ☛ ***.SysAdmin**
- ☛ **Overseer as a login user**
- ☛ **Production system transfers**
- ☛ **analyze_system**
- ☛ **Privilege**

Guidelines for Potential Authors

The Journal publishes two types of article: refereed and invited. Refereed articles should be technically oriented, and based on current or future issues related to computer audit, security or control. This type of article will be reviewed by at least one member of the editorial panel (anonymously). If published, it will be identified as a refereed paper.

An invited article need not be technical or overly academic (even Computer Auditors have a sense of humour!). In fact it need not even be 'invited'. Submission without invitation is encouraged and although this may lead to severe sub-editing by the Editor, submission will virtually guarantee publication.

We also invite members to volunteer for book, product and course reviews (anonymously if required).

Why not call Rob Melville at CUBS (071 477 8646) to discuss how you can get your name in print?

YET ANOTHER DISCOUNT

We are pleased to announce that we have negotiated another discount for you.

You can now attend a leading IIR international conference on computer audit and control, see the separate brochure, and save the cost of your corporate membership subscription into the bargain.

To qualify for this discount you must be a paid-up member of the Group and you must enter your CASG membership number, which is on your address label, on the application form. So make sure that you have renewed your subscription for 1993/94.

LETTERS TO THE EDITOR

From City Treasurers Department
The Guildhall
Nottingham

Dear Rob

I have just read the Summer 1993 issue of the CASG Journal and must congratulate you on the methods used to obtain your keynote article from George Mickhail.

Unfortunately my compliments do not extend to the contents of the article. I can well believe that the 5,000 words were written within a week as it is a poorly thought out piece of pretentious drivel.

Journals like yours are presumably intended to throw light on an area in which expertise is limited. In this particular case, rather than illuminating the subject, the issue has become ever more clouded.

May I suggest that you take more care in the selection of your articles if you wish to preserve the reputation of the British Computer Society.

Yours sincerely
J.M. Ahern
for City Treasurer

Editor: *It is always useful to get feedback from our readers, even when the message seems negative. Firstly, to put things into perspective: George Mickhail certainly did not just sit and write 5,000 random words. The research and background for this piece has taken place over several years, and George has presented his work at major conferences of his other professional body (the Operational Research Society). It was the physical presentation which was quick. Secondly, it is entirely up to the reader to judge the quality of a paper: any criticism or compliment is equally valid. But I do take issue with Ahern on two points: it most certainly is not 'my journal' (even though I have the privilege of being its editor). It is the membership's journal. My role as editor is to decide what the content should be, with support and guidance from other committee members. Our editorial policy is to balance practical articles with those that provoke thought and discussion. It will be a sad day when we stop thinking and discussing; please continue to let us have your opinions.*

ADVERTISING IN THE JOURNAL

Reach the top professionals in the field of EDP Audit, Control and Security by advertising in the CASG Journal.

Our advertising policy allows advertising for any security and control related products, services and jobs.

For more information, phone Rob Melville on 071 477 8646.

BOOK REVIEW

The Micro-Security Auditing Guide,
published by Westminster City Council Audit Services £10.

This is a very useful little book, nicely laid out with a pleasantly jargon-free style. Although for the micro power user it is probably a little too basic for a small department or a section just beginning to tackle micro auditing, it is a very worthwhile investment as it would cost at least the price of the book in research time. There is a series of useful working papers included which would assist new users enormously.

A good investment.

THE SWAP SHOP

PROBLEMS AIRED PROBLEMS AIRED PROBLEMS AIRED PROBLEMS AIRED
HELP WANTED HELP WANTED HELP WANTED HELP WANTED HELP WANTED

OUTSOURCING OF I.T.

Chris Harris of Bexley London Borough is trying to assess the impact on the Internal Audit Department, particularly Computer Audit, if the I.T. department is outsourced. Now it just so happens that this is the theme for our next annual conference which is scheduled for May 1994 (make diary note now!), but Chris would like to discuss the issue before then. How about someone doing an article for this journal? If you would like to contact Chris you can do so, during office hours, on 081 303 7777 x3037.

