



NotesOn: An IT Executive’s Survey And Checklist – Part I

Introduction (V1.4):

This is Part I of IV of my IT Executive checklist, or survey list. It is focused on the first Overview of the company and its IT organization, its Infrastructure and its Software Environments and Tools used. Over the years I’ve worked in quite a few different IT groups, large and small. From experience I’ve learned that there are “things” I need to know almost as soon as I walk into an IT Group. This is a living “work in progress” document that is the result of my “need to know”. It will be upgraded and refined from time to time as conditions and “states of IT” change.

Introduction (V1.4):	1
Survey Checklist Usage:	1
Overview Section:	2
Company Overview – High Level:	2
IT Organization Structure Overview:	3
Infrastructure:	4
General Survey Questions:	4
Infrastructure – Specialized Equipment:	4
Infrastructure – Telecommunications:	4
Infrastructure – Data Center(s):	5
Infrastructure – In-house Testing Labs:	5
Infrastructure – Development Environments:	6
Infrastructure – QA Environments:	7
Infrastructure – Prod Environment:	8
Infrastructure – Disaster Recovery:	10
Infrastructure – Business Continuity Management:	11
Software Environments / Tools:	13
Operating Systems:	13
Database Servers / Engines:	13
Client-Server:	14
Web – Languages (Primary):	14
Web – Web Servers:	14
Web – App Servers:	15

Survey Checklist Usage:

This checklist is not a “one time” tool. It is certainly of great value when you are stepping into an new IT arena, but it can and should be also used iteratively. Take a fresh copy out from “time to time” and walk and talk your way through your IT group. When done compare the new results to prior versions. Note changes and non-changes. Note, also, what is missing that should be there, and vice-versa.





Except for the “Overview” sections, I have included a “value” column before each item for your use. I have not assigned or attempted to assign weights to these items as this is not a “concentrate on this first” list and any weights would be arbitrary. All items on this list are important.

The value column is merely a way to “grade” what is and isn’t working or is and isn’t present. Use any value range you wish, but I would suggest keeping it simple, at most a scale of 0, 1, 2, 3 with 0 being non-existent or “un-acceptable” and 3 being present or “acceptable” but it could be as basic as 0 and 1. One reason for keeping it simple is that when you are stepping into a new role you don’t, yet, have sufficient information, or experience, for proper, accurate, evaluations. That will come with time but as you can’t wait until you “know everything” before making a decision this survey and a simple grading scale will help to get you close.

While each CIO/CTO should use this list for his/her group, every executive and manager on the team should as well, as they too need to understand each area, each area’s scope and each area’s strengths and weaknesses. This is not a “top secret” document it is a survey and diagnostic document meant for use.

This checklist is broken down into several sections. It starts out at a high level and then drills down into more detail. Some of the data in these levels may appear to be redundant, but is not. It’s the difference between the 50,000 and the 500 foot levels.

Finally, remember to *look, ask, listen and verify*. And don’t forget to talk to your Techies.

Overview Section:

Company Overview – High Level:

This section provides a high-level overview as a reference point to the rest of the checklist.

Category	Notes
Mission Statement	
Products Produced	
Services Provided	
Calendar / Fiscal Year End	
Number of Business Units	
Number of Personnel	
National / International Locations	
Public / Private Company	
Pre-IPO?	





Out-sourced / Off-Shored	
Past Successes	
Past Failures	
Current critical issues	

IT Organization Structure Overview:

Your IT organization may not have personnel in all areas but the functions should be covered.

Team	# of Personnel	In Business Unit / Company / Location
Infrastructure - Data Center		
Infrastructure - Telecomm		
Infrastructure - Desktop		
Customer Relationship Mgt		
Business Analysts		
Project Management / PMO		
Security		
Database / System Administration		
Architecture & Development		
QA / QC (Testing)		
Systems Support		
Help Desk		
IT Risk Management		
IT Audit		
IT Finance		
IT HR		





Infrastructure:

We’re starting, at a detailed level, with IT infrastructure because it is the foundation for everything else in your IT group. One cannot assume it is present or present to a sufficient degree that you can “get, or keep, things cranking”. It may be, or some of it may be, but don’t assume. Look. Ask. Listen. Verify.

General Survey Questions:

Value	Question	Response
	Does an up-to-date System Map/Inventory List exist?	
	Is the Data Center(s) out-sourced or off-shored?	
	Is the Telecomm function out-sourced or off-shored?	
	Is Desktop support out-sourced?	
	Are there known performance issues?	

