28 September 1999

Site Audit Checklist

Version 5.00

Author: Geoff Halprin <geoff@sysadmin.com.au>

Introduction

This document contains a structured list of controls and mechanisms which one might expect to find in a mature IT organisation.

This list is by no means comprehensive, and is not represented as such. It should, however, prove useful as a guide for evaluating the major aspects of any site with respect to its IT maturity.

This document is provided on an AS IS basis. No warrantees are made, express or implied, etc. You have to leave your brain turned on. Sorry.

All feedback is welcome and actively sought, in order to continue to develop this list towards a vaguely complete, well-ordered, comprehensive and useful site audit Body of Knowledge.

Evaluating A Site

Evaluation should be based on:

- **Effectiveness** (**Results**). Effectiveness deals with the process being relevant and pertinent and results being delivered in a timely, correct, consistent and useable manner.
- **Efficiency**. Efficiency concerns the provision of information through the optimal (most productive and economical) use of resources.
- **Reliability**. Reliability relates to the consistency of results.
- **Compliance**. Compliance with corporate Processes and Standards.
- **Maturity**. Maturity of the organisation with respect to People, Processes and Technology.

Checklist Organisation

Keyboard Facing Areas (Technical Responsibilities)

<table>
<tr><th colspan="5">POLICY</th></tr>
<tr><th>Control</th><th>Organise</th><th>Protect</th><th>Optimise</th><th>Plan</th></tr>
<tr><td>Change Management</td><td>Facilities Management</td><td rowspan="2">Data Security</td><td rowspan="2">Performance Management</td><td rowspan="2">Capacity Planning</td></tr>
<tr><td>Problem Management</td><td>Network Management</td></tr>
<tr><td>Production Management</td><td>Server Management</td><td rowspan="3">Business Continuity Planning</td><td rowspan="3">Process Automation</td><td rowspan="3">Technology Planning</td></tr>
<tr><td rowspan="2">Asset Management</td><td>Software Management</td></tr>
<tr><td>Data Management</td></tr>
<tr><td colspan="5">Service Management</td></tr>
</table>

Domain: Change Management

Sub-Domain: Change Management Process

- **Flexibility and Scope**. Multi-tiered Change Management Procedures covering all types of change: Emergency, Scheduled, Procedurised, and Automated. Delineation between procedure and authority to execute.
- **Quality Assurance**. Peer review of all change requests. Downtime conferences held after unscheduled outages.
- **Risk Management**. Risk analysis performed – both technical risks and business risks. Back-out plans prepared for each change.
- **User Acceptance**. User acceptance forms a component of the Change Process.
- **Documentation**. All relevant documentation is also updated to reflect the changes.

Sub-Domain: Production Control

- **Responsibility**. Clear responsibility for changes to production environment. No unauthorised changes proceed. Well-defined contact list (responsibility matrix) for all applications.
- **Change Control Board**. Downtime coordination, user notification, risk analysis and Change impact review. Conflict escalation and management procedures.
- **Cause and Effect**. Component inter-dependency graphs (Bill of Materials) for identification of affected components. Fixed acceptance / regression tests for each identified component.
- **Impact Matrix**. Definition of affected user communities for each product.
- **Notification**. Proactive Downtime and Change notification. Maintenance activities are well publicised to user community.

Sub-Domain: Certification Process

- **Testing**. Hardware and software changes tested in a simulated production environment (test lab) before final implementation into production.
- **Parallel Run**. Use of parallel operation for major changes
- **Version Control**. Strict version control enforced.

Sub-Domain: Change Support Automation

- Online change control procedures, linked with problem management system.
- Automated propagation of distributed changes. (Enforced consistency of change across distributed network.)
- Proactive change detection.

Sub-Domain: Software Change Management Plans

- Defined development / integration / production baselines for locally maintained source code.
- Standard Operating Environment. Defined standard platform build levels, including O / S and patches. Approval required for deviation from SOE.