The BCS Security Committee

Within the BCS there are a number of standing Committees reporting to the Professional Board whose task it is to advise Council on matters relating to the policy of the Society. These standing committees should not be confused with Specialist Groups, whose membership is often derived from outside the BCS.

The Security committee is the Society's standing Committee which covers the Computer Security area. A few months ago your chairman had the opportunity, together with the chairman of the Security Specialist Group, to address the Security Committee on area of concern regarding overlap of interests and potential communication problems.

As a result of that meeting, the secretary of the Security Committee, William List, has asked us to publicise the work of the committee more widely. Many of you will no doubt remember that Willie was for many years chairman of CASG and he now acts as our liaison with the Security Committee. Its terms of reference and constitution are provided below.

Terms of reference

The Security Committee is responsible to the Professional Board for:

Monitoring the field of computer security, with the objective of formulating policies which the Society can endorse;

Keeping under review factors such as technical developments and professional attitudes and behaviour which are likely to influence computer security in all its aspects including, physical security, software security, security within communications systems and security involving personnel;

Considering ways of providing systems security against both deliberate and accidental threats, and also providing guidance on monitoring the effectiveness of such measures, and minimising the disruptive effects of events that occur;

Liaising with other Society committees as appropriate, in particular the Data Protection Committee;

Liaising with external bodies as appropriate;

Advising on policies, positions and activities the Society should adopt.

Constitution

Members of the Committee must be Fellows or members (of any grade) of the Society.

The Chairman is appointed by Council, on the recommendation of the Professional Board.

The Vice-Chairman is appointed by Professional Board, on the recommendation of the Committee.

Members are appointed by Professional Board, on the recommendation of the Committee. The members of the committee represent a cross section by age and experience of the varied talents required to provide the Society with proper professional advice.

The Committee is fully aware that it cannot, within its own resources, represent all views in the Society. It has therefore set up a series of teams each led by a committee member to keep up to date in specific areas, identify issues which the Society should be aware of and to do the main work of preparing comments on documents. As a flavour of the work of the Committee the following tasks have been undertaken during the last year:

Comments drafted on: OECD Guidelines; ITSEM and Electronic Signatures;

DTI reports - implementation of the Computer Misuse Act and User requirements for IT Security

Advising the Society's officers on: Computer Pornography; The Society's professional codes of conduct; the necessary steps to be included in the ISM to cover security and appropriate nominations to be the Society's representatives on other bodies.

In addition we are working on a revision to the Guidelines for Good Security Practice, originally written by the Committee in 1990 and the creation of a card providing advice to PC users.

The Committee would welcome assistance from the Specialist Groups in two areas: Individuals who would be willing to participate in the work of our teams, and Identification of matters which Specialist Group members believe the Committee should be addressing.

If any Specialist Group member wishes further information about the Committee and its teams, or wishes to raise matters with the Committee they should contact:

Mr W List
Secretary BCS Security Committee
46 Snakes Lane
Woodford Green
Essex IG8 0DF
Telephone: 081 504 6480

CASG Group Objectives and Constitution

1. NAME

The Group shall be called the Computer Audit Specialist Group (CASG) of the British Computer Society (BCS).

2. OBJECTIVES

a) To encourage research into the audit of information technology and to promote the development of auditing and control techniques to reflect changes in technology, legislation and society.

b) To provide a forum for the development of awareness and competence in information technology audit.

c) To promote the efficient, effective and economical use of audit and control within information technology.

d) To represent the interests of the Computer Audit Specialist Group to other bodies.

e) To be the primary focus for audit and control matters within the BCS.

3. CONSTITUTION

The Computer Audit Specialist Group shall consist of:

a) The Officers, being Chairman, Secretary and Treasurer, all of whom should normally be members of the BCS.

b) Other officers to represent sub-groups or to perform other tasks which may be determined from time to time.

c) Individual fee paying members.

d) Corporate fee paying members, viz Companies, Groups or other organisations wishing to support the purpose of the Computer Audit Specialist Group.

4. ELECTED OFFICERS

a) The officers shall be elected by the Annual General Meeting (AGM) and shall serve from their time of appointment until the end of the AGM following.

b) A vacancy occuring during the term of office may be filled by an appointment by the Management Committee.

c) Other officers may be nominated to fill any other posts created by the Management Committee.

