HOW TO IMPROVE YOUR IT

RUSSELL FUTCHER

How to Improve your IT

Table of Contents

Part 1 - Introduction

Background

One of the outcomes of a 45-year career as an IT Management Consultant and trouble-shooter, is that I gained a hard-earned reputation for being able to dramatically improve IT department performance across the board.

The bulk of my consulting assignments (averaging 6 to 12 months each) involved taking on an IT management position to bring about performance improvement. Performance I define as being made up of: - Organization, People, Metrics, Process, Work Management, Service, Cost-effectiveness, Customer and Staff satisfaction.

My work experience has provided me with a unique perspective on IT as a result of having managed every IT Team. That is, I have been a CIO, IT Manager, Infrastructure Manager, Applications Development Manager, Technical Services Manager, Service Delivery Manager, Service Desk Manager, Data Centre Manager, Architecture Manager, Project Office Manager, as well as Database and Networking Manager. Many of these positions I have held more than once. I have managed 50 staff and 1000 staff. I have also been a Programmer and a Systems Analyst, starting my career with the build of an MVS Mainframe Data Centre. I contribute my success to this breadth and depth of experience.

Performance Housekeeping

The bottom line is that this background allowed me to form a unique appreciation and understanding of how an IT department works and how to get it to work at its best. It also allowed me to determine what essential Performance Housekeeping activities are required to obtain maximum performance within each IT Team and achieve the following benefits:

- Better IT Budget management.
- Business partnerships characterised as joint ventures.
- How to make IT entirely business focussed.
- Understanding the essential elements that make IT work.
- The four most problematic areas.
- How to maximize resources.
- How to substantially improve staff morale and job satisfaction levels.
- Best practices for Managed Services

Performance Housekeeping is conducted at an IT Team level with each Team having specific activities to do. The objectives of Performance Housekeeping are:

- IT Team specific performance improvements and introduction of performance metrics.
- To migrate to the agreed Best Practice IT standard.
- To subject all work to Process.
- To produce all work consistently and with higher quality.
- To handle an increasing workload with the capacity to do more with less.
- Identification and resolution of activities that are categorised as wilful blindness. (adverse effects that are known about but are hidden from management. e.g., data corruption, report errors, back-up failures, invisible and redundant servers, theft, hacking.)
- Automation of recurrent manual activities.
- Workload Management improvements with an emphasis on inter-team workflows.
- Clearing out of work backlogs.
- Reduction of technical risk.
- Identification of hardware assets that require risk mitigation.
- Removal of redundant hardware, systems software, utilities and tools.

Best Practice IT Standards and Transformational Management model

There have also been two other outcomes from my work, the first of these has been the development of the Best Practice IT Standards and the second, a Transformational IT Management model. The development of the Best Practice IT Standards came about as a result of taking note of what worked best in all of the IT departments, I worked in. They became part of my Change blueprint for addressing operational performance issues and bringing about improvements. The Transformational IT Management model came about as a result of reorganizing IT departments and improving Team effectiveness.

After 45 years of IT practice, I can say with absolute certainty that IT is not that difficult to manage and that every IT department needs Housekeeping every five years. IT managers have problems because they either don't understand the basics or do not pay attention to them. CIOs on the other hand have problems because they are distracted by the amount of IT spend, poor customer satisfaction levels and poor operational standards, these distractions keep them away from working on business strategic needs.

It's really quite simple, get the basics right, do your housekeeping and everything else will, as a rule, fall nicely into place.

Part 2 - Performance Housekeeping

IT Entropy

Over time all IT departments suffer from a form of entropy in their performance capability. Progressively they become more complex, run a much higher risk of errors, suffer a decline in technical performance, they lose their IT memory and incur increasing operating costs, all as a result of doing nothing in particular other than running the day to day.

The principle causes of this IT entropy are: (in order of greatest impact)

- The rapid pace of business change where pressure on IT to keep up often means production implementations are not always completed to IT's satisfaction or to a professional standard. Final implementations could be flagged as 'at risk'.
- Introduction of new technologies.
- Increasingly complex systems and applications development environments.
- Increased security requirements.
- Shorter development timeframes with an increased frequency of releases.
- Loss of knowledgeable staff and IT memory.
- Decreasing Workload Management efficiency and poorly defined inter-team workflows.
- Ad-hoc, poorly documented or not fully implemented processes.
- Increased systems management requirements resulting from a swath of new systems software, additional utilities and toolsets, new equipment additions and poorly managed retirements.
- An ever-increasing demand for staff to acquire new skills and knowledge often without training.
- Diminished sense of staff personal accountabilities.
- Management of ageing legacy equipment, systems and applications.

Left unchecked, four key outcomes become deeply rooted into the IT departments operation

- Costs become unmanageable and almost impossible to wind back.
- The risk of loss of systems availability substantially increases, with little chance to mitigate.
- Service Delivery and Customer Satisfaction decline with little opportunity to redress.
- Staff morale suffers and risk of loss of key staff increases.

Conducting a Performance Housekeeping exercise every five years is enough to reduce the risks associated with each of these outcomes.

Performance Housekeeping

Regular housekeeping keeps these outcomes from taking root and from escalating, but I am yet to see an IT department that does any regular housekeeping of any type. I found that to improve overall IT performance, there are a set of basic housekeeping activities that need to be completed for each IT Team. Performance Housekeeping is the name I use to represent all of the IT Teams housekeeping activities.

Performance Housekeeping objectives

Performance Housekeeping within each IT Team is focussed on achieving the following objectives, which are clearly defined and measured.

1. IT team specific performance improvements and introduction of performance metrics.
2. To migrate to the agreed Best Practice IT standards.
3. To subject all work to Process.
4. To produce all work consistently with higher quality.
5. To handle an increasing workload with the capacity to do more with less.
6. Identification and resolution of activities that are categorised as wilful blindness. (adverse effects that are known about but are hidden from management. e.g., data corruption, report errors, back-up failures, invisible and redundant servers, theft, hacking.)
7. Automation of recurrent manual activities.
8. Workload Management improvements with an emphasis on inter-team workflows.
9. Clearing out of work backlogs.
10. Reduction of technical risk.
11. Identification of hardware assets that require risk mitigation.
12. Removal of redundant hardware, applications software, systems software, utilities and tools.

I have used this approach many times across a large number of IT departments - I can tell you that it absolutely works. As an IT manager, I have always had very high standards, this management approach does not suit everyone, I have met many people who accept far less than I do, my take on that being that their IT department performance and in particular Service Delivery reflected this.

Part 3 - A better IT Management Model
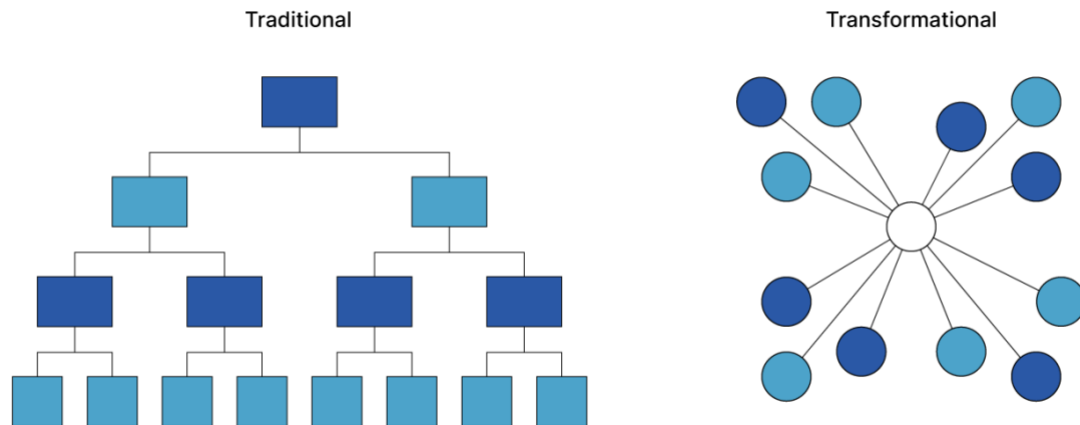
The Traditional IT Management model

The majority of IT departments are managed following the Traditional management model, that is, a hierarchical, command and control structure first introduced during the Industrial Revolution and still in use today with most organizations still employing this model.

For IT, this Traditional management model looks something like this:
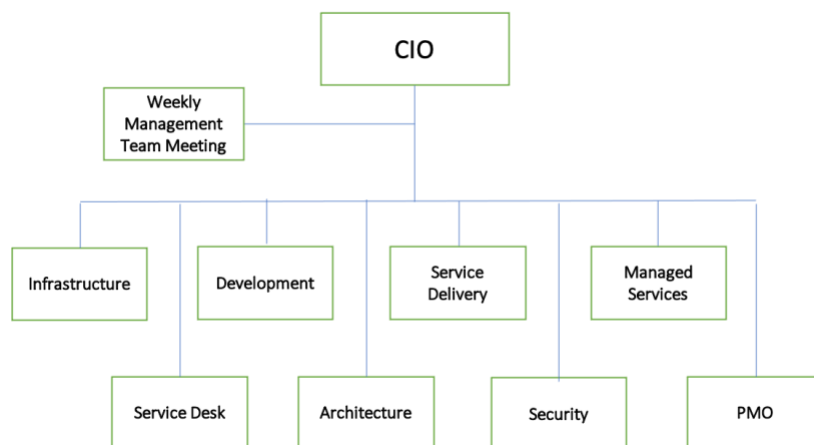
This is a standard hierarchal model shown as an Organization Chart view, with the CIO as the department head and an Executive Management team made up of IT Managers each of whom manages a specific IT Function (an IT Function is an IT Team).

This model has some significant failings:
1. This Traditional, hierarchal way of managing has not changed since the beginning of information processing in the 1960s, this approach also strongly influences the management practices in use, most of which are now outdated.
2. This model tends to be focused on technology first and customers second approach with either little or no consideration of staff needs.
3. It traps the CIO into focussing too much on operational performance and issues as against just focussing on business/strategic needs.
4. The model's biggest problem is that communications between people and teams follow the hierarchical lines of the model, this then supports IT Functions as silos.
5. It perpetuates the traditional management style, which is a command-and-control, rigid, not people-oriented and is outdated.

6. It fails to adequately provide the IT Management Executive with a macro view of IT performance.
7. It reinforces that IT Managers are only responsible for their own IT Function, that is, they are blinkered, siloed, having only a micro view of departmental performance until forced to look outside of their operational boundaries.
8. IT team activities tend to be chaotic under this model.
9. Staff and Customer Satisfaction levels are predominantly low.
10. It does not support tight IT Functional integration, the single most important thing that makes IT work.
11. Performance metrics tend not to be in use due to the siloed nature of the IT Functions.

A better IT Management model

The model I prefer and the one I have always implemented is an IT Performance Management model. I always moved quickly to implement this model which is a hybrid of the older Traditional and newer Transformational - management models. The model looks like this:
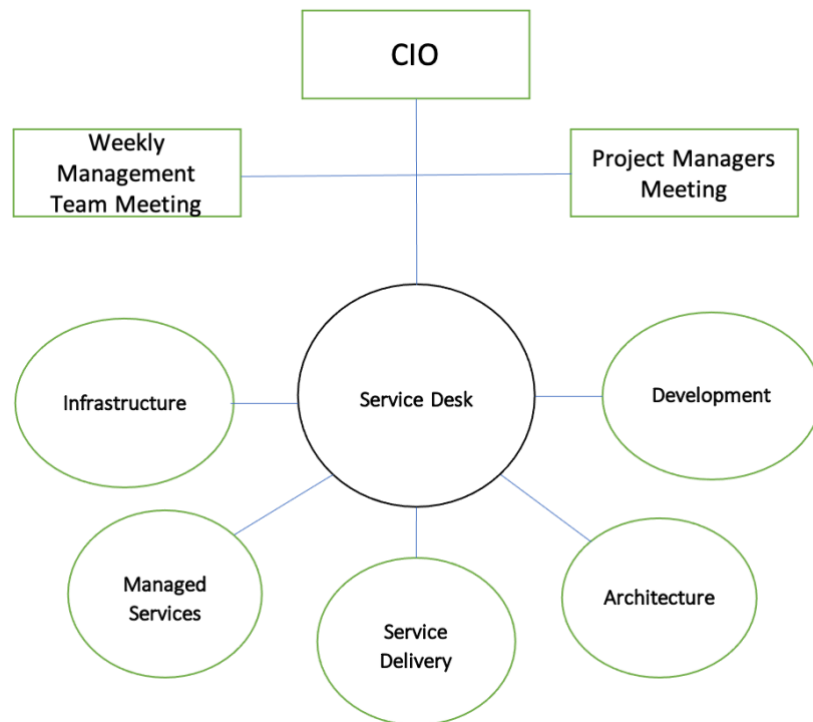

It is still a hierarchal model but for the purposes of reporting lines only. All that has changed is the perspective or view of the IT department. The CIO is still the department head with an Executive Management team made up of the IT Managers. The model is designed to emphasize performance management at a macro or whole department level. It is also designed to improve communications, create a shared Executive Management responsibility for all IT Functions, help implement Transformational management practices, help with High-Performance Team development and finally to fully separate the management of projects away from operational activities.

This model has some significant benefits

1. The Performance Management focus is on customers first, staff second and technology third. It frees up the CIO to concentrate on business and strategic needs. This model is designed to produce performance and operational excellence.
2. The Key Performance metrics are Customer satisfaction, Staff satisfaction, Job completion rates, Failure rates, Quality, Service Delivery and Process adherence.

