

NotesOn: An IT Executive's Survey And Checklist – Part IV

Introduction (V1.1):

This is Part IV of IV of my IT Executive checklist, or survey list. It is focused on Risk Management and Risk Lists (including Disaster Recovery and Business Continuity), Budgets, Company Policies, and Goals & Objectives. 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, large or small.

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 (V1.1):	1
Survey Checklist Usage:	2
What Keeps You Awake At Night:	2
Risks Management:	2
Risks List – Baseline:	4
Quality of products / services	4
Critical IT Projects	5
IT Project Success / Failure Ratio	5
IT Project Key Success / Failure Factors (KSF / KFF)	5
IT Governance	6
IT PMO	6
IT HR	7
IT Supplier / Contract Management	8
IT Strategic Planning	8
IT Security	8
IT Infrastructure	9
IT Shared Services	9
IT Risks Management	9
IT Business Continuity Management	9
IT Disaster Recovery Management	9
IT Finance	10
IT Budget / Resource Management	10
IT Organization (overall)	11
IT Culture	11
Budgets:	11
Company Policies:	13
Goals / Objectives:	14

Survey Checklist Usage:

This checklist is not a “one time” tool. It is certainly of great value when you are stepping into a 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.

The entire 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.

What Keeps You Awake At Night:

Do not become myopic on the subject of Risk (ex: focusing solely on “hackers”). Threats and vulnerabilities exist both internally and externally but they all can be dealt with. First, determine what the risks are and then deal with them on a priority (risk/cost/benefit) basis.

Risks Management:

Risks need to be managed, always have been, always will be. To manage them you need someone(s) to do the management and a methodology, an approach. This first list addresses the management end.

Value	Item	Response
	Is someone(s) in the IT Organization responsible for Risks Management?	



	Has a Risks Management survey / analysis ever been done?	
	If so, does it seem to be inclusive?	
	Were the discovered risks incorporated into strategic and tactical plans?	
	Were the plans executed / followed up on?	
	Does the Risks Survey / Assessment process include the following elements in the decision matrix:	
	Threat recognition (what is out there that could cause harm)?	
	Potential vulnerabilities (what can be harmed on purpose or accidentally by a threat/threats)?	
	Likelihood of occurrence (best educated guess on the odds of an identified threat exposing an identified vulnerability = Y axis of heat map)?	
	Impact of a likely threat exploiting a likely vulnerability (the financial, legal, public relations impact of such an event = X axis of heat map)?	
	Does your Risks Management program include the following steps:	
	Identify potential internal and external risk areas (vulnerabilities)	
	Identify potential internal and external threats / threat sources	
	Analyze the potential risks (threat(s) vs. vulnerability(s))	
	Profile the potential risks (likelihood vs. impact)	





	Prioritize the risks based on potential impact	
	Review the Risks Survey per Risk Management’s RACI (R esponsible, A ccountable, C onsulted, I nformed) Matrix	
	Plan risk mitigation strategy(s)	
	Mitigate the highest risks first then repeat	
	Monitor the risks and mitigation plans	
	Repeat quarterly / semi-annually / annually	

Risks List – Baseline:

Any IT Risks Survey should include at least the following potential risk areas. The list is in the sequence I thought of them and I purposefully made no attempt to re-order them based on a “criticality” order. Your order will vary and you may wish to abbreviate, eliminate portions of and/or add potential risk items/areas. Note: in some cases I’ve included “pointers” to help focus attention on what constitutes a risk in that area:

Value	Item	Response
	Quality of products / services – is a concerted focus placed on and kept on quality?	
	Customer satisfaction (external)	
	Business units satisfaction (internal)	
	Competitor comparisons	
	Out-sourcing – has level of service and quality increased or decreased	
	Off-shoring – has level of service and quality increased or decreased	
	Vendor vs. In-House Applications (Buy vs. Build)	
	Do accurate / verifiable metrics exist to measure the above (vs. anecdotal “data”)?	





	Critical IT Projects (new and existing) – are they identified and risk assessed?	
	IT Project Success / Failure Ratio	
	Is success / failure defined (include Cost, Time, Quality, User Acceptance, Maintainability, and Sales and Repeat Business in the definition)?	
	IT Project Key Success / Failure Factors (KSF / KFF)	
	PLC (Project Life Cycle) Methodology(s) exists, is understood and is followed	
	SDLC (Software Development Life Cycle) methodology(s) exists, is understood and is followed	
	PLC and SDLC are understood as separate Life Cycles, i.e. not confused as identical concepts.	
	PM Training / Mentoring is done (including for IT Executives / Senior IT Managers)	
	Appropriate metrics exist and are used to monitor progress / success? [one gets what one measures so measure carefully]	
	Senior IT Mgt and HR focus on Technical / Managerial personnel retention (see <i>IT HR</i> section)	
	PMO / Portfolio Management – exists and contains appropriate functions (see <i>IT PMO</i> section)	
	Teams are built around project requirements (correct technical skills mix rather than silos):	
	IT team members are not “stuck” in one role only and forever?	
	Project team members held accountable for managing risks and attaining success, and	