5. MANAGEMENT

a) The affairs of the Group shall be managed (subject to the control of the AGM) by a Management Committee comprising:
1) Elected officers
2) Co-opted officers
3) Elected members

b) Co-Option: The Management Committee may co-op members as required.

c) Meetings: The Management Committee shall meet at least four times in its year of office and frequently enough to properly carry out the business of the Group.

d) Notice: At least 14 days notice of the place, date and time of meeting shall be given to each member of the Management Committee.

e) Quorum: The business of the Management Committee may be transacted by not less than four members.

f) In the absence of the Chairman, the committee shall elect one of its number to take the chair for the meeting.

g) Voting: In determining a question by vote at a Management Meeting a simple majority will be sufficient. The chairman of the meeting shall have a second or casting vote if necessary.

h) Sub-Committees: The Management Committee may appoint at any time sub-committees with appropriate terms of reference, each responsible to the Management Committee and under the Chairmanship of a Management Committee member, to assist in carrying out the business of the Group..

i) Working parties: The Management Committee may set up at any time working parties responsible to the Management Committee which shall appoint a Chairman and provide appropriate terms of reference.

j) Branches: The Management Committee may set up at any time branches responsible to the Management Committee which shall appoint a Branch Chairman and provide appropriate terms of reference.

6. ANNUAL GENERAL MEETING

a) Each year the Group shall hold an AGM in May.

b) Notice: The Secretary shall send notice of the date, time and place of the AGM to all members of the Group at least 28 days before the Meeting.

For this purpose a notice printed in the Programme Card of the Group and complying with the above requirements shall be considered sufficient notice.

c) All members of the Group have the right to attend the AGM, for which there shall be no attendance charge.

d) Agenda: The following items shall be included:
   1) Minutes of the previous AGM
   2) Minutes of any Extraordinary General Meeting held since the previous AGM
   3) Chairman's Report
   4) Statement of Accounts
   5) Proposals for alterations to the Constitution
   6) Proposals for alterations to Fees
   7) Election of Officers
   8) Election of Auditors

e) Nominations: Any member is entitled to nominate a person for any elected office on the Management Committee. Such nominations may be proposed and seconded at the meeting if not previously received by the Secretary.

f) Voting: Every question at an AGM shall be decided by a simple majority of the votes cast. Individual members of the Group each have a single vote. The accredited representative of each corporate member also has a single vote. The chairman shall have a casting vote if necessary.

7. EXTRAORDINARY GENERAL MEETING

a) An Extraordinary General Meeting (EGM) shall be convened on a resolution of the Management Committee or within five weeks of receipt by the Secretary of a requisition signed by no less than twenty members (Corporate members having only a single vote) stating the business to be transacted at the meeting.

b) An EGM shall transact only such business as is specified in the resolutions or requisitions convening it.

8. FINANCE

a) Bank account: In accordance with BCS Guidelines, the Group shall have at least one Account (Account A) at Lloyds Bank, Langhams Place Branch, used for normal running expenses. Other accounts at that branch or other places as approved by the Management Committee, may be used for special events or for investment funds.

b) The Group shall follow the BCS Financial Guidelines as issued from time to time.

c) The financial year shall start on 1st May each year.

d) The Treasurcr is rcsponsiblc to thc BCS for submitting draft budgets, recording ongoing expenditure and capital expenditure separately for each by 30 November in the preceding year.

e) The Treasurer is responsible for making available to the BCS a revenue statement at the end of every financial year (30th April) in respect of the Group's normal operations and special events, this statement to be included in the BCS annual accounts subject to audit by the BCS auditors.

f) All cheques drawn on the Group's bank accounts must be signed by any two of Chairman, Secretary and Treasurer. In the event of such signatories being unavailable, then the Management Committee may appoint a member of the Committee to act as second signatory, together with one of the nominated signatories.

g) The accounts of the groups shall be auditied each year by an auditor elected at the AGM.

h) All income and property of the Group from whatever source derived shall be applied solely to the promotion of the objects of the Group.