3. It provides the IT Executive Team with a macro view of IT performance and forces all IT Managers to share in the responsibility for delivering departmental performance outcomes.
4. Under this model, each IT Manager is responsible for all IT Functions, that is, management responsibility is equally shared.
5. New communication lines are opened at inter-team touchpoints which improves integration. (The single most important thing that makes IT work.)
6. The value and quality of information exchanged at these touchpoints is dramatically improved and silos are broken down.
7. IT teams are highly organized under this model and performance is measured.
8. This model can produce operational (day to day activities excluding projects) human resource savings of up to 30%.
9. Displaced operational human resources are redirected to business/strategic projects as dedicated resources paid for by the business with associated IT cost savings.
10. Staff and Customer Satisfaction levels are considerably higher under this model.
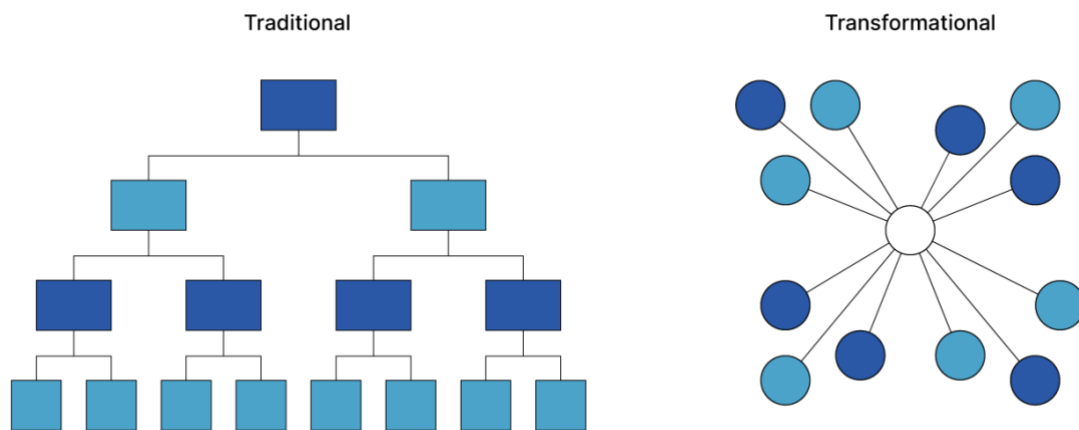
Shift from Traditional to Transformational

Service Desk focus: - You can't manage what you can't measure

As can be seen, the Service Desk is a central feature of the Performance model. I refer to the Service Desk as the Executive Management teams personal CIA. A well-managed Service Desk with an appropriately structured database is all that is needed to manage Performance across all of IT (excluding projects). Even a basic service desk setup is sufficient to satisfy the Performance Management needs. (ITIL improves the management capability but is not essential). Most Service Desk applications can satisfy the Management Reporting needs (Metrics), those that cannot only need to add a fairly simple program to interrogate the database. In around 50% of cases, the database will require restructuring or replacement, this is due mainly to poor design at implementation due primarily to the database being designed around the information needs of the Job Ticket and not around the needs of Management Reporting. In other words, their databases fail because they are arse about.

This work I get underway asap and treat as a high priority, the work is highly justifiable as the Management information the Service Desk provides underpins the entire Performance Management model and its management practices.
I have been constantly amazed over the years to see Service Desks managed as second-class citizens, viewed mainly as a Job ticketing function and not of particularly great value. Nothing could be further from the truth. I have come to learn that the Service Desk is one of the most important of all IT Functions.

Using the Service Desk Database and Queues as information sources, a basic (manual processes) Workload Management system is put in place consisting of Gating, Work Management, Work classifications, Metrics/SLAs and Management reporting. The Service Desk is then able to provide a macro view of all Work across IT. Metrics

by 'Job Type' are then introduced to report on things such as Average and actual Job Completion times, Backlogs, Hold-ups, Repeated jobs, Failed jobs, Recurring jobs and more. Only metrics that can be actioned and improved on are reported on.

The IT Executive Management team now has a view of each teams' performance against the other teams. The degree of inter-team integration can also be measured. Inter-team integration consisting mainly of workflows and touchpoints is the single most important thing that makes IT work. The objective here is to achieve the highest integration level possible. That is, as most jobs in IT need the input of multiple teams, having a seamless workflow, with no hold-ups between the teams, maximizes performance outcomes across the board. This allows SLAs to be achieved with happier customers and staff, it is also a first step to reducing IT spend as a result of reducing and better managing resource needs. There are more steps required to reduce IT spend and improve Performance, changing the management model is a structural and procedural change that acts as a foundation for the changes to follow. It also changes the way the IT Executive Team and all staff view their work – a critical success factor that I will build on.

Part 4 - Four things that contribute to 80% of IT problems

There are four problem areas common to virtually every IT department that account for around 70 to 80% of all of ITs problems and resource usage, those areas are:

1. Workload Management.
2. The Service Desk.
3. Process and Intranet.
4. Managed Services.

Performance Housekeeping (see previous post) identifies and addresses the underlying issues in each of these areas improving performance across all IT teams. This post is a summary of the four areas, the usual issues they each suffer from and the usual outcomes when the issues are resolved. Future posts will detail each of the four areas and provide a detailed Assessment sheet that you can use to identify if you have any of the usual issues along with a sample Actions list on how to resolve them.

1. Workload Management

Workload Management is the process that controls the management of IT work (excluding projects) across all IT teams. It is managed using the Service Desk application and consists of Gating, Work Management, Work Classifications and Management Reporting. A good Workload Management process makes all work visible, accounted for, prioritised, costed and reported on. Two of its key outcomes are that it stops work coming in through back door networks and it provides the Resource Management function with a sound and complete information base making it more accurate. (This really helps given Resource Management is at best – difficult.)

Control of a work approval gate, work classifications, allocation of work requests to Level 2 support work queues, work tracking, IT Team performance monitoring and performance reporting are all the responsibility of the Service Desk. IT teams should receive incoming work only via the Service Desk work queues to which they then apply their own Work Management procedures. All other work falls under projects and is handled separately.

Usual problems
- Lack of an end-to-end Workload Management process.
- Incorrect job allocation to cost centres.
- Gating rule is unenforced.
- Poor inter-team integration.
- Build-up of Installation, Production Support and Maintenance backlogs. (Desktop, Server, Network).
- Service Delivery times adversely affected.
- Customer satisfaction and staff morale are lower.

Usual outcomes
- End-to-end Workload Management process.
- Reduced Installation, Production Support and Maintenance backlogs.
- Faster Service Delivery and Technical Support turnaround times.
- Higher customer and staff satisfaction levels.
- Better inter-team integration.
- All work is visible and accounted for.

Gating

Gating is the process of registering and accepting work into IT. An essential element of the Gating process is the mandatory rule that 'all work is registered (with the Service Desk) before work can commence'. The benefits of this are it stops work coming in through the back door network, it stops the business bypassing priority setting rules, all work is made visible and is accounted for, work is not lost, all work is trackable, and all work is charged to the correct cost centres. Gating supports good Resource Management and helps to identify resource savings; it also facilitates accurate management reporting. Gating also improves staff morale by helping to bring order to areas that are often chaotic, have high rates of rework and are subject to backlogs.

Usual problems
- Gating rule is unenforced.
- All work is not visible or accounted for.
- Incorrect cost centre allocation.
- Use of redundant and overlapping Work Classifications.
- Poor Resource Management.

Usual outcomes
- All work is registered.
- Essential information like cost centre, work classification and priority are captured.
- Standardised work classifications are in use.
- Overlapping work classifications are removed.
- Accurate performance reporting.

Work Management

Work Management is the process of efficiently assigning work to resources, completing and tracking the work through to completion and advising the Service Desk when work is complete. The Work Management objectives are to ensure there are no work request backlogs, that work turnaround times are being met (e.g., OLAs and SLAs) and that customer satisfaction levels are not compromised. Having enough skilled resources available helps achieve work completion times. Resource shortfalls cause work queues to become backed up with old,

dead and outstanding work requests that then result in poor service delivery and lower customer satisfaction levels. Priority 1 and 2 work requests tend to get resolved, but priority 3's do not, they become buried in backlogs. Priority 3 work requests by their nature often contain issues to do with business functionality, more so than systems issues. This in turn affects the businesses' ability to be efficient and provide their own high levels of customer service.

Usual problems

- Priority 3 work request queues often contain hundreds or even thousands of requests (the largest I have seen is 8000) which are impossible to manage and are demoralising for the staff. Failing to address priority 3 work requests has a flow on effect to Maintenance and Production Support where increased resource usage occurs to band aide problems and fix recurring problems. Work Management is also concerned with the identification and resolution of recurring problems which on their own can account for up to 30% of total resource usage and a major irritation to customers.
- Incorrect Work Management procedures are leading to high levels of Desktop, Server and Network installation failures and need for rework.

Usual outcomes

- Reduction of backlogs, resolution of Priority 3's.
- Resolution of recurring problems.
- OLAs, SLAs and other metrics are met.
- Reduced incidence of technical rework.
- Lower technical support costs.
- Technical teams are more proactive than reactive.
- Fewer unplanned outage windows.

Work Classifications

Work Classifications are used by the Service Desk to classify and prioritise all work as it is registered. They are then used by the different IT teams to manage incoming work according to its work queue and priority. Common work classifications across all IT teams are the preferred standard, however, given that the resolution times for Infrastructure and Applications Development work requests can vary significantly, different classifications may exist in this regard, otherwise one scheme should apply to everyone.

Usual problems

- Work Classifications are not standardized.
- Overlapping and redundant Work Classifications in use.
- Too many work queues.

Usual actions

- One Work Classification scheme.
- No overlapping and redundant Work Classifications in use.
- Minimal number of work queues in use.

Management Reporting (metrics)

Performance Management reports that focus on Work Management efficiency. Predefined performance metrics use work queue data to track team efficiencies. Metrics include such things as Completion Times (Actual), Turnaround times (Duration), Queue sizes (Backlogs) and Inter- team transfers (Hold-ups).

Usual problems

- No performance reporting.
- Meaningless metrics.
- Reporting is not used as a management tool.

Usual outcomes
- Meaningful metrics.
- Reporting used as a management tool.

2. Service Desk
Service Desk maxim: You can't manage what you can't measure.

The Service Desk is probably the most important of all IT functions the value of which is often not understood, it has the capability to see every activity right across IT (excluding projects.) When properly established, it becomes the IT departments Workload Management monitor and the IT Management Teams personal CIA. A poorly managed and/or established Service Desk leads to all manner of customer service problems. It must be remembered that for 90% of customers there contact point with IT is the Service Desk, its efficiency is how they rate IT. For IT, it is the window into the customers IT experience in terms of the number and nature of problems being reported. A well-managed Service Desk should be able to tell you at any time what the top 10 problems are and what the top 10 recurring problems are, yet 90% of Service Desks fail this test which is an indicator that the Service Desk is being administrated as against managed. I only ever gave my Service Desk managers one KPI, that was to work towards making the Service Desk redundant. A good Service Desk manager can identify where each IT team is failing to meet performance objectives and where problems are coming from, the Service Desk Manager can then work with the IT teams to improve their quality and efficiency.

Usual problems
- Lack of an end-to-end Workload Management process.
- Cannot see a view of all work
- Workload not subject to performance metrics.
- Unenforced Gating rule.
- Work request backlogs.
- Too many work queues.
- Poor work completion follow-up.
- Not managing top 10 problem types and top 10 recurring problems.
- Poor database design.

Usual outcomes
- End-to-end Workload Management process in place.
- Gating is enforced.
- Macro view of all work with performance metrics in place.
- Accurate job cost allocation.
- Better customer service and satisfaction levels.
- Better staff job satisfaction levels.

3. Process and Intranet
Process maxim: If it's not written down, it doesn't exist.
Intranet maxim: The single source of truth.

Process

IT lends itself perfectly to a high use of process due to the repetitive nature of IT work. Process brings consistency, increased quality, cost-effectiveness, reduced task and project timeframes and fewer errors. It also locks down the operational environment and reduces the number of operational resources required (by reducing the incidence of rework). It provides repeatable consistent outcomes, reduces the incidence of failures and need for rework which reduces costs. Process is necessary because it describes how things are done and then provides the focus for making them better. Process (and other working documents) need to be based on a common template to aid learning and usability.

Usual problems
- Multiple templates in use.
- Broken or incomplete processes in use.
- Poor staff training.
- No Document Management System.
- Work standards and compliance requirements not being met.
- Increased risk.
- Low staff satisfaction levels.
- Inconsistent work quality.
- Decreased productivity.

Usual outcomes
- Introduction of due process.
- Reduced costs resulting from reduced failures and incidence of rework.
- All work is process driven.
- Higher levels of staff satisfaction.
- Consistent work quality.
- Process training for staff.

Intranet

It is not possible to have a high-performing IT department without a fully functioning and managed Intranet. As with process, it is an essential requirement that acts as the IT single source of truth. Most Intranets fall into disrepair, they become full of outdated processes and other working documents and often have an unfriendly user interface. For example, for process to work well it must be quick and easy to find, be based on a common template, be baselined and be the only version available.

Usual problems
- Multiple sources of documentation.
- Multiple versions of documentation.
- Lack of a full-time Intranet appointed owner.
- Lack of a Document Management System.
- Redundant process, how-to guidelines and other documentation in use.

Usual outcomes
- Single source of all documentation.
- Process and how-to guidelines are single version baselined.
- An Intranet owner.
- Introduction of a Document Management System.

4. Managed Services

Outsourcer maxim: We do your mess for less.

Managed Services providers unless carefully managed will take the upper hand largely ignoring the Contract Schedules and managing the contract exclusively for their own benefit. The correct approach is for the client (who is paying for the service) to manage according to the Contract Schedules and to their benefit. This requires a strong contract manager and contract management practices.

Usual problems

- Poor contract management.
- Both parties not having a sufficient working knowledge of the contract.
- Contract management meetings not being held regularly.
- No contract diary.
- Supplier not meetings SLAs and other contract obligations.
- Financial disputes.
- Business projects not being delivered.
- Issues and disputes are not handled in accordance with contract terms.
- Lack of accurate client management reporting.

Usual outcomes

- A full-time client contract management role to maintain constant vigilance over service delivery, contract obligations and financials.
- A contract diary that shows important events and obligations.
- Providers contract manager is held accountable for contract performance.
- Both parties to have knowledge of each other's practices and procedures.
- Weekly contract review meetings.
- Active management of SLAs and other schedule-based obligations.

Part 5 – Best practice IT Standards

Over the last 40 years I have worked in many IT departments. One of the things I made a habit of looking for was what was contributing to great performance within each IT Function and for the department as a whole. My investigations became a list of activities that I added to my IT Performance blueprint and which I called the Best practice IT Standards. These standards play a large part in delivering:

1. Outstanding business partnerships.
2. High-quality, cost-effective project delivery.
3. Technical excellence.
4. Better trained and fewer technical resources.
5. Consistent 99.9% systems availability.
6. Lower IT expenditure.
7. Longer IT memory.
8. Far less failures and need for rework.
9. Higher staff morale and job satisfaction levels.