Infrastructure – Specialized Equipment:

Value	Item	Response
	Inventory control scanners / equipment in use	
	Document management scanners/mass storage in use	
	RFID chips in use	
	Mfg/Production monitoring sensors/equipment used	
	Security scanners/keypads/ID cards/etc. used	
	Wi-Fi networks used	
	Other:	

Infrastructure – Telecommunications:

Value	Item	Response
	Telecommunications systems In-House / Out-sourced	





	E-mail servers / systems	
	Phones / PBXs / systems	
	PDA / Blackberry / etc. systems	
	PTT / IM servers / systems	
	SharePoint servers / systems	
	Other:	

Infrastructure – Data Center(s):

Value	Item	Response
	Number of data centers	
	Data Centers In-house / Out-sourced	
	When was the last “true cost” developed?	
	Disaster Recovery/fail-over site(s) in place?	
	How often are tests done? (also see below)	
	Is the data center(s) secure?	
	How? When last audited? Who audited?	
	Is there adequate emergency power backup?	
	Do uninterruptable power supplies exist?	
	Do generators exist? Have they been tested?	

Infrastructure – In-house Testing Labs:

In addition to the “standard” Development, QA and Production environments it is often necessary to have a separate “Testing Lab” that emulates the “real world” in which IT products operate. This is especially true if the Data Center(s) has been out-sourced.





Value	Item	Response
	Does IT have adequate testing labs?	
	Are there test servers (database, app, web, etc.)?	
	Are there test desktop/laptop units (Wintel, Mac)?	
	Are all platforms available (UNIX, Windows, Linux, AIX, etc.)?	
	Is load/stress testing software used?	
	Is VM (Virtual Machine) Software used?	

Infrastructure – Development Environments:

The IT Development teams need a separate, isolated, development environment for each server type, operating system, and, potentially, version. Changes are never, ever, done directly to Production. Ever. Production data is never allowed on Dev servers. Ever.

Value	Item	Response
	Does IT have an adequate Dev environment of:	
	Application servers	
	Database servers	
	Web servers	
	File servers	
	Misc. servers (e-mail, FTP, etc.)	
	Are the Dev teams working on current S/W versions?	
	Is security maintained on these servers:	
	By department?	
	By project?	
	By function (DBA, PM, Sr. Developer, etc.)	
	By individual unique ID?	





	Do generic/batch ID's exist?	
	Is security too loose allowing anyone to change code?	
	Is security too tight making it difficult to work?	
	Does Security remove ID's when Dev members leave?	
	Are servers "security patched" regularly?	
	Is versioning control software used?	
	Are backups of all servers done nightly (at least)?	
	If Prod data is loaded into Dev is it scrubbed first?	

Infrastructure – QA Environments:

QA environments must exist. Do not ever use Production as a "test" environment. Unlike Dev, which can be scaled down, QA servers, etc., *must* duplicate the Production environment. In QA, "close enough" isn't. Ideally QA should have separate servers; you can share QA and Prod servers but this has increased risks. QA can have Prod data on it but scrubbing of PCI/PII data, etc. should be done to protect against security leaks.

Value	Item	Response
	Is there a separate QA environment(s)?	
	Does it match, or closely match, the Production?	
	Is there an adequate QA environment for:	
	Application servers	
	Database servers	
	Web servers	
	File servers	
	Misc. servers (e-mail, FTP, etc.)	
	Are QA teams working on versions matching Prod?	
	Is security maintained on these servers:	
	By department?	





	By project?	
	By function (DBA, PM, Sr. Developer, etc.)	
	By individual unique ID?	
	Do generic/batch ID's exist?	
	Is security too loose allowing anyone to do updates?	
	Is security too tight making it difficult to work?	
	Does Security remove ID's when QA members leave?	
	Are servers "security patched" regularly?	
	Is versioning control software used?	
	Are backups of all servers done nightly (at least)?	
	Is QA audited for controls compliance?	
	Are critical QA servers at a distant Data Center from Prod?	
	If so, are they set up as DR failover from Prod?	
	Has failover / replication been tested?	

Infrastructure – Prod Environment:

Nothing, save for emergency fixes, should be done in Prod directly. All changes should be developed in Dev and tested and certified in QA. Access to Prod servers should be limited and monitored.

Value	Item	Response
	Is there a separate Prod environment(s)?	
	Does it match, or closely match, the QA environment?	
	Is there an adequate Prod environment for:	
	Application servers	
	Database servers	





	Web servers	
	File servers	
	Misc. servers (e-mail, FTP, etc.)	
	Are Prod teams working on versions matching Prod?	
	Is security maintained on these servers:	
	By department?	
	By project?	
	By function (DBA, PM, Sr. Developer, etc.)	
	By individual unique ID?	
	Do generic/batch ID's exist?	
	Is security too loose allowing anyone to do updates?	
	Is security too tight making it difficult to work?	
	Does Security remove ID's when Prod members leave?	
	Are servers "security patched" regularly?	
	Is versioning control software used?	
	Are backups of all servers done nightly (at least)?	
	Are backups stored at a distant location (see DR notes)	
	Is Prod audited for controls compliance?	
	Are critical Prod servers at a distant Data Center from QA?	
	If so, are they set up for fail-back from QA?	
	Has fail-back been tested?	