9. DISSOLUTION

In the event of the winding up or dissolution of the Group any surplus assets remaining after discharge of liabilities shall automatically rest in the BCS.

In the event of an authorised officer of the Group not being available to conduct the transfer of any assets, then an appropriate officer of the BCS shall have the required power.

10. BRITISH COMPUTER SOCIETY

a) The Group shall be governed by the rules of the BCS as these apply to Specialist Groups of the BCS. Where it is considered that a rule of the Group is in conflict with a BCS rule governing Specialist Group activities, the BCS rule shall apply.

b) The Chairman of the Group must be a Fellow, Member or Associate Member of the BCS.

c) Other elected officers of the Group should normally be members of the BCS.

d) The Chairman, or other elected Committee Member of the Group, is ex officio a member of the BCS Specialist Groups Management Committee.

e) The Group must advise the Chairman of the Specialist Group's Management Committee of the names of any elected officers who are not members of the BCS.

f) All members of the Group's Management Committee shall abide by the Code of Conduct relating to members of the BCS.

g) The Group may use the BCS name to enhance the reputation of their own activities, but must not being the BCS into disrepute.

h) No member of the Group may speak on behalf of the BCS without proper authority from the BCS.

casg

Management Committee

CHAIRMAN	John Mitchell	Little Heath Services	0707 654040
SECRETARY	Raghu Iyer	KPMG Peat Marwick McLintock	071 236 8000
TREASURER	Fred Thomas	Retired Consultant	0371 875457
MEMBERSHIP SECRETARY	Jacqui Race	The Stock Exchange	071 797 3551
PUBLICATIONS	Nigel Smith	NJ Associates	0707 334421
MONTHLY MEETINGS	John Bevan	Audit and Computer Security Services	0992 582439
	Alison Webb	Independent Consultant	0223 461316
CONFERENCE ORGANISER	Paul Howitt	Tesco Stores Ltd	0992 644250 Ext 54320
DISCUSSION GROUPS	Bill Barton Steve Pooley	The Rank Organisation plc Independent Consultant	071 872 6720 0580 891036
MARKETING & PR	Jarlath Bracken	Zurich Insurance	0705 853019
JOURNAL EDITOR	Rob Melville	City University Business School	071 477 8646 SC355@CITY.AC.UK

casg
Computer Audit Specialist Group

The British Computer Society

Membership Application/Renewal

(Renewals are due in August of each year)

PLEASE RETURN TO
Mr A J Thomas
Treasurer BCS CASG

3 Kings Court
The Maltings
Great Dunmow
Essex CM6 1UX

I wish to APPLY FOR / RENEW (delete as appropriate) my membership of the Group in the following category and enclose the appropriate subscription.

CORPORATE MEMBERSHIP (Up to 5 delegates)* * Corporate members may nominate up to 4 additional recipients for direct mailing of the Journal and attendance at our meetings (see over)	£75
INDIVIDUAL MEMBERSHIP (NOT a member of the BCS)	£25
INDIVIDUAL MEMBERSHIP (A member of the BCS) BCS membership number: ____________________	£15
STUDENT MEMBERSHIP (Full-time only and must be supported by a letter from the educational establishment). Educational Establishment: ____________________________	£10

Please circle the appropriate subscription amount and complete the details below.

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE:
(STD Code/Number/Extension)

PROFESSIONAL CATEGORY: (Please circle)

1 = Internal Audit	4 = Academic
2 = External Audit	5 = Full-Time Student
3 = Data Processor	6 = Other (please specify)

SIGNATURE: DATE:

PLEASE MAKE CHEQUES PAYABLE TO "BCS CASG"
AND RETURN WITH THIS FORM TO THE ADDRESS SHOWN ABOVE

ADDITIONAL CORPORATE MEMBERS

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

PROFESSIONAL CATEGORY:
1 = Internal Audit
2 = External Audit
3 = Data Processor
4 = Academic
5 = Full-Time Student
6 = Other (please specify)

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

PROFESSIONAL CATEGORY:
1 = Internal Audit
2 = External Audit
3 = Data Processor
4 = Academic
5 = Full-Time Student
6 = Other (please specify)