IT Function matched with its Best practice IT Standard

IT Function	Best Practice IT standard
Service Desk and ITSM	ITIL compliant Service Desk application and ITIL/ITSM Service Management framework.
Workload Management.	End-to-end process comprised of Gating, Work Management, Work Classifications and Management Reporting.
Process and Intranet	All work to be process driven, with documentation management and templates managed in accordance with the Capability Maturity Model (CMM Level 2).

	All process, how to guidelines and other documentation to be sourced only from an Intranet. All documents to be baselined with a single production version. The Intranet acts as the IT memory and single source of truth
Managed Services	Contract manager with a outsource diary, detailed knowledge of SLAs and contract schedules and weekly contract reviews.
Staff Training	Vendor product training.
Infrastructure.	Fleet upgrade strategy.
	Capacity Management function for servers and network.
	Desktop refresh strategy.
	Standard Operating Environment (SOE).
	DBMS management function.
	Server performance management function.
	Formal naming standards for servers and network hardware.
Applications Development. Methodologies.	Tailored SDLCs, Applications development suite, Documented legacy applications. Documented methodologies, guidelines and policy on use of scripts.
Projects.	End to end project management delivery process with supporting templates, guidelines and reporting documents.
Project Management Office.	Active PMO (as against passive), project management processes, templates and guidelines.
Quoting, Scoping, Estimating.	Services catalogue, standard quotation template.
Security.	Five levels of security management with penetration testing.
Change Control.	Change Advisory Board (CAB) with evidential submission criteria.
Disaster Recovery.	BCP, DRP. Testing, back-up site.
Architecture.	Application. - Applications guidelines and catalogue. Technical. - Hardware, Server, Desktop and Systems software guidelines and catalogue. Data. - Database Tables, Records, Fields, Naming definitions, guidelines and dictionary.
Diagrams.	WAN, LAN, Server, Architecture.
Technical Resource Management.	Minimise number of technical resources, maximise number of project resources.
Data Centre.	Asset protection, error free batch processing, on time on-line availability.
Tools and Utilities.	Vendor supported with OS, systems software and applications upgrade paths.

Part 6 – Service Desk and ITSM

You can't manage what you can't measure

Service Desk

The IT Service Desk is the principal interface between IT and the business. The business mostly rates its IT experience based on the performance of the Service Desk. For IT on the other hand, the Service Desk is the window into the business in terms of the number and nature of problems it is experiencing and how efficiently they are resolved.

The Service Desk is involved with critical Service Management processes and centrally manages the actual configuration of the service environment, (i.e., hardware and software components, including support contracts) together with SLAs. It operates best when it is based upon the Best practice IT standard of a ITIL (Information Technology Infrastructure Library) compliant Service Desk Application. There are a range of ITIL compliant applications available, overall, they dramatically improve and speed up the process of complaint to resolution, especially important when you have SLAs and performance metrics in place.

The ITIL solution provides an optional ITSM Service Management framework made up of processes, procedures, tasks and checklists. ITSM focuses on aligning IT services with the needs of the business and meets high-performance service management standards. It enforces the policing of Level 2 problem ticket resolution, is process-driven and provides a view of service management performance and integration across the whole of IT.

A Help Desk by way of comparison is tactical and reactive, using a basic call/issue logging application that creates a problem ticket and then passes the ticket to Level 2 support teams. Notification of completion of the problem closes the ticket. Focus is on short-term, immediate issues with problems being solved on a case-by-case basis. It operates on a break-fix model, is user-oriented and requires fewer resources to manage a relatively simple Help Desk Application. Policing that a ticket has been resolved however is not always enforced. It is not based on a Service Management Framework and does not integrate with other management processes like change or problem management also the Work Classification set-up sometimes suffers from poor definition and enforcement. The key performance measure for a help desk is the closure of completed tickets with descriptive cause and fix information, should the problem reoccur.

A properly established and well managed Service Desk is probably the most important of all IT functions as it has the capability to monitor and help manage all IT operational work (all work excluding projects).

It is the IT departments Workload Management monitor and should at any time be able to tell you for example what the top 10 business problems and top 10 business recurring problems are, yet 90% of Service Desks fail

this test which is an indicator that the Service Desk is not well managed. A good Service Desk manager has the ability to identify where each IT teams problems are coming from and the team's performance against metrics, therefore the Service Desk Manager is able to work with the IT teams to improve their work quality and efficiency.

The Service Desk owns the Workload Management process that controls all IT work (excluding projects). This process consists of Gating (work approval), Work Classifications (priority setting and allocation of work to Level 2 Support) and Management Reporting (performance of and tracking of work across IT Teams). This process makes all work visible, accounted for, prioritised, costed and reported on. Two of its other outcomes are that it stops work coming in through back door networks and it provides the Resource Management function with a sound information base, making it more accurate.

Gating is the process of registering and accepting work into IT. An essential element of the Gating process is the mandatory rule that 'all work is registered (with the Service Desk) before work can commence'. The benefits of this are it stops work coming in through the back door network, it stops the business bypassing priority setting rules, work is not lost, all work is trackable, and all work is charged to the correct cost centres. Gating helps to identify resource savings; facilitates accurate management reporting. and improves staff morale by helping to bring order to areas that are often chaotic, have high rates of rework and are subject to backlogs.

Work Classifications are used by the Service Desk to classify and prioritise all work as it is registered. They are then used by the different IT teams to manage incoming work according to its work queue and priority. Common work classifications across all IT teams are the preferred standard, however, given that the resolution times for Infrastructure and Applications Development work requests can vary significantly, different classifications may exist in this regard, otherwise one scheme should apply to everyone.

Management Reporting are Performance Management reports that focus on Workload Management efficiency. They consist of predefined performance metrics that use work queue data to track team efficiencies. Metrics include such things as Completion Times (Actual), Turnaround times (Duration), Queue sizes (Backlogs) and Inter- team transfers (Hold-ups).

ITIL/ITSM (Information Technology Service Management)

The Best practice IT standard for Service Management is ITSM (Information Technology Service Management). ITSM is implemented under the Service Desk and affects multiple IT teams. ITIL and ITSM are UK government standards, now accepted as global standards, that are manifested in a library of books describing 'best practices' for delivering and managing IT service functions. The aim of ITSM is to facilitate improvements in efficiency and effectiveness in the provision of quality IT services within any organisation. While preferable, not every ITSM process (note ITSM is a set of processes, not software) needs to be implemented with only the critical processes really needing to be covered.

When fully implemented, ITSM looks like this:
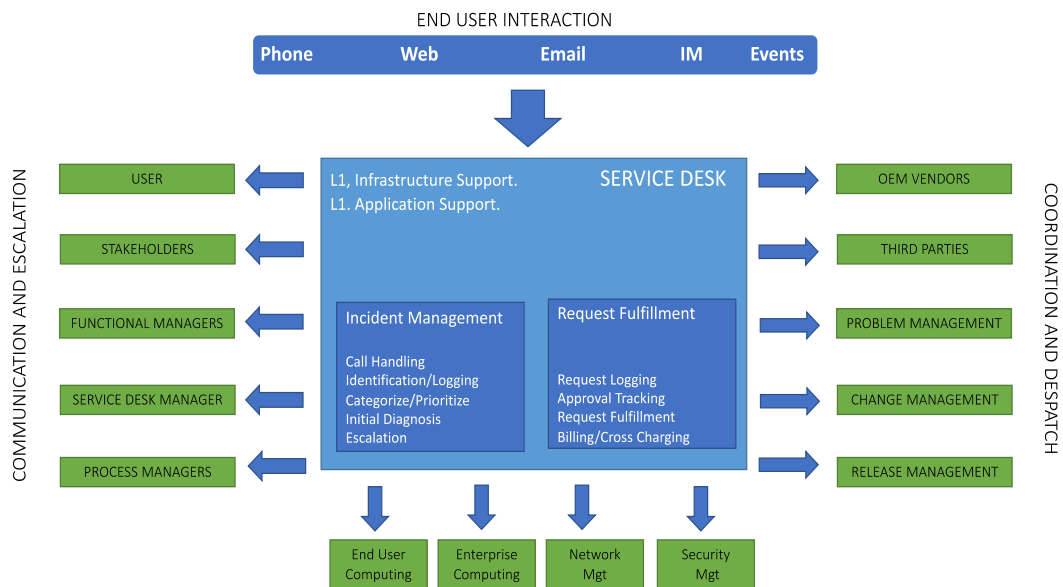
ITSM within the Service Desk environment

Critical ITSM processes

1. **Incident management**: Resolve's symptoms in the short term by providing a temporary workaround so that service availability is restored with minimal interruption. Incident Management and Service Request Management.
2. **Problem management**: Problem management solves the underlying root cause for an incident. Problem management will reduce the number of incidents by addressing the root causes of failure and minimize the impact of incidents.
3. **Availability Management**: Focuses on achieving and measuring the agreed availability levels for the services environment, including coordination of planned downtimes.
4. **Change Management**: Coordinates, prioritizes, authorizes, schedules resources for, and assesses the risk of changes. Change requests come in primarily via the Incident Management or Problem Management processes. Changes are typically required to effect required alterations to the existing environment to introduce a new component, modify or remove a current component, correct an error reported and diagnosed via Incident Management or Problem Management processes.
5. **Capacity Management**: Predicts capacity management that ensures that the business' requirements for capacity and performance are being met. Needs to be integrated with the service desk (by assisting with the diagnosis of performance-related incidents and problems) and problem management in the resolution of capacity related issues. Requires a predictive capacity management function that ensures that the business' requirements for capacity and performance are being met. Requires constant measurement, modelling, reporting along with the designing of services that meet service-level agreements (SLAs). Costs are reduced by using capacity more wisely and risk is reduced by the ability to manage periods of peak demand. Capacity management provides the IT department and business with control over how resources are being used and provides a consistent view of capacity utilisation of the available production potential.
6. **Service Level Management.** The goal of ITIL Service Level Management is to ensure that agreed levels of current IT services are provided, (SLAs) and future services can be delivered within agreed targets.

Non-critical ITSM processes

7. **Supplier Management**. Ensures that the organisation obtains value for money from suppliers and contracts.
8. **Configuration Management System**. A set of tools and data that that is used for collecting, storing, managing, updating, analysing and presenting data about all configuration items and their relationships.
9. **Escalation Management**. Focuses on ensuring incidents or problems encountered within the services environment have the appropriate levels of visibility. Requires an escalation and communications plan and escalation closure criteria.

Performance Assessment

To carry out a Service Desk and ITSM Performance Assessment, download the Service Desk Assessment Worksheet from the Resources Page on Russellfutcher.com.

Actions

The usual actions resulting from the assessment are:

1. Putting in place an end-to-end Workload Management process.
2. Enforcing the Gating rule of 'All work must be registered before it is undertaken'.
3. Reducing the number of Work Queues.
4. Enforcing the capture of Cost Centres and Priorities.
5. Rationalising Work Classifications and remove redundancies.
6. Deleting Work Requests older than 12 months.
7. Analysing with a view to deletion Work Requests older than 6 months.
8. Batching backlogged Work Requests and create projects.
9. Batching backlogged Priority 3's and treat as Priority 2's until cleared.
10. Putting in place either ITSM critical processes or in-house processes.

Part 7 – Process and Intranet
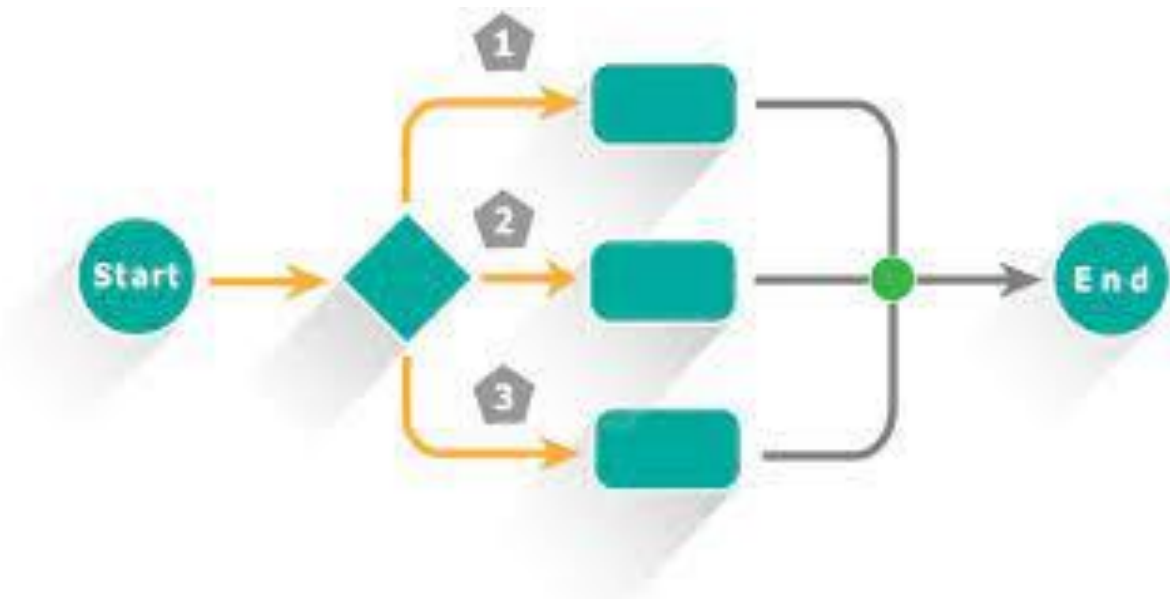
Process

Process maxim: If it's not written down, it doesn't exist.

The best practice standard is the use of a document management system, a process driven environment, (wherever feasible, for all work practices) and use of a standard, common document template for process, how-to guidelines, and other documentation. The template must adhere to documentation management principles. All documentation types are to be stored on an intranet.

IT lends itself perfectly to the use of process due to the repetitive nature of IT work. Process brings consistency, increased quality, cost-effectiveness, reduced task and project timeframes and fewer errors. It also locks down the operational environment and reduces the number of operational resources required (by reducing the incidence of rework). It provides repeatable consistent outcomes, reduces the incidence of failures which reduces cost. Process is necessary because it describes how things are done and then provides the focus for making them better. Process (and other working documents) need to be based on a common template to aid learning and usability.