- Register of production applications (including locally maintained source), including version and local customisation information, vendor information, maintenance contract information.

Domain: Problem Management

Sub-Domain: Help Desk

- Central point for logging of all support calls. Use of help desk is actively encouraged, directly contacting support staff discouraged, help desk contact information is well advertised.
- Procedures for logging all calls documented and communicated effectively. (Confirmed by statistics on percentage of calls handled by correct procedure.)
- Multiple call logging/tracking mechanisms. Phone, email, automated (from applications).

Sub-Domain: Trouble-Ticketing System

- Central system for recording of call and resolution details.
- System allows users to log calls directly in. System allows for users to obtain status of a call.
- Escalation. System supports automatic escalation.
- Diary function for recording all activity on a call. Tickets are updated as resolution progresses.
- Call history for caller and equipment available.
- Reporting functions. Ability to report on key metrics (See Service Management below).

Sub-Domain: Workflow Management

- Coverage. All trouble-tickets, change requests, service requests and faults are logged into system.
- Effective escalation procedures. Escalation on inactivity and on unassigned calls. Escalation management for after-hours support. Statistics on number of calls escalated.
- System forms basis for support team workflow.

Sub-Domain: Problem Resolution and Causal Analysis

- Problem is "owned to resolution", including all vendor management.
- Root cause analysis to prevent recurrences. Trend analysis on hardware failures. Analysis of faults by platform, application, user, location, etc.
- Database of symptoms and resolutions (SRDB) available to all support staff.

Sub-Domain: Service Management

- Follow-up calls to customers to verify satisfaction
- Regular customer satisfaction surveys.
- Performance statistics gathered from trouble-ticketing system. Calls opened vs. closed each month. Calls re-opened each month. Response time distribution. Staff performance statistics. Trend analysis.
- Performance goals set and publicised. Incentives in place to ensure responsiveness, customer satisfaction and cost effectiveness.

Sub-Domain: Event Management

- **Event Logging**. All significant events are centrally logged in a consistent format.
- **Event Monitoring**. Automated procedure for detecting significant event triggers.
- **Event Notification**. Notification of support personnel upon significant event trigger. Acknowledgment and Escalation procedure for all notifications.

Domain: Production and Operations Management

Sub-Domain: Operations Management

- **Coverage**. Operations facility manned at appropriate times and levels to meet system coverage expectations. Remote operational support where applicable.
- **Training**. Operators trained adequately on all duties.
- **Documentation**. Operational Procedures Manual is accurate, complete and used.
- **Monitoring**. Monitoring of system consoles, network management consoles, etc. Job and Print Queue monitoring. Event management functions for production processing during all periods of scheduled uptime.
- **Duty List**. Defined operator duty list. Audit trails. Exception reporting. Automated notification of incomplete/failed duties.
- **Batch Processing**. Defined list of batch jobs to be run, inputs, outputs, exception conditions. Provision for ad-hoc batch processing.
- **Report Distribution**. Print run and report distribution and security.
- **Storage Management**. Management of various media, such as backup media, via documented procedures.

Sub-Domain: Production Control

- **Production Control**. Scheduling of batch jobs.

Domain: Asset Management

Sub-Domain: Asset Register

- **Identification**. Physical identification of each asset.
- **Asset Register**. Revision levels, maintenance agreement details, lease details, company division in possession of asset (charge-back), asset location.
- **Hardware Management**. Physical location map for assets.
- **Software Management**. License restrictions. Original media labelled. Stored centrally.

Sub-Domain: Asset Tracking

- **Asset Register**. Accurate and current inventory register. Regular asset verification. Automated tools for inventory verification.
- **Hardware Management**. Regular physical stock takes. Network probes.
- **Software Management**. Location of master media. Is it labelled? Automated inventory scans. License conformance verification.

Sub-Domain: Asset Procurement and Management Procedures

- Process for selection and purchase of new assets.
- Procedures for requesting purchase of new assets, adding/moving desktop, adding/moving major host and decommissioning hardware.

