

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

Introduction (v1.3):

This is Part II of IV of my IT Executive checklist, or survey list. It is focused on a continuation of the Software Environments and Tools used, and then with Security, and IT Controls. 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 (V1.3):	1
Survey Checklist Usage:	1
Software Environments / Tools (cont’d):	2
Application Suites:	2
Reporting Tools:	3
ETL / Data Transformation/Integration Tools:	3
Batch / Job Schedulers / Distributed Resource Managers:	4
Backup Software:	4
Security - Encryption:	5
Data (In Flight):	5
Data (Landed):	5
Data Encryption / Protection Strategies:	6
Security – IT Controls	7
Sarbanes-Oxley (a.k.a. SOX):	7
PCI (Payment Card Industry) Data Security Standard:	9
PII (Personally Identifiable Information):	10
HIPAA (Heath Insurance Portability and Accountability Act):	13
Safe Harbor (European PII Data Safeguards):	13
Business Information Security Levels:	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.

Software Environments / Tools (cont’d):

Note: the software packages / utilities listed are in no particular order other than as I thought of them. Neither is usability implied.

Application Suites:

It is important to know how many application suites are already in place. There could be several. Large companies in particular will often have this issue, particularly if there are multiple business units spread out nationally and/or internationally. This is hardly an exhaustive list but, rather, a starting point and is subject to change.

Value	Question	Response
	SAP	
	Oracle	
	Sage	
	NetSuite	
	MS Dynamics GP	
	QuickBooks Enterprise (Intuit)	
	Other:	
	Other:	



	None:	
--	-------	--

Reporting Tools:

As with the case above, large companies may have multiple reporting tools. This is one area where standardization to avoid unnecessary licensing and support costs *may* come into play. Just make sure that you don't lose functionality in the process.

Value	Question	Response
	Business Objects	
	Crystal	
	IBM Cognos	
	Excel	
	Actuate	
	Other:	
	Other:	
	Other:	

ETL / Data Transformation/Integration Tools:

Unless you are a small business owner, which typically (though not universally) means you are dedicated to one business suite or even one office suite, you have had, have and will have different software packages wrapped around different database engines. You will also be extracting data from external providers and sending data to external receivers. One rule in IT you have been able to rely on, to date, is there are few to no standards between software suppliers or between businesses (though XML is helping). Therefore, sooner or later, you will need to extract data from one source, transform it into another format and export it to a different destination, hence: Extract, Transform and Load, also known as data transformation or integration.

Value	Question	Response
	Informatica	
	WebMethods	
	MS SQL Server DTS / SSIS (SQL Server 2008)	



	Talend	
	Other:	

Batch / Job Schedulers / Distributed Resource Managers:

Batch schedulers are the unsung heroes behind the scenes of most enterprise wide systems. A good quality scheduler can save hours of coding, hundreds of hours of manual processing, properly announce errors to appropriate support personnel, allow the defining of dependencies, etc.

Value	Item	Response
	Maestro (IBM Tivoli)	
	Cron (UNIX)	
	Windows Scheduler	
	VMS Batch	
	Automate7	
	Other:	
	Other:	

Backup Software:

There are almost as many backup packages / utilities as there are accounting packages. A few are listed below but it is hardly a complete list. The key questions are: does it work now, can data be easily found and restored from it in part or in whole, is it scalable, does it run across a wide array of platforms, what backup medias can it utilize, for enterprise systems is there a master control console/system administration level that allows monitoring of all backups and reporting of failures.

Value	Item	Response
	Acronis	
	IBM Tivoli Storage Manager	
	UltraBac	
	Symantec	





	Yosemite	
	OmniBack	
	Other:	
	Other:	

Security - Encryption:

It almost goes without saying that data and infrastructure security is now and forever a core function of IT. Long gone are the days of the innocent hackers as seen in the Disney-esque movies. There is a small percentage of not very nice people out there who steal and destroy because they think they can (and sometimes do). Security in the Internet-age is now a way of life and part of the cost of doing business.

Data (In Flight):

Value	Item	Response
	FTP (File Transfer Protocol) is NOT used—not secure	
	sFTP (secure File Transfer Protocol) or equivalent	
	PGP Encryption Software	
	Other in-flight encryption method(s) / utilities:	

Data (Landed):

Value	Item	Response
	Do the current versions of the QA and Production database have and make use of column and row level encryption? (Presumes Dev servers never, ever, have Production data on them.)	
	What software add-ons, if any, are in use to encrypt not only the databases but the database servers? (If the database server is wide open the database may be able to be hacked directly or indirectly)	





Data Encryption / Protection Strategies:

Value	Item	Response
	Is there an IT Security group / department? That is manned and funded?	
	Is a defense-in-layers strategy in place?	
	Has the architecture and security method(s) <i>ever</i> been audited/hacked by <i>external</i> security auditors?	
	Are the network servers (all types) encrypted? If not, what security measures are taken?	
	Are Firewalls in place, monitored and updated?	
	Are DMZ's in place and monitored?	
	Are virus scanners / spyware sweepers in place, monitored and updated?	
	Is a human being looking at the database and network monitoring reports? (Or do they go into an e-file somewhere never to be looked at until the auditors show up?)	
	Is security patching done on all servers on a regular basis based on security threat level? Are the patches tested before they're put into Production?	
	Are reverse-proxy servers and other similar means used to prevent direct access to internal data from external sources (i.e. no direct access is permitted)?	
	Are web pages serving up secure information using HTTPS rather than HTTP?	
	Are employee and contractor laptops permitted? If permitted are they scanned regularly?	
	Are in-place desktops/laptops scanned regularly for viruses and spyware? Are the scanners updated regularly? Are the desktops/laptops "locked down" to prevent general users from uploading personal	





	software?	
--	-----------	--

Security – IT Controls

There are a host of regulations regarding much of the information stored in business (and sometimes personal) systems. Their purpose is, primarily, to protect the public from mis-use of the information or from mis-representation of financial business information (in the case of S-Ox). These regulations were translated into a series of controls by regulation type that IT must apply under most circumstances. Make sure IT and IT Audit (if it exists) fully understand each of these control areas and how to implement and audit them.