Usual problems

- Multiple templates in use.
- Broken or incomplete processes in use.
- Poor staff training.
- No Document Management System.
- Work standards and compliance requirements not being met.
- Increased risk.
- Low staff satisfaction levels.
- Inconsistent work quality.
- Decreased productivity.

A Process Performance Housekeeping review is the largest in terms of effort and time. It requires one or two dedicated resources to complete with assistance from all team members. It usually takes two steps to achieve the Best practice IT Standard.

Step 1. Baselined.
Three rules are introduced to govern the use and control of all documentation.

How to Improve your IT

1. Rule 1, If it is not baselined then it does not exist. All process, how-to guidelines and other documentation must be formally documented and baselined (finalised, ready for use).

2. Rule 2, The use of baselined process, how-to guidelines and other documentation is mandatory.

3. Rule 3, Only baselined documents are held on the Intranet.

Step 2. CMM Level 2.
This step accepts that existing documentation templates may vary. This Step includes the Rules from Step 1, adding a single, common documentation template and approach based on the Capability Maturity Model Level 2, (CMM Level 2). This is a process and documentation methodology applied to software development, infrastructure projects and business project planning. The model describes a five-level evolutionary path of increasingly organized and systematically more mature processes.

1. **Initial level:** - processes are disorganized, even chaotic. Success is likely to depend on individual efforts, and is not considered to be repeatable, because processes would not be sufficiently defined and documented to allow them to be replicated.
2. **Repeatable level:** - basic project management techniques are established, and successes could be repeated, because the requisite processes would have been made established, defined, and documented.
3. **Defined level:** - an organization has developed its own standard software process through greater attention to documentation, standardization, and integration.
4. **Managed level:** - an organization monitors and controls its own processes through data collection and analysis.
5. **Optimizing level:** - processes are constantly being improved through monitoring feedback from current processes and introducing innovative processes to better serve the organization's needs.

One of the most significant benefits of using CMM level 2 is that a standard template is used for all process, how-to guidelines and other documentation. The template has a common look and feel, includes completion instructions for the user and complies with documentation management principles. Accordingly, all staff and especially new staff quickly learn how to use process and other documentation in the most optimum fashion. It brings a consistency of approach, improves project quality, reduces cost by reducing the need for rework, improves estimates, scheduling and business outcomes.

Actions to take
Record on a spreadsheet under Intranet and non-Intranet-based, these document types
1. Processes in use.
2. How-to guidelines or similar in use.
3. Methodologies in use.
4. Scripts in use.
5. Technical processes in use.
6. Project processes in use.
7. Gating processes in use.
8. Work management processes in use.
9. Reporting processes in use.
10. All other IT related documentation.

Add spreadsheet columns to record against each document type, documents that are
1. Duplicated.
2. Redundant, old or dead.
3. Ad-hoc, not formalised.
4. Incomplete.
5. Drafts.

6. Not baselined. (not finalised, not ready for use.)
7. Candidates for automation. (manual process that could be automated).

Next steps

1. Determine actions to be taken against each document type as to its suitability to be a baselined Intranet version.
2. Create a Task List suitable for loading into a Project Schedule.
3. Submit the Task List as recommendations for improvement.

Sample Task list

1. Appoint (as a role or position) and train a document administrator in document management principles.
2. Investigate a Document Management System.
3. Determine which documents will be kept and used for baselining.
4. What work is required to baseline the documents?
5. Determine which documents can be disposed of?
6. Determine an 'owner' and the duties of the owner for each process.
7. Which manual processes can be automated?
8. What work is required to create a standard, common documentation template.
9. Review all documents, rework as required and mark each as baselined when complete.
10. Identify umbrella processes that involve inter-team workflows, (activities where multiple teams are involved with the same task) and clearly define the end-to-end process, including hand-off points and deliverables.
11. Create a single version of each baselined document.
12. Convert baselined documents to the common template.
13. Load baselined documents onto the intranet.
14. Investigate moving to CMM Level 2.
15. Determine further works required and scope out.
16. Breakdown the scope of works to task level, ready for loading into the change management project schedule.

Usual outcomes

- Introduction of due process.
- Reduced costs resulting from reduced failures and incidence of rework.
- All work is process driven.
- Higher levels of staff satisfaction.
- Consistent work quality.
- Process training for staff.

Intranet
Intranet maxim: The single source of truth.

It is not possible to have a high-performing IT department without a fully functioning and managed Intranet. As with Process, it is an essential requirement that acts as the IT single source of truth. Most Intranets fall into disrepair, they become full of outdated processes and other working documents and often have an unfriendly user interface. For example, for process to work well it must be quick and easy to find, be based on a common template, be baselined and be the only version available.

Usual problems

- Multiple sources of documentation.
- Multiple versions of documentation.

- Lack of a full-time Intranet appointed owner.
- Lack of a Document Management System.
- Redundant process, how-to guidelines and other documentation in use.

The best practice standard is that all Process, how-to guidelines and other documentation are sourced only from an Intranet. The Intranet is the repository of IT work practices and IT memory. Team-based repositories are not allowed as they introduce the risk of duplication, lack of version control and non-adherence to process and documentation rules.
(An Intranet is a network internal to an enterprise that uses the same methodology and techniques as the internet but is accessible only to employees).

For reasonably sized IT departments (min 100 staff), a dedicated Intranet Administrator trained in document management and preferably CMM level 2 is required. Having a library with documentation examples within the intranet is required. Processes and other documentation under development need to be held under separate cover and not on the production Intranet. The Intranet needs to act just as a production environment acts and meet the test of being the 'single source of truth.'

Actions to take
Record on a spreadsheet all the following Intranet-based document types.
1. Processes in use.
2. Guidelines or similar in use.
3. Methodologies in use.
4. Scripts in use.
5. Technical processes in use.
6. Project processes in use.
7. Gating processes.
8. Work management processes.
9. Technical processes.
10. IT Policies.
11. IT Other.

Add spreadsheet columns to record against each document type, if it is
1. Duplicated.
2. Redundant, old or dead.
3. Ad-hoc, not formalised.
4. Incomplete.
5. Drafts.
6. Not baselined. (finalised, ready for use.)
7. Candidates for automation. (manual process that could be automated).

Next steps
1. Compile responses to the actions.
2. Create a Task List suitable for loading into a Project Schedule.
3. Submit the Task List as recommendations for improvement.

Sample Task list
1. Compare the 'Process and other Documentation' spreadsheet with the 'Intranet' spreadsheet. Determine which documents are to be kept for baselining and which are to be disposed of.
2. Identify umbrella processes that involve inter-team workflows, (activities where multiple teams are involved with the same task) and clearly define the end-to-end process that binds the teams.
3. What work is required to baseline the documents?

4. Which manual processes can be automated?

Usual outcomes

- Single source of all documentation.
- Process and how-to guidelines are single versions baselined.
- An Intranet owner.
- Introduction of a Document Management System.

Part 8 - Managed Services

Why do you need to assess your management of Managed Services? Because you pay a hefty sum for them and often do not get what you deserve.

Managed Services (Outsourcing)

"We do your mess for less"

Outsourcing your IT is a good solution for controlling IT costs, but it can be fraught with dangers if not properly managed.

I have been an Outsourcing Contract Manager for several large, complex Financial Services IT contracts. The key lesson I learnt is that unless carefully and skilfully managed, the promised services and improvements are not always forthcoming. This is despite the fact that the Outsourcing business model is a good one where the provider can make use of an IT shared services to standardise the clients' environment, reduce their cost of delivering services and make it easier to achieve SLAs. But not all contracts or clients are moved under shared services as this involves up-front costs for the provider, rather the clients' services are left as is (no change to platforms or software) with reduced chances of achieving SLAs. This is where the Outsourcer saying of "We do your mess for less" comes from.

Clients need to maintain the upper hand when it comes to managing their IT contracts to stop the provider managing the contract exclusively for their own benefit.

The correct and really only available client approach is to make sure that contract obligations are being honoured by managing according to the contract Schedules noting that most providers actively fight this approach as they do not want to be held accountable to the contract or have it managed in this way.

Managing according to the Contract Schedules

Firstly, let's be clear on how a contract is constructed. It is in two parts, the Terms and Conditions and the Schedules. The Terms and Conditions set out the legalese of the contract, this is where the lawyers do their work, post contract execution a client is really only interested in a few sections – 1) Meetings, 2) Financial Obligations and 3) Contract Disputes. The Schedules on the other hand are the guts, the details of the contract, they spell out the Services and Improvements to be delivered along with associated SLAs. (E.g., If a File Server fails it must be recovered within one hour).

The Schedules are lengthy due to the sheer volume of Services to be provided which is why when preparing and negotiating the contract, 80% of the time is taken up with the Schedules. The Schedules also spell out improvements to be made to the client's environment such as the rationalization of servers, rollout of a SOE and so on. They also describe methodologies, approaches and techniques to be used by the provider in the execution of the contract. This is why the people who will manage the contract after its execution need to be part of the Schedules construction and negotiation phase.

> *You write it, you agree to it, you live with it*

Usual Contract Management problems

- Unanticipated costs.
- Poor Service Delivery.
- Poor Project Delivery.
- Financial disputes.
- Lack of a client contract management office.
- Contract Managers not party to the contract negotiation.
- Poor contract management practices such as no contract diary.
- Inexperienced Contract Manager. (The client contract manager needs to have a working knowledge of each of the outsourced services (e.g., Development, Infrastructure, Communications).
- The IT Architecture function is outsourced. (This must be retained in-house to ensure that the client controls the IT Strategy to ensure alignment with the Business Strategy.)
- The legal department manages the contract. (This is a huge no no, as the lawyers only understand the Terms and Conditions and not the Schedules, which represent the day-to-day work).
- Contract management meetings not being held weekly.
- Supplier not meetings SLAs and other contract obligations.
- Issues and disputes are not handled in accordance with the contract Terms.
- Lack of accurate client management reporting.

Best Practice Client Contract Management

The Best practice IT Standard for Contract Management is the establishment of a Contract Management Office for the exclusive management of Managed Services contracts. The Office set-up is based on managing the contracts according to their Schedules. This requires the following:

- A Contract Manager role or position depending on the scope and scale of the contracts. The Contract Manager needs to have been party to the contract negotiations.
- An Outsourced Function SME for each of the major Service areas that have been Outsourced. For example, if Infrastructure including Network and Communications has been outsourced then an Infrastructure Manager on the client side is required. Again, this may be a role or a position depending on the scope and scale of the contract.
- A Service Delivery Manager role or position is required to counterbalance the providers Service Desk and Service Delivery functions. This is a full-time position requirement.

- The IT Architecture function is to remain in-house in order to ensure that the client retains control over their technology destiny and to ensure alignment of the IT and Business strategies.
- Creation of a Contract Diary that includes all events and obligations for both parties, such as regular meetings and contract annual reviews.
- Weekly Service Delivery meetings to review as a minimum all Service Delivery activities, Service Desk performance, SLA performance, Project performance, delivery of Improvements, Financials, Reporting, Client customer satisfaction levels and Disputes. The providers Service Desk should also table two reports 1) Top ten Problems report and 2) Top ten Recurring Problems report.

This Contract Management Office set-up earned a Gartner's best practice award

---

Usual Outcomes

- The squeaky wheel gets the oil.
- Both parties have a detailed knowledge of the contract Schedules.
- Client is able to maintain constant vigilance over service delivery, contract obligations and financials.
- The Managed Service providers performance improves, sometimes to the point of actually delivering according to their obligations.
- Should the providers performance be particularly bad, the client has a recorded history or events that can be used for legal action or for the withholding of payments.
- Contract management practices such as a Weekly review meeting and a Contract Diary keeps the client in the driver's seat.
- The provider's contract manager is held accountable for contract performance.

Performance Assessment – assess your current position

Taking a moment to answer the following questions gives you a good perspective on where you are in terms of managing your contracts and what level of performance you are receiving.

- How would you describe the outsourcer relationship? (partnership, friendly, contractually based, acrimonious.)
- Are their separate contracts or separate sets of Schedules for each cloud platform? (Refer below)
- Are you incurring unanticipated costs?
- Are new Services negotiations held in good faith?
- Are issues and disputes being handled to your advantage?
- Are there any current or possible future contract disputes?
- How would you rate SLA compliance? (L, M, H)
- Are business targets being met?
- What if any financials are outstanding by both parties?
- Is there a Contract Diary?
- Where is the IT Architecture function located?
- Who controls Security Standards?
- Who owns Data privacy (For example, does the outsourced data include personal data or competitively sensitive data such as trade secrets)?
- Who owns the data and is data encryption implemented?
- On termination of the contract, what data formats are available?
- Who reviews the providers technology lock-in position (Where the supplier implements a proprietary solution)?
- How satisfied are the clients' customers?
- How would you rate project delivery performance? (Low, Medium, High)
- How would you rate Service Delivery performance? (L, M, H)

- How would you rate the providers Service Desk performance? (L, M, H)
- Is the providers contract manager held responsible for the client's overall satisfaction within the contract performance?
- Does the providers contract manager have a detailed knowledge of the client account?
- Does the providers contract manager have detailed knowledge of the customer's practices and procedures?
- Do both parties have a working knowledge of the contract Schedules?
- What regular client reporting is being received?
- What if any outstanding matters are there?
- Have you personally toured the disaster recovery back-up site?
- How familiar are you with the DR plan?
- Where is the DR plan physically located?
- If you share a back-up data centre with other customers, where are you in the recovery queue?
- Have your staff been walked through the DR plan as an Implementation exercise.

Reference information

Cloud-based Outsourcing Models and Platforms

Today, rather than being responsible for managing infrastructure, cloud-based solutions have enabled IT departments to dispense with the processes of acquiring, updating, and maintaining software and hardware, leaving these to third-party providers. By doing this, organizations can allocate a more significant share of their budget to activities that better contribute to improving business outcomes. Leveraging managed services from a cloud service or hosting provider allows organizations to free up their IT staff to work on more strategic, revenue-generating projects, instead of focusing on operating infrastructure.

Outsourcing Models

Software as a Service (SaaS) is access to applications, hosted by an outsourcer that are accessible via the internet.

Platform as a Service (PaaS) is an outsourced platform hosted by an outsourcer that facilitates the development, test, and management of web applications.

Infrastructure as a Service (IaaS) is the provision of outsourced resources (servers, storage, networking) via the internet on a user pays basis.