Sub-Domain: Hardware Installation and Maintenance

- Appropriate staff, contractors or maintenance contract for installation of equipment.

Sub-Domain: Resource Accounting

- Charge-back model promoting efficient use of resources.
- Model accurately maps resource usage to responsible business unit.
- Realistic depreciation model that reflects the company's investment model and technology end-of-life expectations.

Domain: Facilities Management

Sub-Domain: Data Centre Management

- **Equipment Labelling**. All equipment adequately identified. All data points labelled. All cables numbered at both ends.
- **Environmental Controls**. Power supply, UPS, power distribution. Air conditioning. Fire control. Environmental failure monitoring and alerting.
- **Physical Security**. Key assets in physically secure location. Security system is appropriate.
- **Computer Environment**. Racks, cabling, false flooring.
- **Planning**. Room for expansion. Physical room, network, power.

Sub-Domain: Equipment Management

- **Maintenance**. Maintenance Contracts for all core devices. Appropriate for level of service being offered to customers.
- **Console Management**. Console management in place. Restricted (privileged) network access to consoles. Fall-back access mechanism.

Sub-Domain: System Documentation

- **Document Management**. Version control, format and style, identification, location.
- **Styles**. Cookbook, users guide, and reference styles.
- **Physical Maps**. Data centre layout, data centre wiring, LAN/WAN topology maps, building wiring maps, telephone termination records.
- **Logical Maps**. Host responsibilities map, IP address allocation register.
- **Key Support Documentation**. SRM (Site Reference), APM (Administrative Procedures), EPM (Emergency Procedures), SAG (System Administration Guide).
- **Access and Use**. Location of system documentation well publicised. Documents are used. Online procedures and documentation.

Domain: Network Management

Sub-Domain: Network Strategy

- Enterprise wide network strategy documented and well understood.
- Network has been designed to meet needs of present environment and planned growth patterns.
- Network design linked to business requirements.
- Network design reviewed regularly for continued applicability.

Sub-Domain: Network Management

- Network Management Console. Platform implemented, configured appropriately, well understood and used.
- Proactive monitoring of the network availability, including all key network devices and links.
- NMC provides pro-active alerts of network outages or failure of other key performance metrics. Regular reports on network performance.
- All network devices use common protocol (e.g. SNMP) to report faults.

Sub-Domain: Network Operations

- Clearly defined procedures for the allocation and recovery of network addresses. Accurate network register maintained.
- Clearly defined procedures for addition, removal and movement of network devices.
- Proactive tool to scan network for exceptions: duplicate addresses, illegal addresses.
- Tools for identifying and isolating faults. Tools well understood. Staff appropriately trained.

Sub-Domain: Network Gateways

- Documented policy for the implementation of network gateways. Policy includes security requirements for gateway implementation.
- Documented policy covering dial-in, dial-out and other remote access facilities. Central modem banks operated for dial-in and dial-out services as required.
- Procedures for severing gateways and dial-in connections in the case of suspected security incidents.

Sub-Domain: Network Security

- Mechanisms in place to protect enterprise network from exterior networks. (Firewalls).
- Intrusion Detection System (IDS) in place to detect illegal traffic on internal network segments. Mechanisms for monitoring for illegally connected gateways / modems.
- Regular network security audits performed.

Domain: Server Management

Sub-Domain: Host Management Standards

- Account Management Standards: Account naming standards, Home directory location standards.
- File and Directory Standards: Corporate directory structure. File naming conventions. File storage policy.

Sub-Domain: Host Installation and Configuration Standards.

- Host naming standards.
- Operating system installation profiles. Filesystem layout standards, filesystem naming standards (virtual partitions), centralised configuration baseline (jumpstart, ignite, rdist, stow).
- Local software environment (/opt/local) baseline.
- Desktop installation profiles.
- Product installation and configuration standards.