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

PROFESSIONAL CATEGORY:
1 = Internal Audit
2 = External Audit
3 = Data Processor
4 = Academic
5 = Full-Time Student
6 = Other (please specify)

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

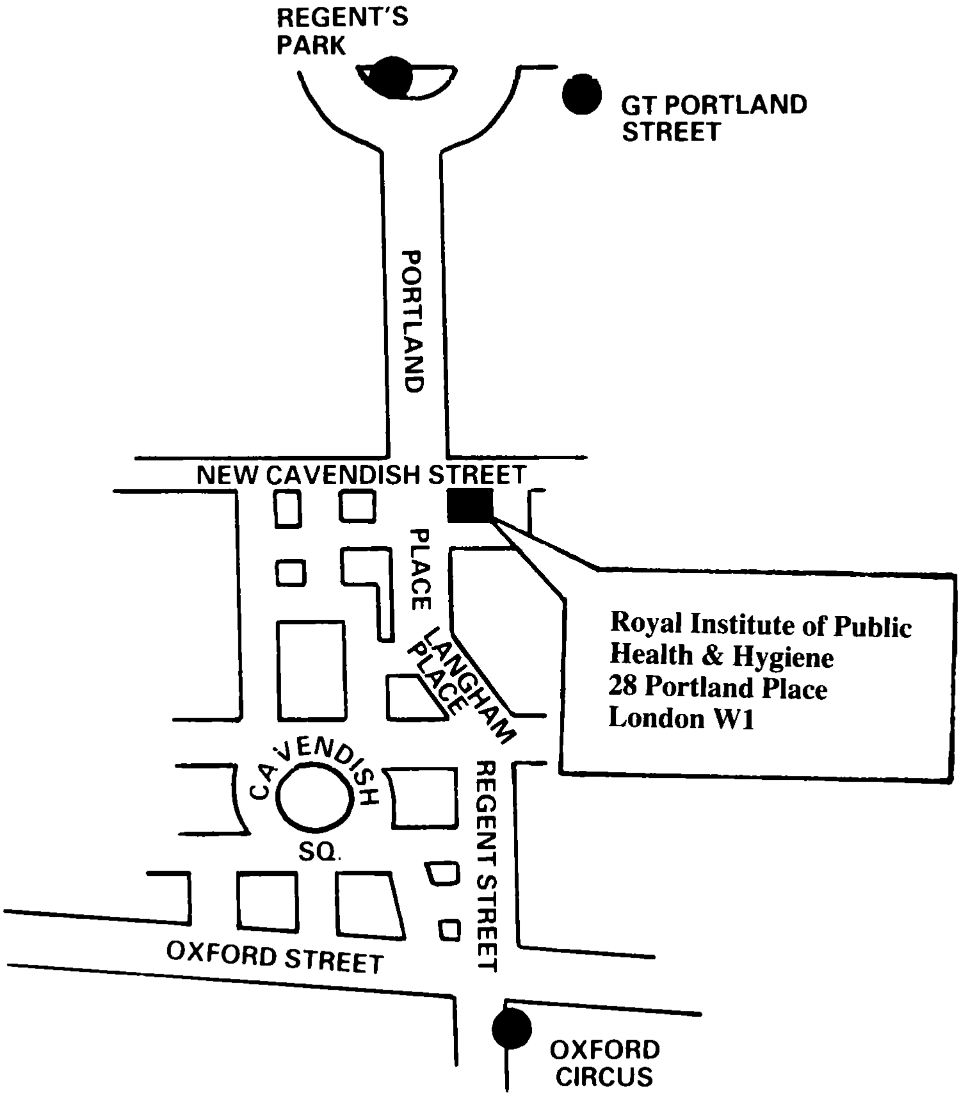
ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

PROFESSIONAL CATEGORY:
1 = Internal Audit
2 = External Audit
3 = Data Processor
4 = Academic
5 = Full-Time Student
6 = Other (please specify

Venue for Members' Meetings



Royal Institute of Public
Health & Hygiene
28 Portland Place
London W1

SUBMISSION DEADLINES

Spring Edition	14th February
Summer Edition	14th May
Autumn Edition	14th August
Winter Edition	14th November