	receive appropriate training and mentoring.	
	IT Team members provide critical support for what they've designed and built (support is not "someone else's" problem)?	
	Governance – processes, procedures, standards, oversight, etc. <i>in support of delivery and service</i> – exists (see <i>IT Governance</i> section)	
	IT Governance – does it exist as a living/breathing entity and function?	
	IT Steering Committee exists – has overall ownership of IT priorities:	
	Consists of key business leaders and IT management	
	Obtains consensus of IT's budget based priorities	
	IT Leadership Committee exists (key senior execs / managers) – has overall ownership of and oversight over:	
	IT Budgets	
	IT Suppliers / Contracts	
	IT Architecture / Standards	
	IT Security	
	IT Change Management	
	IT QA	
	IT Delivery / Support	
	IT Audit	
	IT HR	
	IT PMO – does it exist and does it have overall:	





	Ownership of Project Life Cycle – Intake / Initiation to Closeout (but not SDLC or SW Development PnP's):	
	Project Manager Management (but does not manage projects, that's Development's / Engineering's zone):	
	Administration	
	Training	
	Project Gate / Checkpoint Review Committee (but does not own QA/QC or IT Audit)	
	Strategic Planning Assistance (but does not own or do Architecture)	
	Application Inventory List	
	Project Monitoring / Reporting	
	Cost / ROI Tracking	
	Project Metrics	
	IT HR – does it exist as a focused function?	
	Is there for the employees as well as to protect the company?	
	Ensures growth / promotion paths exist for all IT personnel?	
	Ensures IT roles / titles comparable to industry standards?	
	Ensures IT salaries / bonuses competitive?	
	Ensures Performance Reviews:	
	are fact based and goals and objectives oriented?	
	are consistent across IT / Company?	





	can be appealed to a “higher authority”?	
	IT Supplier / Contract Management – does it exist and are the following minimum controls in place:	
	Reviewed by CFO / Finance	
	Reviewed by Legal	
	Purchase Requisitions verified against	
	Purchase Orders verified against	
	Purchase Order authorization process	
	Supplier / Vendor Solvency analyzed:	
	High risk suppliers / vendors identified	
	Alternative, lower risk, sources identified	
	IT Strategic Planning – does this function (developing and promoting the right goals for the future, the right tools and teams to get there) exist?	
	Takes input on bottom-up basis, requiring all levels to provide accurate data (i.e. not disconnected from “the troops”)	
	Plans communicated clearly and timely	
	IT Security – does this function (responsible for systems, data, infrastructure and IT employees) exist?	
	Helps enforce compliance with all IT Audit (SOX, PII, PCI, HIPAA, Safe Harbor) controls	
	Ensures Disaster Recovery / Business Continuity plans in place, maintained and tested	
	Ensures Building security in place and adequate	





	Ensures desktops / laptops secured and encrypted per IT Audit controls and Business Data Security levels	
	IT Infrastructure – does the function / role of building and monitoring company wide Data Center(s), Network(s), Desktop Support, Telecomm exist?	
	Infrastructure Inventory List	
	Scalability / expansion capability of	
	Energy efficiency of (ROI on Going Green)	
	IT Shared Services – does the function of developing and supporting enterprise software systems / services common across all/most business units exist?	
	Cost-Benefit ratio / ROI of Sharing	
	Credibility of IT organization	
	Security of (internal and external)	
	Disaster Recovery / Business Continuity planning and testing	
	IT Risks Management (see <i>Risks Management</i> list)	
	IT Business Continuity Management – does role exist and is it engaged in strategic and tactical planning	
	IT Disaster Recovery Management – does role exist and is it engaged in strategic and tactical (i.e. architectural) planning	
	Does a DR Systems Inventory List exist?	
	Have DR Tier (criticality) criteria been defined and agreed upon companywide?	
	Have most / all critical systems needing DR capability been identified?	
	Has each DR candidate been assigned a Tier / criticality value?	