Desktop as a Service (DaaS) is the provision of virtual desktops, accessed over the internet and hosted by an outsourcer.

Cloud Platforms

Managed cloud hosting is a process in which organizations share and access resources, including databases, hardware and software tools, across a remote network via multiple servers in another location. However, before considering costs, the critical focus of managed cloud hosting is on security and consistent availability. Cloud computing is a user pays service that facilitates network access to shared resources (networks, applications, servers, storage) accessed via the internet.

Private cloud. The private cloud infrastructure provides a dedicated network and equipment that are operated solely for the customer's business.

Public cloud. The public cloud is made available to the general public by a supplier who owns, operates, and hosts the cloud infrastructure and offers access to users over the Internet.

Community cloud. The community cloud infrastructure is a multi-tenant cloud service model that is shared among several organizations and is governed, managed, and secured commonly by all the participating organizations or a third-party managed service supplier.

Hybrid cloud. The hybrid cloud is composed of two or more clouds (private, public, and/or community clouds) that remain separate but are bound together, offering the advantages of multiple deployment models.

Part 9 - Staff Training

I am a great believer in keeping staff training levels up to date. Unfortunately, in times of cost cutting and budget restraints, training is usually the first cost centre to be cut, this I have always resisted as the benefits of keeping product training up to date are substantial. The importance of training cannot be overstated. Companies invest large amounts in hardware, software and services but often fail to train or fall behind in the training of their staff in these products (hardware, systems and applications software, software suites and utilities). Failing to train staff on products they use is simply an inefficient and often costly use of those assets. Having untrained staff using IT products is also a risk, and when training on new technologies falls behind, capability and productivity suffer as does staff morale and the professionalism of the IT department.

The Best practice IT standard is:

- A product must be from a reputable vendor who provides training, technical support and a technical upgrade path.
- At least two members of staff must be trained at product purchase.
- Free, off the Web products are not allowed unless there is an extenuating circumstance due to the inherent risks they introduce and potential negative effects on system upgrade paths.

Product training ensures:

- Proper product installation and integration.
- Proper OS and systems software configuration set-up.
- Proper Application interface set-up.
- Proper application of product functionality.
- Risks of introducing the product are reduced.
- The use of scripts decreases.
- Capacity management integration improves.
- Security integration is better.

- Staff morale and confidence improve as staff are vendor qualified.

When a staff member who has been working on a product without training, then subsequently goes for training, this is what tends to happen.

- Software gets reinstalled.
- OS and systems software configurations get changed.
- Application interfaces get changed.
- New functionality is used, software and business outcomes improve.
- Risks are reduced.
- The use of scripts decreases.
- Capacity management improves.
- Security gets tighter.
- Morale and confidence improve.

Performance Assessment

The Performance Assessment is to do a thorough audit of all products in use and match against each - staff training needs. The Roles and Responsibilities template also recorded staff training and training needs.

Conduct a Product/Training Audit

- Record on a spreadsheet the following items. (Some items may need to be grouped, like hardware types as the volumes may be high).
- Desktop and Mobile hardware.
- Server Hardware.
- Network hardware.
- Systems software.
- Utilities.
- Infrastructure toolsets.
- Applications development toolsets.
- Applications.
- Legacy systems.
- Other.

Against each product, record:

- Staff member name who has been trained on the product.
- Staff member name who requires training on the product.

Questions to ask

- Which products are in use without staff training?
- Which staff need vendor training on which products?
- Which products are in use that are not vendor supported?
- Which products are Web freebies?
- How many staff have been trained on legacy systems?
- Are there individual staff training plans in place?
- Is staff training up to date with new technologies?
- Is there a shortage of critical skills?
- Are skill shortages due to lack of staff, staff turnover or lack of training?

Part 10 – Infrastructure

There is a saying that CIOs lose their jobs because of bad Infrastructure Managers. I add to this that the Infrastructure Managers are bad because they fail to understand the basics and that the devil is in the detail. I have managed many Infrastructure departments small and large, and whilst I can say that they are indeed a challenge, if you put the basics in place, they are easy to manage. IT Infrastructure is complex and critical to all IT operations, consisting mainly of Service Delivery, Installations, Maintenance, SOEs, Server and Desktop refresh strategies and Networks and Communications. Pay attention to the basic needs of these and things look after themselves.

The Best practice Standard is 99.9% Server and Network availability, a hardware fleet upgrade strategy driven by applications capacity needs, response time objectives, systems capacity management requirements, hardware failure rates and fleet ageing, A systems software upgrade strategy and desktop refresh strategy are also required.

Ask your Infrastructure manager to conduct this Performance Assessment, think of it as a health check. It is the assessment I have always conducted in my early days as a CIO or Infrastructure Manager as it quickly lets me understand the degree of risk I am carrying. Try it out for yourself.

Performance Assessment

1. Servers

The results of this Server hardware audit are also used to check on the accuracy and completeness of the IT Budget and provide input into the next IT Strategy (Risk analysis).

Actions

Record on a spreadsheet all the following. (By unit or group by type. Show total numbers).

- List all systems servers.
- List all web servers.
- List all applications servers.
- List all e-mail servers.
- List all back-up servers.

- List all other server types in use.
- List all server management software in use.
- List all maintenance/support agreements in place.

Rate all of the above as either (H, M, L) risk based on probability of failure.
Does the budget reflect all software licensing and maintenance costs for the above items?

Questions to ask

1. What server recovery processes exist?
2. What is the average production server's failure rate? (unplanned shutdown).
3. What is the average production applications server's failure rate? (unusable to users).
4. How is server resource utilisation managed? (CPU, memory and disk-space (used and free))
5. Is there a formal process for server physical and logical installation?
6. Is there a formal manual or automated process for server recovery?
7. When was the last test of restoration from a back-up completed?
8. How are back-ups confirmed as complete?
9. How often are full image restores used?
10. Is the reinstallation of systems and applications software manual or automated?
11. Is resource utilisation trending in place for critical systems?
12. Are all servers included in the depreciation schedule?
13. Are all servers covered by a maintenance agreement?
14. Is critical infrastructure covered by high priority maintenance agreements?
15. Has the infrastructure disaster recovery plan been tested?
16. Is there a server refresh strategy in place?

2. Other hardware

Actions

- Record on a spreadsheet all the following.

    o List all desktops (by unit or group by type).
    o List all routers (by unit or group by type).
    o List all switches (by unit or group by type).
- Based on failure rates or equipment age, rate all the above items as either (H, M, L) risk.

Questions to ask

1. How effective are desktop service delivery and repair procedures?
2. How quickly can a router or a switch be replaced?
3. What are the router and switch failure rates?
4. Is critical infrastructure covered by high priority maintenance agreements?
5. Are patches up to date?
6. Is there a desktop refresh strategy in place?

3. DBMS

Questions to ask

1. How many staff are involved with database administration?
2. Are there user account and share management procedures in place?
3. Administration services for active RDBMS in use?
4. What daily housekeeping procedures are in use?
5. How is capacity management, managed?
6. How is performance analysis/tuning conducted?
7. Does a systems software upgrade strategy exist?

8. Who owns and manages software license management?
9. What vendor support arrangements are in place?

4. Naming standards

Often hardware does not have a formal naming standard, instead names of planets or mountains or similar are used which is unprofessional and can lead to a variety of problems. The best practice standard is the use of a server, router and switch naming standard consisting of 'type' (for servers -web, system, print, production, application), 'location code' and 'incremental number.' A good naming standard makes it easy to deploy, identify and filter through hardware farms, especially when you may have hundreds, or thousands of units deployed. There are important advantages to adopting a formal naming standard, one that scales as the population grows.

- It speaks to the professionalism of the IT department.
- New staff can quickly learn to identify hardware types.
- Mistakes caused by selecting the wrong piece of hardware are far less likely.
- Disaster management benefits when staff and third parties need to identify and prioritise the hardware recovery sequence.

5. Tools and utilities

The best practice standard is that all software tools and utilities are vendor supported with an OS, systems software and applications upgrade path. Tools and utilities have a nasty habit of multiplying, especially when they are freely downloadable from the Web. Most technical and engineering staff have their own set of utilities for fixing problems as against a set of approved vendors supported products. The Best practice IT Standard is a vendor supported, shared set of utilities in order to have confidence that common and consistent outcomes will be produced.

Actions
- Record on a spreadsheet all the following.

    o List all software tools and utilities in use.
    o List all scripts in use.
    o List all SOE's in use.
- Rate all the above items as either (H, M, L) risk based on being vendor or non-vendor supported.

Questions to ask
1. What tools/utilities redundancies exist?
2. What scripts redundancies exist?
3. What tools, utilities and scripts can be removed?
4. Should there be a policy of not downloading products from the Web?
5. Is software distribution fully automated?
6. Are production and development SOEs isolated?
7. Are their redundant SOEs, what can be removed?

Build an Infrastructure Scope of works
1. Collate all of the Reponses gathered into a task list.
2. Prepare a risk analysis for all hardware and software and DBMS.
3. Update asset registers.
4. Update budget depreciation amounts and other asset related costs.
5. Review production servers with high failure rates. (unplanned outages).
6. Review production applications servers with high failure rates. (unusable to users).
7. Establish server resource utilisation management. (CPU, memory and disk-space (used and free))
8. Create a process for server recovery by type.

9. Create a hardware fleet upgrade strategy.
10. Create a systems software upgrade strategy.
11. Create a desktop refresh strategy.
12. Put in place database monitoring.
13. Determine further works required and scope out.
14. Breakdown the scope of works to task level, ready for loading into the change management project schedule.
15. Risk mitigation actions from risk assessment.
16. Fully automate software distribution.
17. Remove redundant, tools, utilities and scripts.
18. Replace non-vendor supported products with vendor supported products.
19. Train staff on supported products.
20. Standardise engineering toolsets.
21. Investigate standardising on a common naming convention for servers, routers, switches and migrate to over next six months.
22. Determine further works required and scope out.
23. Breakdown the scope of works to task level, ready for loading into the change management project schedule.
24. Determine further works required and scope out.

Part 11 – Applications Development

The Best practice IT Standard is comprised of:
1. A thoroughly documented and tailored where appropriate, development lifecycle methodology. (Systems Development Lifecycles-SDLC) with associated how-to guidelines and procedures.
2. A vendor supported, integrated applications development toolset.
3. Development and test databases refreshed daily.
4. As the applications portfolio is usually a mix of packaged solutions and in-house developments, both require thorough documentation, especially legacy applications.
5. Development work like enhancements requires rigorous functional gap analysis and review of business processes before work is undertaken.
6. The use of scripts is minimised as they tend to organically grow which makes them problematic and requiring manual intervention to run.

Performance Assessment
Testing
1. What is the approach to testing?
2. Does the testing approach cover people (numbers and skills), capacity, software and tools, overall technical environment, processes (e.g., function test, performance and load test, problem reporting, management and fixing), and the user functions?
3. Does testing cover off usability, reliability, functionality, and performance versus the documented requirements.
4. How is testing planned and documented?
5. How are test statements planned and documented?
6. Do test plans include component tests, integration test, regression tests, system test and acceptance test.
7. How are acceptance criteria for the system deliverables defined?

Quality Assurance
1. What quality management tools and techniques are in use?
2. How is quality assurance integrated with sub-contractors?

Conversion
1. What format do the conversion strategies take?
2. Are conversion rules, programs and final data file definitions defined?
3. How is the original environment described?
4. What if any conversion tools are in use?
5. Are conversion and integrated acceptance test plans defined?
6. How is the clean-up of converted data defined?
7. How is a newly converted system compared with the original to assess identical results?
8. What data integrity issues exist?

Sample Task list
1. Create an end-to-end testing process including the use of test harnesses, scripts and conditions.
2. Review the use of and management of development and testing environments.
3. Review recent application failures (unusable to users), assess cause and ensure mitigations been put in place.
4. Introduce a Rule of 'fix a problem once'.
5. Split DBAs into Systems and Applications.
6. Locate application DBAs with developers.
7. Create any necessary umbrella processes that involve inter-team workflows including hand-off points and deliverables.
8. Pending how often conversions are undertaken, consider creating a conversions process that includes sub-contractors.
9. Determine extent of data integrity issues and how to resolve.
10. Define and agree a test environment.
11. investigate QA toolsets.
12. Determine further works required and scope out.
13. Breakdown the scope of works to task level, ready for loading into the change management project schedule.

Methodologies

The Best practice IT Standard:
Is that applications development methodologies are guiding all development activities, there are five primary types:

1. The waterfall model: - this is the classic SDLC model, with a sequential process that has goals for each applications development phase. The waterfall model simplifies task scheduling, because it is linear with no iterative or overlapping tasks.
2. Rapid application development (RAD): - based on the approach that solutions can be developed more quickly using development workshops to collect system requirements. Makes use of prototyping and reiterative design testing.
3. Joint application development (JAD): - this model involves the client or end-user in the design and construction of an application through a series of collaborative workshops.
4. Prototyping: - in this model, a prototype (an early approximation of a final system or product) is built, tested, and then reworked as necessary until an acceptable prototype is finally achieved from which the complete system or product can now be developed.
5. Synchronize-and-stabilize: - this approach calls for different development teams working in parallel on different parts of an application. Requires regular synchronization of code.

Performance Assessment
1. How often are development databases refreshed from production databases?
2. Are the methodologies in use tailored?
3. What methodology how-to guidelines exists?

4. Are there matching Work Breakdown Schedule templates in use?
5. What is project delivery performance like (timely delivery of all software developed by (and subcontractors) to defined acceptance criteria (i.e. on schedule, within budget, with required function, with required performance and to the specified quality)?
6. Is there an agreed and documented procedure for interfacing with subcontractors?
7. How are subcontractors advised of in-house development standards?
8. Are regular performance reviews of progress including monitoring actual versus plan on a task and effort basis conducted with sub-contractors?
9. Is Quality Assurance involved in code inspections?
10. Is there a clear and unambiguous view of the overall application architecture and, is this conveyed to subcontractors?
11. Is a close and continual liaison with the technical architect maintained to ensure that all matters potentially affecting system capacity and performance are communicated and understood?
12. How are applications security requirements managed?