Sub-Domain: Centralised Configuration Management

- Central naming services. DNS, NIS, NIS+, etc.
- Centralised host configuration management mechanism. DHCP, BOOTP, RARP.
- Centralised host configuration file management (hosts, ethers, netmasks, etc). Synchronisation mechanism for host configuration files (rdist, sdist, rsync).
- Central host configuration baseline.

Sub-Domain: Centralised Host Administration

- Use of a Host Configuration Management Host to control the configuration of other hosts. (CAB, rdist, stow)
- Central log host where all system logs are maintained and reviewed.

Sub-Domain: Automated Housekeeping

- Regular house cleaning. Well-defined daily, weekly and monthly duties for system accounts.
- Duties include: Log file roll-over and archive management, and system backups.
- Duties maintained in revision controlled script, rather than ad-hoc list of **cron** (or similar) entries.
- Centralised, uniform master housekeeping scripts, configuration driven.

Sub-Domain: Automated Administration

- Key repetitive functions automated for increased consistency and reduced overhead: Account management, password management, applications startup/shutdown.
- Strategy of continuing review and automation of key administrative processes.

Sub-Domain: Information Flow Management

- Central administration aliases. All tools direct results and errors to central aliases, not directly to people.
- Key aliases defined: root-adm, backups-adm, webmaster, ftpmaster, hostmaster, newsmaster, postmaster, mailer-daemon.
- From operations team. Distribution aliases, motd, etc.

Sub-Domain: Continuing Review of Practices

- Regular review of overall network and system architecture for continued application to environment.
- Controlled Improvement Programmes instituted to improve quality of service and reduce management overheads.

Domain: Software Management

Sub-Domain: Software Distribution and Management

- Defined policy for software location, distribution and replication, and software currency.
- Automated tools to distribute software to relevant servers / desktops across company.
- Mechanism for interrogation of servers / desktops to verify inventory against central register.

Sub-Domain: Production Acceptance Process

- Documented process for moving new applications (or upgrades) into production environment.
- Process includes use of test lab to build profile and study sociability of product. Process includes documenting deployment strategy for migration into distributed production environment.
- Process includes customer acceptance testing, and definition of regression test suite for use by operations (change management). Process relates directly to SLA.
- Process applied to all products, including internally developed and public domain software.
- Process includes definition of installation and configuration steps for product.

Sub-Domain: Application/Service Monitoring

- Metrics defined and tools in place for application availability and load monitoring, and collection of application vital statistics.
- Regular reporting of application availability and performance.
- Active (automated) notification of application failures. Interface to problem management system.
- Use of proxy agents to provide a single consistent mechanism for gathering statistics (e.g. SNMP gateway).

Sub-Domain: Application Distribution and Synchronisation

- **Software Distribution**. Mechanisms: NFS, Automounter, rdist / sdist / rsync, etc.
- **Software Replication**. Some candidates: Man pages, answerbook, local (core) software.
- **Core Network Services**: DNS, Time servers (NTP), Mail, News, License, Internet Proxies.
- **Workload Audit**. Regular review of application, service and data distribution for continued applicability to environment. Migration of services / data where appropriate. Redundancy of services / data where appropriate.

Sub-Domain: License Management

- Register of software licenses and license restrictions maintained and accurate. All original license certificates filed in central repository, and labelled appropriately.
- Licenses centralised to a few core license servers.
- Use of redundant license servers to ensure license availability.

Domain: Data Management

Sub-Domain: Data Management Policy

- Clear, enforced policy, covering: scheduling, reporting, logs, media standards, media volume naming, labelling and storage, media rotation and retention schedules, offsite backups, and filesystem coverage.
- Responsibilities are well-defined.
- Data archiving policy.