Infrastructure – Disaster Recovery:

Disaster Recovery is, or should be, part and parcel of every infrastructure project and every new system build and install. If you build it into the plan first it will be more cost effective than retrofitting (or the complete loss of systems and data). Some of this data has been touched on above but is localized here for continuity. **Note:** per earlier SEC findings and recommendations, DR data centers and/or backup tape storage should be at least 200 miles away from the primary production data center. Though this has been changed to a “risk zone” separation standard the original advice is still a fair absolute minimum distance guideline to which to adhere.

Value	Item	Response
	Data Center Emergency Power	
	UPS Systems in place and tested?	
	On-site generators in place and tested?	
	Fuel supplies on hand or available for 30 days?	
	Dual city power from separate sub-stations?	
	H/W systems replacement parts inventory?	
	Server/Applications priority recovery list?	
	Application priority list?	
	Server reboot sequence per app list?	
	Emergency Operations Center & Structure	
	Does one exist?	
	Coordination point with emergency services?	
	Preparedness drills?	
	Personnel rosters maintained off-site?	
	DR Plans maintained and stored off-site?	
	BC Plans maintained and stored off-site?	
	Emergency/Crisis Management	
	Internal Emergency teams?	



	Red Cross Emergency/First Aid training?	
	Adequate emergency supplies for 3 days +:	
	Water	
	Food	
	First aid kits / tools	
	Sheltering in place locations/supplies	
	Separate communications radios	
	Emergency update phone number	
	Emergency update web-site	

Infrastructure – Business Continuity Management:

Disaster recovery is a part of and a partnership with Business Continuity planning/strategy. DR takes care of IT systems. BC addresses the people, buildings, communications, processes, procedures, etc. At a high level:

Value	Item	Response
	If no plans exist, survey(s) need to be done including:	
	# of people per building	
	Basic services/facilities required	
	Telecommunications replacement	
	Critical IT systems list developed	
	Manual systems / forms / processes	
	Transportation needs determined	
	Security systems / people	
	BC management teams / alternates	
	BC activation plans / notifications	
	BC Plan exercises / table-top and dry-runs	





	If Business Continuity Plans exist ensure they include:	
	Manual processes determined	
	Manual forms determined and stored off-site	
	System tape backups stored off-site (minimum 200 miles away)	
	Critical operations determined / priority set	
	Critical IT systems determined / priority set	
	Several BC recovery sites scouted	
	Rental furniture / equipment sources located	
	Telecommunications replacement plan set	
	Security systems / people addressed	
	BC management team with alternates exists	
	BC activation alert system exists	
	Public notifications	
	Employee notifications	
	BC exercises done / plans updated	
	If IT DR plans / environments don't exist, get them done a.s.a.p.	
	If IT DR plans exist ensure they at least include as appropriate:	
	Hot Site locations, up and running and tested	
	Warm Site locations exist, meet critical needs	
	Cold Site location (build from floor up)	
	New server inventories exist locally	
	Current software versions are off-site	
	Backups of critical systems done and off-site	





	Backup restores tested regularly	
--	----------------------------------	--

Software Environments / Tools:

It is important to know what the “softer side” of IT is comprised of, is it a hodge-podge of types, versions, legacy, and cutting / bleeding edges? Is there a uniform purchase and acquisition strategy in place? The following lists are not complete (there are too many packages around for that) but it gives an indication of the typical range to look for. No order is implied on the lists, they are in the sequence I thought of them.

Operating Systems:

Value	Item	Response
	Microsoft Win2K, 2003, 2008 Server software	
	Microsoft XP, Vista, Windows 7, etc.	
	Mac OS / OSX	
	UNIX	
	Linux	
	AIX	
	Other:	

Database Servers / Engines:

Value	Item	Response
	MS SQL Server 2000, 2003, 2008, etc.	
	Sybase	
	Oracle	
	DB2	
	MySQL	
	PostgreSQL	
	MS Access	





	Filemaker Pro	
	Lotus Notes	
	Other:	

Client-Server:

Value	Item	Response
	Visual Basic (VB)	
	VB.Net	
	PowerBuilder	
	(C#, Java, etc. can also be used to develop C-S S/W)	
	Other:	

Web - Languages (Primary):

Value	Item	Response
	ASP.Net	
	VB.Net	
	C, C++, C#	
	Java	
	PHP	
	ColdFusion (also a Web App Server)	
	PowerBuilder (versions 9 and later)	
	Other:	

Web - Web Servers:

Value	Item	Response





	IIS (Microsoft)	
	Apache-Tomcat (Apache Software Foundation)	
	Sun Java Web Server	
	Google	
	Other:	

Web - App Servers:

Value	Item	Response
	JBoss (Redhat)	
	JRun (Adobe/Macromedia)	
	Websphere (IBM)	
	ColdFusion (Adobe/Macromedia)	
	Other:	

Part II will cover IT Methodologies, Application Suites and Environments, Reporting Tools, Data Transformation Tools, Batch Schedulers, Backups, Data Encryption, Controls / Security.

Part III will address Applications Environment, IT Personnel and Client Relationships.

Part IV will conclude the series by reviewing Risks / Risk Management, Budgets, Company Policies and Goals/Objectives.

Hope this helps.

DP Harshman