Sample Task list
1. Review software licenses.
2. Risk analysis of in-use methodologies.
3. Assess methodologies fit for purpose.
4. Document in-house methodologies and customisations to packaged methodologies.
5. Determine further works required and scope out.
6. Breakdown the scope of works to task level, ready for loading into the change management project schedule.

Part 12 –Security

The Best practice IT Standard is comprised of.

Five levels of managed security with penetration testing, underpinned by CARTA (a strategic approach to information security that was introduced by Gartner in 2017).

Security levels

1. **IT security**. Refers to securing digital data, through computer network security. It is accountable for preventing unauthorized access to organizational assets such as computers, networks, and data and it maintains the integrity and privacy of corporate information and the blocking of hackers.
2. **Information security**, on the other hand, refers to the processes and tools designed to protect business information from unauthorised access.
3. **Network security**. Used to prevent unauthorized or malicious users from getting into a network, ensures that capacity, reliability, and integrity are not compromised. The Network security risk profile increases as business increase the number of endpoints and migrates services to the public cloud.
4. **Endpoint security**. Protects mobile phones, laptops, and desktops. It restricts access to malicious and typically includes malware protection and device management.
5. **Internet security**. The protection of information that is sent and received in browsers. Includes network security involving web-based applications. These protections come in the form of firewalls, anti-malware, and anti-spyware, ransomware.
6. **Cloud security**. Applications and data held in a cloud-based data centre. The usual security measures do not protect users who are connecting to the internet. Cloud security secures software-as-a-service (SaaS) applications and the public cloud.

CARTA

Within the CARTA approach, decisions and security responses are made based on risk and trust. There are three phases of IT Security where CARTA plays a role: Run, Plan and Build. In the Run phase, CARTA lets the organization use analytics to focus only on the biggest threats and automate the majority of the incidents. In the Build phase, CARTA plays a role in DevSecOps, as teams identify threats and eliminate them from apps they are building and use things like a digital risk rating service to analyse open-source components they may want to use. In the Plan phase, CARTA invites organizations to use analytics to determine the risks of things such as having employees change passwords frequently versus the productivity impact and decide how much risk to accept. (Source, SUSE).

Performance Assessment

1. Does your security function cover the five security types?
2. Is there a security manager?
3. Does the security manager report to the Infrastructure manager?

4. Is your security managed in-house, or is it outsourced?
5. What types of annual penetration testing takes place?
6. What resolution times for new threats are you receiving from your external suppliers?
7. What is the number of security violations per month?
8. Are the security violations trending upward?
9. What are the number of monthly security violations/hacks by security type?

Sample Task list

1. Carry out a risk analysis of the five security functions.
2. Review all five levels of security for completeness.
3. Arrange external penetration testing.
4. Define and design a systems security architecture.
5. Determine further works required and scope out.
6. Breakdown the scope of works to task level, ready for loading into the change management project schedule.

Part 13 – Projects and Project Management Office

Projects
How do Projects Fail? (One day at a time)

The Best practice IT Standard is:
A rigorous end to end, project management lifecycle with supporting how-to guidelines and templates.

Performance Assessment
1. What project management software is in use? Is it a standard?
2. Are project managers sufficiently experienced and trained?
3. Is the end-to-end project lifecycle process documented with supporting documentation on project plan, milestones, work breakdown structure, status reports, quality control, and SDLC methodology inclusion?
4. Is there a project master- plan showing all active and pending projects as well as project interdependencies?
5. How are independencies managed?
6. How many pending projects are currently on the project list?
7. How many projects are in-flight (active)?
8. Are project initiation and monitoring processes clearly defined?
9. Is there a rigorous approach to project evaluation, approval and prioritisation?
10. What project management and control measures are in place?
11. Is the quality of project scope and requirements documentation, estimating, project plans & status reports of sufficient quality?
12. How do you assess project quality?
13. Are project post implementation reviews carried out?
14. Is proper escalation and expectation management in use?
15. How do you assess scheduling capability?

16. How do you assess estimating capability?
17. How are budgeting and cost controls managed?
18. What can the PMO do to help dedicate more technical staff to projects?

Sample Task list

1. Assess project initiation and management risks.
2. Assess need for project manager training.
3. Develop umbrella processes to manage intra-project dependencies and workflows?
4. Is the project master plan reviewed regularly?
5. Appoint a projects master plan owner with accountabilities.
6. Create a scheduling and estimating guide.
7. Create budget and cost management guidelines.
8. Determine further works required and scope out.
9. Breakdown the scope of works to task level, ready for loading into the change management project schedule.

Project Management Office

The Best practice IT Standard is:

Is an active PMO. An active PMO receives standardised reporting from project managers, provides common traffic light style management reporting to the business and IT, actively monitors and polices project progress against cost and schedule and holds project managers accountable for their performance. Additionally, it provides a suite of project management processes, templates and how-to guidelines, such as how to estimate, create a schedule or produce a weekly progress report. It provides clearly defined project roles and responsibilities and an end-to-end projects delivery process that combines business and IT. An active PMO should be considered once the average number of small to medium-sized projects exceeds 15 per annum.

A high degree of project management standardisation is essential for ensuring quality and timely outcomes. This is because the standards in place become common to all projects, with all involved knowing what is expected of them irrespective of what team they are in. Finally, it provides a program management function across all of IT to oversee and coordinate the project schedules, resources, cross-project dependencies and the timely resolution of critical issues. It owns the macro view of all projects (the master plan). It provides the following management support to project managers and projects:

1. Governance and administrative support system for tracking issues, tracking changes, producing status reports and ensuring that the project runs smoothly.
2. Project management experience, including project planning and tracking skills (using an automated project management tool).
3. Assistance with project controls. These include the management control systems for deliverables, quality, inventory, costs, time recording, billing, security/confidentiality, service level agreements, risks, issues, problems and changes (both technical and contract).
4. Scheduling, organizing, preparing materials for and minutes for regular project meetings.
5. Owning and maintaining the central repository of information for the project. The central repository contains the project plans, the library of project deliverables, project filing and general project information, such as a contract, a holiday chart and contact points for all people associated with the project.

In contrast to an active PMO, the passive PMO does not monitor or police project progress against cost and schedule, nor does it hold project managers accountable for their performance. It receives reporting from project managers and may provide basic management reporting in turn.

Performance Questions

1. Is the PMO Passive or Active?

2. If passive, how is project performance assessed?
3. If an active PMO, how is project performance assessed?
4. Is there a Projects Portfolio Master Plan/Schedule?
5. How is the projects portfolio managed?
6. How are project inter-dependencies scheduled and managed?
7. Describe the end-to-end project process from inception to completion.
8. Do processes and how-to guidelines support the end-to-end project process?
9. What PMO software support is in use?
10. Are process templates standardised?
11. Are IT and business reporting integrated?
12. Does project status reporting use a traffic light reporting format?

Sample Task list
1. Review the end-to-end project implementation process.
2. Review templates and how-to guidelines.
3. What project management software is standard?
4. introduce software support for project monitoring?
5. Determine further works required and scope out.
6. Breakdown the scope of works to task level, ready for loading into the change management project schedule.

Part 14 - Quotations and Change Control

Quotations
The Best practice IT Standard is:

A quotation template that formalizes and integrates the three processes of scoping, estimating and quoting. The quote requires the scoping of hardware, software and services with prices from an IT services catalogue and/or an architecture products catalogue. The quote should have a fixed validity period.

Around 50% of business work requests disappear after a proper quotation has been prepared. Using the 'Mandatory, Highly Desirable, Nice to Have' technique when determining scope in conjunction with a IT services catalogue improves accuracy and rapidly speeds up the quoting process.

Sample Catalogue Listing

The official definition of an IT Services Catalogue is from ITIL and it defines it as a database or structured document with information about all IT Services that includes information about deliverables, prices, contact points, ordering and request processes.

Category	Service
Software	Software Distribution, Licensing, Implementation, Licensed Software, Web Developer Tools
Support and Training	FAQs, Online Help, Training Programs, Teaching and Learning, Knowledge Sharing
Networks and Connectivity	Wi-Fi, VPN, LAN, WAN, Network Monitoring
Messaging and Collaboration	Email, Instant Messaging, Mailing Lists, Calendar, File Sharing, Fax
Voice	Mobile, Telephone, Audio Conferencing, Video Teleconference, Radio
Accounts and Access	Identity Management, Guest Accounts
Cloud Services	Provisioning
Data Centre	Off-site Storage, Facility Management
Hosted Services	Web Hosting, Database, Data storage, Backup Services, Content Management
Security	Security and Privacy Policy, Disaster Recovery, Network Monitoring
Video	Video Equipment, Television
Print	Printing, Copy, Printer Maintenance
Infrastructure	Web Services, Wiring Services, Load Balancing, Mainframe
Hardware	Desktop PC, Laptop, Mac, Mobile Device, Server, Accessibility Resources, Tape Management
Professional Services	Strategy, Planning, Project Management, Document Management, Application Integrations, Digital Asset Management

Performance Assessment

1. How are quotations currently prepared?
2. How accurate are current quotations?
3. Are there scoping and estimating processes integrated to form a single quote?
4. Is there a standard quotation template in use?
5. Is there an IT services catalogue?
6. If there is no IT services catalogue is in use, how are hardware, software and services identified and priced?
7. How long is IT bound by its quotations?

Sample Task list

1. Create an IT services catalogue.
2. Create a standard quotations template for use across IT.
3. Create an umbrella quotation process to manage the activities of multiple teams involved with creating a quotation.
4. Create an estimating guide.
5. Who will prepare quotes?
6. Who will own the quotation process?
7. Determine further works required and scope out.
8. Breakdown the scope of works to task level, ready for loading into the change management project schedule.

Change control

The Best practice IT Standard is:

A Change Advisory Board (CAB) being in place, with evidence-based change control acceptance criteria needing to be approved before a change is promoted to production. Since Change Control is the process that promotes changes into production systems with the intent of no disruption to those systems, the CAB is held accountable for any post-promotion to production systems availability issues, stability issues, integrity issues and failures.

Performance Assessment

1. Are Change Control and Version Control processes in use?
2. Are these processes documented?
3. What change management software is in use?
4. Is there a Change Advisor Board (CAB)?
5. If not, how is change control managed?
6. Are CAB acceptance criteria clearly spelt out?
7. Does CAB enforce its acceptance criteria and process?
8. Is the CAB accountable for any postproduction promotion problems?
9. What authority does the CAB have?
10. Are the CAB acceptance criteria documented and enforced?
11. Who is the final CAB arbitrator?
12. Who can override CAB?
13. Do the CAB acceptance criteria include items like?
    a. Back-up testing completed.
    b. Disaster Recovery plan updated?
    c. First level Service Desk staff trained.
    d. Level 2 support staff trained.
    e. Interface testing completed.
    f. Software licensing in place?
    g. Parallel runs completed?
    h. Operations procedures updated?
    i. Known problems reported to Service Desk?

14. Are there any current change control operational issues?
15. What is the promotion to production update failure rate?
16. Is there a warranty period for production changes and releases?
17. How are urgent fixes managed?

Sample Task list

1. What is the level of risk of introducing errors or untested changes into the production environment?
2. What needs to be done to mitigate any risks?
3. Review the process for introducing urgent fixes.
4. Implement a CAB.
5. Review CAB submission guidelines.
6. Empower the CAB.

Part 15 - Disaster Recovery

The Best practice IT Standard is:

A detailed Business Continuity Plan (BCP) with a matching Disaster Recovery Plan (DRP) and a back-up site agreement. The BCP and DRP should at minimum have been paper tested several times.

Most of us think of a disaster as being a data centre that has been gutted by fire or hit by an aircraft, in other words, it's off the air. While these disaster types rarely happen, flooding however is a common cause, as is power outages, that's when the generators don't kick in (murphy's law), sabotage is another and data corruption is a big contender. Each of these can have catastrophic consequences for a business. Back-up data centres are the best protection you can get, and then they are only as good as the WAN link that connects them, and they can fail when needed (murphy's law again). It's all an insurance game where by and large you get what you pay for.

However, when the crunch comes, only people can recover systems and restore businesses. The trouble is there is very little sensible information prepared in advance, and what there is must be kept current. Being prepared (defeating murphy's law) usually means that you won't suffer a disaster; but you must have a plan.

Consider this table below. Prepared by an enterprising guy for a SharePoint application, this small example is a good reminder that disasters can start from little things and have significant effects.

Dependency	Assumptions
User Interface / Rendering Presentation components	• Users (end users, power users, administrators) are unable to access the system through any part of the instance (e.g., client or server side, web interface or downloaded application). • Infrastructure and back-end services are still assumed to be active/running.
Business Intelligence / Reporting Processing components	• The collection, logging, filtering, and delivery of reported information to end users is not functioning (with or without the user interface layer also being impacted). • Standard backup processes (e.g. tape

	backups) are not impacted, but the active / passive or mirrored processes are not functioning. • Specific types of disruptions could include components that process, match and transforms information from the other layers. This includes business transaction processing, report processing and data parsing.
Network Layers Infrastructure components	• Connectivity to network resources is compromised and/or significant latency issues in the network exist that result in lowered performance in other layers. • Assumption is that terminal connections, serially attached devices and inputs are still functional.
Storage Layer Infrastructure components	• Loss of SAN, local area storage, or other storage component.
Database Layer Database storage components	• Data within the data stores is compromised and is either inaccessible, corrupt, or unavailable
Hardware/Host Layer Hardware components	• Physical components are unavailable or affected by a given event
Virtualizations (VM's) Virtual Layer	• Virtual components are unavailable • Hardware and hosting services are accessible
Administration Infrastructure Layer	• Support functions are disabled such as management services, backup services, and log transfer functions. • Other services are presumed functional
Internal/External Dependencies	• Interfaces and intersystem communications corrupt or compromised

Figure 5. Alexander Windel, Senior Microsoft Premier Field Engineer.

To be prepared, at a minimum you need

- A disaster recovery plan (DRP) and a business continuity plan. (BCP).
- Determine the Maximum Tolerable Downtime (MTD) for each application.
- Determine a reasonable Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each application.
- Sort applications into MTD or RTO order.
- Develop priorities and RTO's.
- Develop recovery strategies for each application.
- Prepare a hardware inventory (e.g., servers, desktops), applications and data inventories. Make sure that all the back-ups are working. Develop a list of critical applications and data and the hardware to run them. Make sure that application copies are available for re-installation on replacement equipment. Develop a priority list of hardware and application restorations.
- Create an emergency response team.
- Create procedures for declaring a disaster.