Sub-Domain: Backup and Restore

- **Scope and Schedule**. Regular backups of all business data. Mechanism (method, transport, scheduler) is appropriate.
- **Media Verification**. Random restores performed regularly to verify media. Duplication of media where appropriate.
- **Backup Media**. Consistency of media types. Consolidation onto one or few different media types.
- **Volume Management**. Electronic tape labels, naming conventions, retention/rotation schedules enforced.
- **Logs**. Logs detailing age and number of uses of each tape. Tape rotation and retention enforced.
- **Backup Failures**. Clearly defined procedures for dealing with backup failures.
- **Off-site Backups**. Off-site backups implemented and tested.
- **Service Guarantee**. Tested and benchmarked restore times. Worst-case restore time within SLA.
- **Coverage Verification**. Proactive (automated) filesystem coverage checks.

Sub-Domain: Storage Management

- Data management strategy defined. RAID, HSM, Offline storage.

Sub-Domain: Data Availability

- **Formal Definition**. All application availability requirements defined. Definition includes: type, size, growth expectations, security ratings, availability requirements.
- **Data Location**. Data is located on appropriate resources. Common data replication across WAN.
- **Availability Management**. RAID and HA mechanisms implemented where appropriate.

Sub-Domain: Database Management

- All database schemas defined in well-known location to assist with table and index rebuilds. Backup and restore instructions for each application.
- Physical and logical database structure clearly defined.
- Regular data exports.
- Tools for monitoring status, growth, performance.

Domain: Data Security

Note: This section looks at the organisation's maturity with respect to managing data security – not the maturity of those security practices. That is an entire Body Of Knowledge in its own right.

Sub-Domain: Security Policy and Architecture

- Well communicated information security policy. Policy based upon RFC1244, AS-4444 or other standard.
- User Responsibilities Acceptance Form. Completed by all staff and contractors.
- Formal security stance, model and architecture defined.

Sub-Domain: Security Organisation

- Management Information Security Forum exists to provide high level direction.
- Information Security Coordination. Security information is communicated across functional units. Cooperation between organisations.
- Allocation of Information Security Responsibilities. Appropriate resourcing of those responsibilities.

Sub-Domain: Security Management

- Process for receiving and evaluating (in a timely manner) all vendor and *CERT advisories for applicability.
- Process for reporting and investigating (in a timely manner) suspected security breaches.
- Procedure for the regular changing of all passwords for privileged access accounts.
- Clear responsibility and adequate resources allocated to Security Management processes

Sub-Domain: Security Monitoring

- Security logs reviewed on a daily basis (or better).
- Automated alerts tripped by defined events.
- Audit trails: privileged functions, external access.

Sub-Domain: Security Mechanisms

- Regularly used security methodologies and tools (access control, authentication, integrity checking software, encryption, gateways, proxies, firewalls, IDS).
- Virus control systems are in place, usage is enforced, and tools are kept up-to-date.
- Methodologies and tools are regularly reviewed to ensure continued applicability and reflect current industry practices.

Sub-Domain: Security Audits

- Independent Review of Information Security. Process for regular review of security architecture, controls and mechanisms for continued applicability (security audits).
- Audit includes: physical, network, host and data security.

Sub-Domain: Management Reporting

- Incident investigation reports, exposure assessments, action plans.

Domain: Business Continuity Planning

Sub-Domain: Risk Assessment and Contingency Planning Standards

- **Risk Assessment Standards**. Identification and prioritisation of critical business processes and systems. Determination of the potential impact of various types of disaster on business activities.
- **Contingency Planning Standards**:
  a. What is the objective of the contingency?
  b. What resources will be required?
  c. How long can the contingency sustain service?
  d. What are the criteria for invoking this contingency?
  e. What are the procedures for invoking this contingency?
  f. What are the procedures for operating in contingency mode?
  g. What are the criteria for returning to normal operating mode?
  h. What are the procedures for returning to normal operating mode?
  i. What are the procedures for recovering lost or damaged data?
  j. What are the roles and responsibilities for this contingency plan?