	Do Tier 1 / most critical systems currently have a DR plan / architecture implemented? Has it been tested?	
	Is DR planning part of the architecture / design process for all systems, regardless of Tier value?	
	Is the DR server(s) for each application at least 200 miles away from the primary production server(s)?	
	Is DR data / status tracked as part of the Application Inventory List (see ... Checklist Part III – Application Inventory List)?	
	IT Finance (Budget / Cost / ROI Management):	
	Evaluates economic conditions / trends (projections vs. actual)?	
	Ensures focus is not too heavily on cost reduction and not heavily enough on ROI (i.e. slashing of costs no matter what)?	
	Approval authority over all significant project costs and all capital investments?	
	Oversight of Contract / Vendor management functions?	
	Oversight of Budget / Resource Management?	
	IT Budget / Resource Management (see also <i>Budgets</i> section):	
	Does the function exist in <i>each</i> IT group?	
	Does the data role up in a meaningful way (managers → directors → VPs → CIO / CFO)?	
	Is the budget planning process managed in a timely manner?	
	Is the approved budget managed against	





	actuals?	
	Is “burn rate” forecasting done and reported?	
	IT Organization (overall):	
	Is it tuned for success, i.e. focused on delivery and service?	
	Is it administration top-heavy (see ... Checklist Part III’s administration/technical ratio)?	
	Do redundant functions exist?	
	Do all IT members know their roles and responsibilities (vs. “hey you, do ____”)?	
	Have functions / roles been out-sourced and/or off-shored that shouldn’t have been?	
	Is the ROI on IT demonstrably present?	
	IT Culture – is it focused on empire building (i.e. heavy on politics and in-fighting) vs. building an empire (i.e. a single, focused, well trained, well organized team)	

Budgets:

Value	Item	Response
	IT Budgets are done on:	
	Calendar Year?	
	Fiscal Year (FY)?	
	If Fiscal, FY Begin Date is:	
	Are annual IT budgets:	
	done?	
	done in reference to a companywide Annual Operating Plan (AOP)?	





	done before the start of the new budget year?	
	done top-down / bottom-up / both?	
	cuts done with attention to delivery and services or are they “arbitrary” off-the-top reductions (ex: by percentage)?	
	reviewed and approved by IT Steering and Leadership Committees?	
	Are IT budgets based on:	
	estimated resource requirements (requires resource allocation / load balancing analysis)?	
	estimated upcoming project costs (requires approved new projects list and high-level expense / capital estimates)?	
	estimated extant system support / maintenance / licensing / software costs?	
	estimated infrastructure expansion / support costs (data center, desktop support, etc.)?	
	estimated telecomm expansion / support costs?	
	estimated outside services (legal, external audit, consultants / contractors not charged to a project, etc.) costs?	
	estimated overhead costs (upper management, travel, meals, sick days, vacations, training, books / publications, etc.)?	
	estimated promotion / merit increase / bonus pool costs?	
	Are project related costs tracked on an expense vs. capital investment basis?	





Company Policies:

I've touched on elements of this section elsewhere but those items are included here as well to retain proper an complete focus on the subject:

Value	Item	Response
	Does an Employee (HR) Manual exist? If so, is it required reading with employee certification?	
	For salaried?	
	For contractors / consultants?	
	For unions?	
	Does a Company Policy Manual exist, as separate from or included with the Employee manual?	
	Do the appropriate work-place safety (chemical, equipment hazards, etc.) manuals exist? If so, are they required reading with employee certification?	
	Do the following (operating and procedural) guides exist and are they used:	
	Telephone / AV systems: How To and Usage Rules?	
	On-boarding Checklist (for new contractors and employees)?	
	Employee orientation training / checklist?	
	IT Security Guidelines / Policies?	
	IT Audit Controls Guide / Training (as appropriate to position held)?	
	Business Applications User Training Manuals?	



Goals / Objectives:

We've touched on some of these elsewhere but, again, they are localized here to attain maximum focus:

Value	Item	Response
	Is an Annual Operating Plan / Annual Strategic Plan done?	
	If done, is the AOP used?	
	If done, is it compiled based on input from all areas of the organization?	
	Are the AOP steps and estimates reviewed against "actual" regularly? Annually? Ever?	
	Is IT plugged into all Company-wide initiatives while they are in the planning stages?	
	Is the company-wide AOP translated into Goals / Objectives for the entire IT organization?	
	Does each IT department / group align its goals and objectives to the IT organization's goals and objectives? Prior to the start of the year? Ever?	
	Is there an IT Steering Committee that helps to align, and maintain alignment of, Company-wide and IT goals and objectives?	
	What company initiatives are coming up that you and IT absolutely need to be aware of immediately?	

Part I presented the Overview section, Infrastructure and Software Environment / Tools.

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

Part III addressed Applications Environment, IT Personnel and Client Relationships.

Hope this helps.

DP Harshman