- Develop an emergency communications plan.
- Investigate alternative back-up data centres and or processing alternatives.
- Document the DR plan.
- Practise paper based dry runs of the DR plan and emergency response teams' procedures.

Some business applications cannot tolerate any downtime

They make use of a back-up data centre that can handle all their data processing needs, they run paralleled data mirroring between the two centres, this is a costly solution that only larger companies can afford.

However, there are other solutions available for small to medium-sized businesses with critical business applications and data to protect. Many companies have access to more than one facility. Hardware at an alternate facility can be configured to run similar hardware and software applications when needed. Assuming data is backed up off-site or data is mirrored between the two sites, data can be restored at the alternate site, and processing can continue.

Cloud-based disaster recovery as a service (DRaaS), WAN optimized replication, for highly efficient use of backup storage is growing in popularity, especially among SMBs and mid-sized organizations. The service is based on the protected capacity of your cloud platform and stores a configurable number of daily, weekly, and monthly backups for one base price.

Some vendors provide "hot sites" for IT disaster recovery. These sites are fully configured data centres with commonly used hardware and software products. Subscribers may provide unique equipment or software either at the time of a disaster or store it at the hot site ready for use.

Performance Questions

1. Is there a BCP in place?
2. Is there a DR Plan in place?
3. Have the plans been paper tested by the disaster recovery response team?
4. What kind of back-up, alternate site arrangement is in place?
5. What is the current level of risk?
6. How do you rate your back-up provider?
7. What fundamental rights do you have under the back-up agreement?
8. If the back-up site is a shared outsourcers site, what rights and privileges do you have?

Sample Task list

1. Conduct a risk analysis.
2. Investigate what level of DR you need.
3. Work with the business to build a BCP.
4. Form a DR response team.
5. Paper test DR plans with response team.
6. Determine further works required and scope out.
7. Breakdown the scope of works to task level, ready for loading into the change management project schedule.

Part 16 Architecture and Diagrams
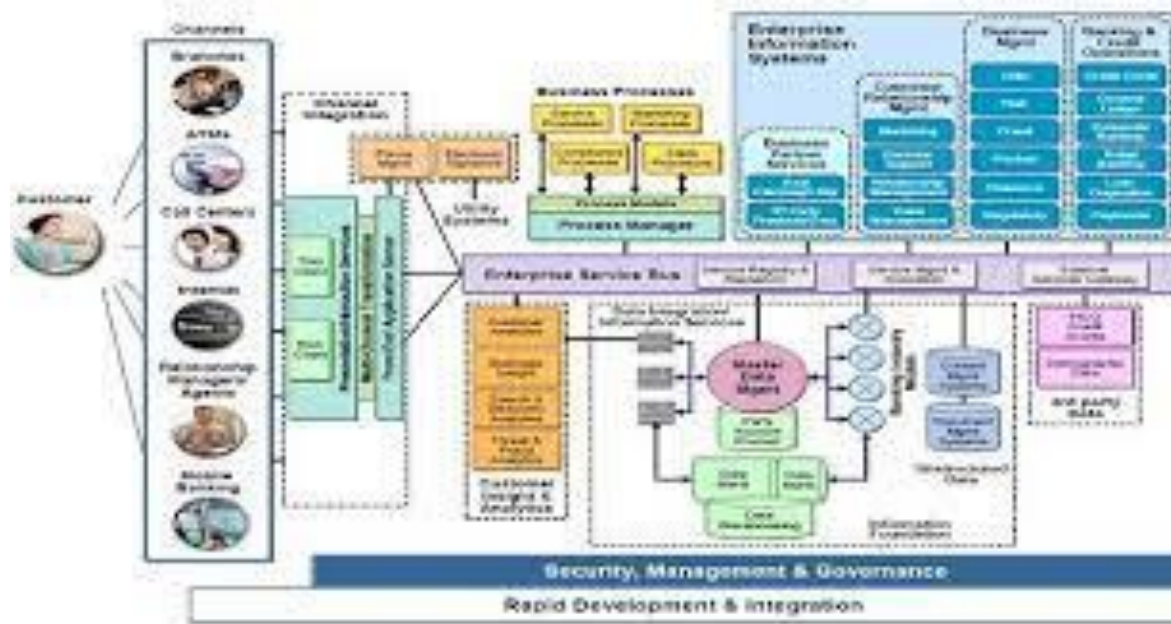
Architecture

The Best practice IT Standard is:

An architecture team that owns data, infrastructure and applications architectures supported by architecture guidelines and a technical architecture catalogue. A technical architecture catalogue is essential; it helps with products standardisation, reduces product redundancy, sets product strategy and guides purchasing decisions. Architecture principles are also required.

Not every IT department has an architecture function, although at minimum IT architecture works on a set of principles that guide the use and deployment of all IT resources and assets across the company. They are developed to make the IT environment as productive and cost-effective as possible. The principles are used in a several different ways.

To provide a framework within which the company can start to make conscious decisions about IT.
Formulation of hardware and software evaluation criteria.
Assessment of existing IT Systems and future strategic product mix.
Cost Savings from deploying standardised, integrated hardware and software.

When an architecture function is absent, the lack of corporate data models and applications architecture constrains ITs ability to support the business decision making process adequately. IT becomes focused on responding to tactical business requirements creating a discontinuity between business and technical strategy.

There are three types of IT architectures and guidelines.

1. Application. Applications guidelines and catalogue.
2. Technical.   Hardware, Server, Desktop and Systems software guidelines.
3. Data.   Database Tables, Records, Fields, Naming definitions/dictionary.

Performance Assessment

1. Is there an architecture function or team?
2. Are there technical architecture diagrams in place?

3. Are there applications architecture diagrams in place?
4. Are there data architecture diagrams in place?
5. Is there a technical products catalogue in place?
6. Who does the architecture manager report to?
7. How is work gated through architecture for approval?
8. How is architecture integrated with team processes?

Are technical specifications documented? (These should define IT hardware configurations, systems and applications software configurations and supporting network configurations.
Is the overall technical architecture of a solution matched with the defined requirements?
Are projects supported with an end-to-end design study, to cover areas such as performance, recovery, disaster recovery and operability?
Are project technical risks assessed?

Sample Task list
1. Document technical procedures for systems back-up and recovery.
2. Establish an Architecture function.
3. Review IT management team composition to add an Architecture Manager.
4. Include a process to technically assure subcontractors development and test environments.
5. Define and implement a means of performance prediction and performance management for new systems.
6. Determine further works required and scope out.
7. Breakdown the scope of works to task level, ready for loading into the change management project schedule.

Diagrams
The Best practice IT Standard is:
The use of diagrams to assist the work of different teams. Diagrams provide visual references that are quick to interpret and are particularly useful for planning purposes such as equipment changes, new deployments, capacity and topology management. With an architecture function in place, diagrams can be produced using common standards and toolsets. Otherwise, teams can develop their own diagrams using a common tool such as 'Visio'. Diagrams are only useful if their level of detail is fit for purpose, and they are kept up to date; otherwise, their value is questionable.

Diagrams are produced in three levels with each level being an explosion of the former level.

1. Level 1.   Highest level, macro view, used for scoping and high-level planning.
2. Level 2.   Intermediate level, detail view, used for deployment planning.
3. Level 3.   Lowest level, maximum detail view, used for capacity management.

Performance Questions
1. Are there applications development diagrams?
2. Are there WAN / LAN diagrams?
3. Are there infrastructure server diagrams?
4. What tools are in use to create diagrams?
5. Are diagrams up to date?
6. Are diagrams available in all three levels?
7. Determine diagramming needs of each team.
8. Who owns the production and maintenance of diagrams?

Sample Task list

1. Appoint one or more diagramming resources as roles.
2. Investigate a standard diagramming tool.
3. Produce diagrams.
4. Add a step to appropriate processes to update diagrams.
5. Consider having architecture own the tool and diagramming standards.
6. Determine further works required and scope out.
7. Breakdown the scope of works to task level, ready for loading into the change management project schedule.

Part 17 - Data Centre and Operations

The Best practice IT Standard is:

Protection of data centre assets, completion of the nights batch processing, successful completion and verification of back-ups and on-line systems availability ready for the next day's business opening hours. The performance and capability of data centre operations are assessed every night and every morning. Production and development batch processing, scripts, job scheduling and job run sheets are assessed daily. Confirmation of database availability, completion of overnight back-ups through to the successful initiation of on-line production systems ready for business opening hours is also assessed daily. As a result, a thorough health check is usually not warranted unless there have been recurring problems.

Performance Assessment

1. Data Centre Security.
   a. How often are physical security systems tested?
   b. Video Tests?
   c. Man Traps/Bollards?
   d. Doors/Vents/Fan exhaust?
3. Redundancy.
   a. How often are water and back-up water systems checked?
   b. How often are back-up communications links checked?
4. Is the data centre manual up to date in respect of?
   a) Changes to movement sensors, alarms.
   b) Intruder monitoring, external security services.
   c) Electronic access controls.
   d) Off-site media transport and storage.
   e) Air Conditioning.
   f) Fire suppression systems.
   g) Generator testing.
   h) Equipment maintenance schedules.
   i) UPS and generator testing.
   j) Surveillance checks.
   k) External physical penetration testing.

l)   Review the data centre maintenance procedures.
m) Review the data centre operations manual.
5. Operations.
   n)   If there are processing problems, what tend s to be the most common cause, 1) change control, 2) job scheduling, 3) run sheets, 4) other?
   o)   Is the operator's manual up to date?
       a)   Manage and schedule batch jobs.
       b)   Batch job dependencies.
       c)   Printer definitions and queue management.
   p)   Is an operator (hand over) diary in use?
   q)   Who manages data restoration services?
   r)   Who creates the application production scheduling calendar?
   s)   When was the last disaster recovery plan walkthrough?

Sample Task list

1. Determine what risks are evident or may exist in the data centre physical and logical environments?
2. Arrange an assessment of physical security.
3. Are support facilities being regularly tested? (Back-up communications, generators, water supply, fire suppression).
4. Determine further works required and scope out.
5. Breakdown the scope of works to task level, ready for loading into the change management project schedule.

Part 18 Technical Resource Management
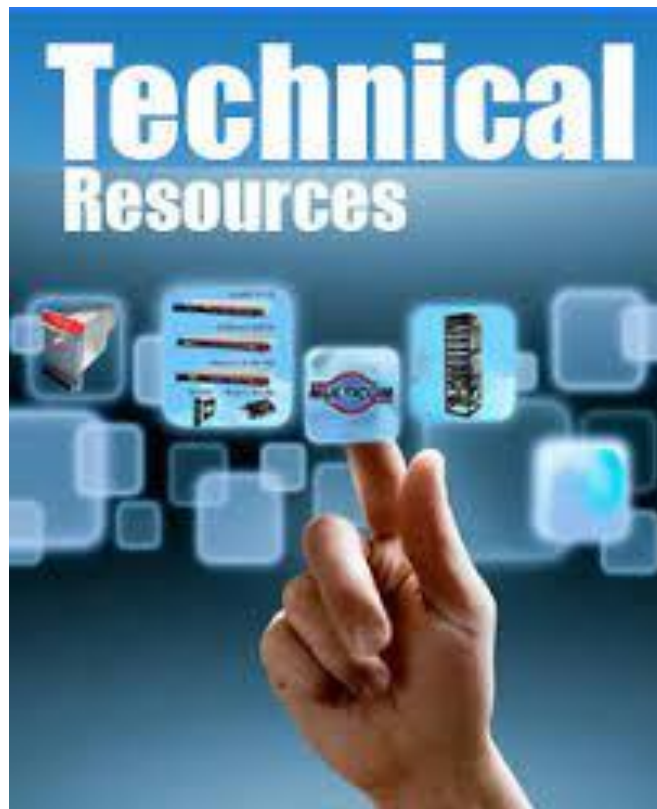
The Best practice IT Standard is:

The best practice standard is a resource management approach that uses minimal technical and applications resources. This means that available resources require skillsets and knowledge to be able to service production support and projects needs at the same time.

Projects and production support are equally important. One keeps the production environment running, the other fosters business growth, preferably they should not be traded off against each other.

Problem

- Projects to meet their deadlines require dedicated resourcing with specific skillsets and knowledge.
- Production support to resolve production issues requires resources with specific skillsets and knowledge.
- Required skillsets and knowledge are usually in short supply.
- A resource conflict occurs when production support and projects need the same resource at the same time. Production support takes precedence which causes project schedule slippage.
- The question is how to resolve the resource conflict.

Options

- Have technical and applications resource pools large enough to support both activities at the same time. (This is costly, wasteful and project needs are not constant).
- Backfill production support or project needs with contractors. (This is Inefficient and costly).
- Schedule resources part-time on projects hoping to satisfy both activities needs. (Does not solve the resource conflict issue and production support wins).

- Do forward resource planning and bring in and train contractors to work on projects. (Projects usually require specific systems and applications skills and knowledge that contractors may not have).

Best practice options

- Review the Projects Master Plan for the next 12 months and employ entry level or inexperienced resources to supplement the more knowledgeable production support staff.
- Train entry level staff on as many production support activities as possible.
- Reduce, remove, automate as many as possible, manual production support activities including the use of scripts.
- Resolve all production support recurring problems.
- Introduce a Rule of 'fix problem once'.
- Train more production support staff on supported systems and applications.

Performance Assessment

1. How are resource conflicts resolved?
2. Are skilled resources dedicated to projects?
3. If you have a staffing shortfall what is its nature and where is it?
4. How many contractors do you currently have?
5. What is the longest period a contractor has been on board?
6. In which areas are you using contractors?
7. Are contractors asked to document their work thoroughly and is this enforced?

Sample Task list

1. Bring in more entry level staff.
2. Backfill and reduce reliance on contractors.
3. Review staffing needs by team.
4. Have contractors document their work and enforce it.
5. Have contractors' mentor and train staff and enforce it.
6. Determine further works required and scope out.
7. Breakdown the scope of works to task level, ready for loading into the change management project schedule.