Sub-Domain: Business Continuity Planning Process

- BCP Process. There should be a managed process in place for developing and maintaining BCPs across the organisation.
- BCP Forum. A forum, staffed with appropriate resources, exists to define and review BCPs.
- BCP Communication. The BCPs are effectively communicated to the organisation.
- BCP Testing. Each BCP is tested. A testing schedule exists for the regular testing of each BCP.
- BCP Review. Each BCP is reviewed and updated regularly.

Domain: Performance Management and Capacity Planning

Sub-Domain: Performance Monitoring

- **Performance Monitoring**. Monitoring and recording of key processing metrics.
- **Performance Analysis**. Regular analysis of performance metrics to identify bottlenecks. Rectify or recommend remedies.
- **Process Interlock**. Capacity Planning Interlock

Sub-Domain: Workload Distribution and Balancing

- Application workload and Host workload reviewed on regular basis. Services migrated between hosts as required.

Sub-Domain: Resource Utilisation and Capacity Planning Function

- **Trend Analysis**. Function exists and is adequately resourced.
- **Trend Reporting**. Capacity utilisation reports generated and presented to management regularly.

Domain: Process Automation

- **Candidate Identification**. Regular review of change requests and help desk tickets to identify candidate procedures for automation.
- **Documentation**. All process automation scripts are documented.
- **Audit Trails**. All scripts keep appropriate log information for audit and problem investigation purposes.
- **Coding Standards**. Standards exist covering: scripting language selection, coding standards, configuration information (format and location), deployment policy, audit information (format and location).

Domain: Technology Planning

- Regular Review of technology and how it may be applicable to the organisation.
- Participation in industry forums to gather information about practical implications of technology.
-

Domain: Service Management

- Service Definition. SLA, security (Confidentiality, Integrity, Availability).
- Service Activation. Procurement, analysis, deployment.
- Service Assurance. Defined regression / acceptance test for each service / product.
- Service Monitoring. Metrics, SLO.
- Service Support. Appropriate resources available to support service.
- Service Review.

Example services:

Printing services, Fileservers, database servers, DNS.

Domain: IT Organisation

Sub-Domain: Computing Policy

- Policy exists, is publicised, and consulted.
- Policy covers necessary topics.
- Acceptable usage statement. User responsibilities.
- Staff educated on policy.
- Computing Resources Access Request Form. Ensures staff have read and agreed to comply with computing policies.

Sub-Domain: IT Organisation and Staff Management

- **Structure**. Effective organisational structure. Clear, written and well understood internal charters and interfaces between functional areas.
- **Organisational Capability**. Appropriate expertise, job mix, job profiles. Organisational performance benchmarking.
- **Organisational Atmosphere**. High morale, low staff turnover, motivated staff, team atmosphere.
- **Staff Management and Development**. Adequate staffing levels, accurate job descriptions, appropriate staff training and regular appraisals, staff incentives. Staff development program exists and is appropriate.

Sub-Domain: Organisation Interlocks

- **HR Organisation Interlocks**. Automatic notification of staff commencement, termination, suspension / leave, and position changes.

Sub-Domain: Customer Management

- **Clearly Defined Deliverables** (services, products) – Service Level Agreements. Tiered SLA. Reflects reality, provides for extensions, incentives for service improvements.
- **Clearly Defined Expectations** (Service Level Objectives): availability, performance, responsiveness, problem resolution, support hours. Appropriate metrics to measure performance against SLOs.
- **Resource Accounting/Charge-back**. Central facilities and desktop services.
- **Responsibility Matrix**. Clearly defined responsibilities. Escalation procedures.
- **User Education**. Training programmes.
- **User Communication**. Newsletters, newsgroups, motd, email, Web site.
- **Customer Satisfaction**. Ad-hoc support call follow-up. Regular surveys.

Sub-Domain: Vendor Management

- **Contract Details Repository**. Repository maintained, linked to Asset Register.
- **Vendor Performance**. Logs of support history, metrics for evaluating performance, performance reviews.
- **Access Security**. Sign-in sheets, controlled remote access. Login session audit trails.