End of Series Summary

1. Introduction

My work experience has provided me with a unique perspective on IT as a result of having managed every IT Team. That is, I have been a CIO, IT Manager, Infrastructure Manager, Applications Development Manager, Technical Services Manager, Service Delivery Manager, Service Desk Manager, Data Centre Manager, Architecture Manager, Project Office Manager, as well as Database and Networking Manager. Many of these positions I have held more than once. I have managed 50 staff and 1000 staff. I have also been a Programmer and a Systems Analyst, starting my career with the build of an MVS Mainframe Data Centre. I contribute my success to this breadth and depth of experience.

2. Performance Housekeeping

The bottom line is that this background allowed me to form a unique appreciation and understanding of how an IT department works and how to get it to work at its best. It also allowed me to determine what essential Performance Housekeeping activities are required to obtain maximum performance within each IT Team and achieve the following benefits:

Best Practice IT Standards

From my work I developed the Best Practice IT Standards that came about as a result of taking note of what worked best in all of the IT departments, I worked in. They became part of my Change blueprint for addressing operational performance issues and bringing about improvements. Over time all IT departments suffer from a form of entropy in their performance capability. Progressively they become more complex, run a much higher risk of errors, suffer a decline in technical performance, they lose their IT memory and incur increasing operating costs, all as a result of doing nothing in particular other than running the day to day.

3. A better IT Management model

The model I prefer and the one I have always implemented is an IT Performance Management model. I always moved quickly to implement this model which is a hybrid of the older Traditional and newer Transformational - management models. The model looks like this:
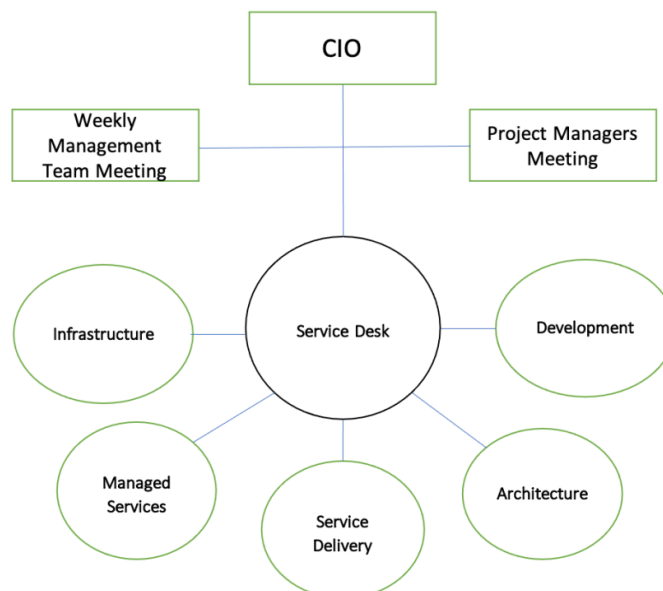
4. Four things that contribute to 80% of IT problems

There are four problem areas common to virtually every IT department that account for around 70 to 80% of all of ITs problems and resource usage, those areas are:

5. Workload Management.

6. The Service Desk.
7. Process and Intranet.
8. Managed Services.

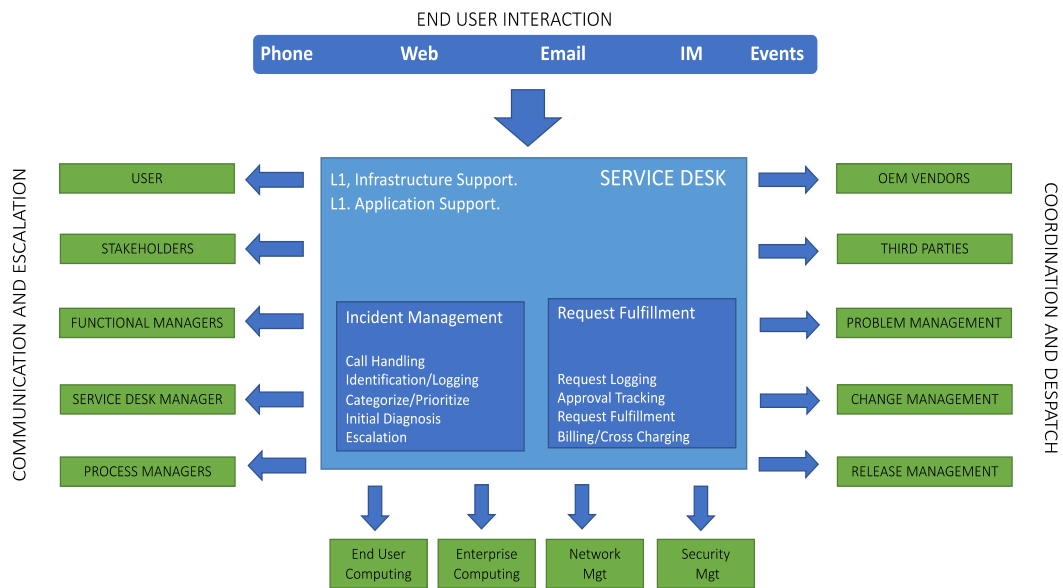## 5. IT Function matched with its Best practice IT Standard

IT Function	Best Practice IT standard
Service Desk and ITSM	ITIL compliant Service Desk application and ITIL/ITSM Service Management framework.
Workload Management.	End-to-end process comprised of Gating, Work Management, Work Classifications and Management Reporting.
Process and Intranet	All work to be process driven, with documentation management and templates managed in accordance with the Capability Maturity Model (CMM Level 2). All process, how to guidelines and other documentation to be sourced only from an Intranet. All documents to be baselined with a single production version. The Intranet acts as the IT memory and single source of truth
Managed Services	Contract manager with a outsource diary, detailed knowledge of SLAs and contract schedules and weekly contract reviews.
Staff Training	Vendor product training.
Infrastructure.	Fleet upgrade strategy.
	Capacity Management function for servers and network.
	Desktop refresh strategy.
	Standard Operating Environment (SOE).
	DBMS management function.
	Server performance management function.
	Formal naming standards for servers and network hardware.
Applications Development. Methodologies.	Tailored SDLCs, Applications development suite, Documented legacy applications. Documented methodologies, guidelines and policy on use of scripts.
Projects.	End to end project management delivery process with supporting templates, guidelines and reporting documents.
Project Management Office.	Active PMO (as against passive), project management processes, templates and guidelines.
Quoting, Scoping, Estimating.	Services catalogue, standard quotation template.
Security.	Five levels of security management with penetration testing.
Change Control.	Change Advisory Board (CAB) with evidential submission criteria.
Disaster Recovery.	BCP, DRP. Testing, back-up site.
Architecture.	Application. - Applications guidelines and catalogue. Technical. - Hardware, Server, Desktop and Systems software guidelines and catalogue. Data. - Database Tables, Records, Fields, Naming definitions, guidelines and dictionary.
Diagrams.	WAN, LAN, Server, Architecture.
Technical Resource Management.	Minimise number of technical resources, maximise number of project resources.
Data Centre.	Asset protection, error free batch processing, on time on-line availability.
Tools and Utilities.	Vendor supported with OS, systems software and applications upgrade paths.

6. Service Desk and ITSM
You can't manage what you can't measure
The IT Service Desk is the principal interface between IT and the business. The business mostly rates its IT experience based on the performance of the Service Desk. For IT on the other hand, the Service Desk is the

window into the business in terms of the number and nature of problems it is experiencing and how efficiently they are resolved.

7. Process and Intranet

Process maxim: If it's not written down, it doesn't exist

The best practice standard is the use of a document management system, a process driven environment, (wherever feasible, for all work practices) and use of a standard, common document template for process, how-to guidelines, and other documentation. The template must adhere to documentation management principles. All documentation types are to be stored on an intranet.

8. Managed Services

"We do your mess for less"

I have been an Outsourcing Contract Manager for several large, complex Financial Services IT contracts. The key lesson I learnt is that unless carefully and skilfully managed, the promised services and improvements are not always forthcoming. This is despite the fact that the Outsourcing business model is a good one where the provider can make use of an IT shared services to standardise the clients' environment, reduce their cost of delivering services and make it easier to achieve SLAs. But not all contracts or clients are moved under shared services as this involves up-front costs for the provider, rather the clients' services are left as is (no change to platforms or software) with reduced chances of achieving SLAs. This is where the Outsourcer saying of "We do your mess for less" comes from.

9. Staff Training

I am a great believer in keeping staff training levels up to date. Unfortunately, in times of cost cutting and budget restraints, training is usually the first cost centre to be cut, this I have always resisted as the benefits of keeping product training up to date are substantial. The importance of training cannot be overstated. Companies invest large amounts in hardware, software and services but often fail to train or fall behind in the training of their staff in these products (hardware, systems and applications software, software suites and utilities). Failing to train staff on products they use is simply an inefficient and often costly use of those assets. Having untrained staff using IT products is also a risk, and when training on new technologies falls behind, capability and productivity suffer as does staff morale and the professionalism of the IT department.

10.Infrastructure

There is a saying that CIOs lose their jobs because of bad Infrastructure Managers. I add to this that the Infrastructure Managers are bad because they fail to understand the basics and that the devil is in the detail. I have managed many Infrastructure departments small and large, and whilst I can say that they are indeed a challenge, if you put the basics in place, they are easy to manage. IT Infrastructure is complex and critical to all IT operations, consisting mainly of Service Delivery, Installations, Maintenance, SOEs, Server and Desktop refresh strategies and Networks and Communications. Pay attention to the basic needs of these and things look after themselves.

The Best practice Standard is 99.9% Server and Network availability, a hardware fleet upgrade strategy driven by applications capacity needs, response time objectives, systems capacity management requirements, hardware failure rates and fleet ageing, A systems software upgrade strategy and desktop refresh strategy are also required.

11.Applications Development

7. A thoroughly documented and tailored where appropriate, development lifecycle methodology. (Systems Development Lifecycles-SDLC) with associated how-to guidelines and procedures.
8. A vendor supported, integrated applications development toolset.
9. Development and test databases refreshed daily.
10. As the applications portfolio is usually a mix of packaged solutions and in-house developments, both require thorough documentation, especially legacy applications.
11. Development work like enhancements requires rigorous functional gap analysis and review of business processes before work is undertaken.
12. The use of scripts is minimised as they tend to organically grow which makes them problematic and requiring manual intervention to run.

12.Security

Five levels of managed security with penetration testing, underpinned by CARTA (a strategic approach to information security that was introduced by Gartner in 2017).

7. **IT security**. Refers to securing digital data, through computer network security. It is accountable for preventing unauthorized access to organizational assets such as computers, networks, and data and it maintains the integrity and privacy of corporate information and the blocking of hackers.
8. **Information security**, on the other hand, refers to the processes and tools designed to protect business information from unauthorised access.
9. **Network security**. Used to prevent unauthorized or malicious users from getting into a network, ensures that capacity, reliability, and integrity are not compromised. The Network security risk profile increases as business increase the number of endpoints and migrates services to the public cloud.
10. **Endpoint security**. Protects mobile phones, laptops, and desktops. It restricts access to malicious and typically includes malware protection and device management.
11. **Internet security**. The protection of information that is sent and received in browsers. Includes network security involving web-based applications. These protections come in the form of firewalls, anti-malware, and anti-spyware, ransomware.
12. **Cloud security**. Applications and data held in a cloud-based data centre. The usual security measures do not protect users who are connecting to the internet. Cloud security secures software-as-a-service (SaaS) applications and the public cloud.

13.Projects and Project Management Office

How do Projects Fail? (One day at a time)

A rigorous end to end, project management lifecycle with supporting how-to guidelines and templates.

Is an active PMO. An active PMO receives standardised reporting from project managers, provides common traffic light style management reporting to the business and IT, actively monitors and polices project progress

against cost and schedule and holds project managers accountable for their performance. Additionally, it provides a suite of project management processes, templates and how-to guidelines, such as how to estimate, create a schedule or produce a weekly progress report. It provides clearly defined project roles and responsibilities and an end-to-end projects delivery process that combines business and IT. An active PMO should be considered once the average number of small to medium-sized projects exceeds 15 per annum.

14. Quotations and Change Control

A quotation template that formalizes and integrates the three processes of scoping, estimating and quoting. The quote requires the scoping of hardware, software and services with prices from an IT services catalogue and/or an architecture products catalogue. The quote should have a fixed validity period.

Around 50% of business work requests disappear after a proper quotation has been prepared. Using the 'Mandatory, Highly Desirable, Nice to Have' technique when determining scope in conjunction with a IT services catalogue improves accuracy and rapidly speeds up the quoting process.

15. Disaster Recovery

A detailed Business Continuity Plan (BCP) with a matching Disaster Recovery Plan (DRP) and a back-up site agreement. The BCP and DRP should at minimum have been paper tested several times.

Most of us think of a disaster as being a data centre that has been gutted by fire or hit by an aircraft, in other words, it's off the air. While these disaster types rarely happen, flooding however is a common cause, as is power outages, that's when the generators don't kick in (murphy's law), sabotage is another and data corruption is a big contender. Each of these can have catastrophic consequences for a business. Back-up data centres are the best protection you can get, and then they are only as good as the WAN link that connects them, and they can fail when needed (murphy's law again). It's all an insurance game where by and large you get what you pay for.

16. Architecture and Diagrams

An architecture team that owns data, infrastructure and applications architectures supported by architecture guidelines and a technical architecture catalogue. A technical architecture catalogue is essential; it helps with products standardisation, reduces product redundancy, sets product strategy and guides purchasing decisions. Architecture principles are also required.

Not every IT department has an architecture function, although at minimum IT architecture works on a set of principles that guide the use and deployment of all IT resources and assets across the company. They are developed to make the IT environment as productive and cost-effective as possible. The principles are used in a several different ways.

17. Data Centre and Operations

Protection of data centre assets, completion of the nights batch processing, successful completion and verification of back-ups and on-line systems availability ready for the next day's business opening hours. The performance and capability of data centre operations are assessed every night and every morning. Production and development batch processing, scripts, job scheduling and job run sheets are assessed daily. Confirmation of database availability, completion of overnight back-ups through to the successful initiation of on-line production systems ready for business opening hours is also assessed daily. As a result, a thorough health check is usually not warranted unless there have been recurring problems.

18. Technical Resource Management

The best practice standard is a resource management approach that uses minimal technical and applications resources. This means that available resources require skillsets and knowledge to be able to service production support and projects needs at the same time. Projects and production support are equally important. One keeps the production environment running, the other fosters business growth, preferably they should not be traded off against each other.