I have tried to include the primary controls for each of the regulation types, but the lists are intended as prompters not as exhaustive / definitive legal representations; that would take a small book at least.

Note: in many cases the controls are redundant such that, for example, compliance with some PII controls also meets compliance regulations for PCI and HIPAA controls.

Sarbanes-Oxley (a.k.a. SOX):

SOX systems are those that materially affect the General Ledger and Financial Reports. The definition of “materially” is subject to discussion and change.

Value	Item	Response
	Networks processing / retaining SOX data are secure:	
	Firewalls / DMZs in use and monitored.	
	Anti-virus / spyware software in use and updated.	
	Network security tested regularly.	
	An inventory, with diagrams, exists of SOX data storage locations and is verified / updated regularly.	
	Separation of duties (access to Prod, update of executables, etc.) is maintained and monitored.	
	Change / Version control is in place, documented and monitored.	
	Proper testing and system owner acceptance is in place.	
	Emergency production changes are authorized,	





	tested and obtain system owner acceptance.	
	Problem / bug management is in place, documented and monitored.	
	Access control is maintained:	
	By role.	
	Each user must have a unique, non-generic, ID that is not shared. (Batch processing ID's must be approved and monitored and used for no other purpose.)	
	Passwords changed regularly, strong passwords required.	
	Access rights changed upon termination or role change.	
	Access to Data Center / physical servers controlled.	
	Access to Applications controlled and monitored.	
	Access to Dev, QA and Prod database(s) controlled.	
	Access logs / audit trails maintained and monitored.	
	Security breaches detected and reported.	
	System interfaces to/from are designed and tested to ensure completeness and accuracy of transmitted data.	
	Security patches kept current and tracked.	
	Vendors with data access provide SAS 70's.	
	SAS 70's reviewed and evaluated against company security requirements.	
	IT SOX Controls are certified by control owners.	
	IT SOX systems audited regularly.	



PCI (Payment Card Industry) Data Security Standard:

PCI controls revolve around the use and storage of Credit and Debit card information. These controls are very stringent and, in brief, violation could result in severe fines and/or use of and the rights to process credit/debit cards. An excellent starter reference is: https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf.

Value	Item	Response
	Networks processing / retaining cardholder data are secure:	
	Firewalls / DMZs in use and monitored.	
	Anti-virus / spyware software in use and updated.	
	Network security tested regularly.	
	An inventory, with diagrams, exists of PCI data storage locations and is verified / updated regularly.	
	PCI data stored no longer than necessary after authentication.	
	PCI data encrypted in-flight and when landed (includes servers, desktops, laptops).	
	Electronic access must be encrypted (SSH, HTTPS, etc.).	
	Access tightly controlled.	
	Access Controls:	
	Segregation Of Duties: PCI data restricted to need-to-see/know.	
	Users (internal and external) granted need-to-know access have been vetted / credentialed including criminal and credit checks. Re-vetting occurs regularly and routinely.	
	No generic ID's, each user must have unique ID that is never shared. (Batch processing ID's must be approved and monitored and used for no other purpose.)	



	Strong passwords in use and changed regularly (no vendor defaults must ever be retained).	
	Physical access to Data Center restricted and monitored.	
	Electronic access to PCI data (in databases or other forms) tracked via audit trails.	
	Electronic access points must be logged off automatically if left unattended for more than a reasonable / appropriate amount of time.	
	Removal of PCI data from premises and/or systems is monitored (if allowed or not); includes access to printers, PDF versions, or via removable media, etc.	
	Access terminated upon transition out of need-to-know role or termination.	
	Policies exist on distribution of PCI data (internally and externally) and are monitored.	
	Develop and maintain PCI security policies with applicable sanctions for violations.	
	Regularly assess risks (existing and new) and update policies and procedures as appropriate.	
	Suspicious / unauthorized access attempts or entries must be reported and investigations begun immediately and remediated as quickly as possible.	
	Training in PCI security policies implemented and for employees and contractors and refreshed regularly.	
	PCI controls audited regularly by internal audit and “qualified assessors”.	

PII (Personally Identifiable Information):

PII controls revolve around the use and storage of personal information other than PCI data, such as full name, home address, phone numbers, social security numbers, bank account numbers, medical data, place and date of birth, mother’s maiden name, passport data and so forth. It can also include business related information





such as work address, office numbers, office e-mail, ID numbers, pay/salary grades, salary, etc. These controls should be just as stringently monitored as SOX and PCI as the loss of PII data can be a national and potentially international Public Relations (and legal and financial) disaster.

Value	Item	Response
	Networks storing PII data are secure:	
	Firewalls / DMZs in use and monitored.	
	Anti-virus / spyware software in use and updated.	
	Network security tested regularly.	
	An inventory, with diagrams, exists of PII data storage locations and is verified / updated regularly.	
	PII data stored only when/where necessary .	
	PII data encrypted in-flight and when landed (includes servers, desktops, laptops).	
	SSN removed as a “referential key”, replaced with a non-related internal identification number.	
	SSN not stored in more than one location, and that is heavily encrypted and protected.	
	SSN never printed on reports, checks, ID cards, bar coding, etc.	
	When required to be present on a display, SSN masked and unavailable to unauthorized personnel.	
	Electronic access should be encrypted (SSH, HTTPS, etc.).	
	Access tightly controlled.	
	Access Controls:	
	Segregation Of Duties: PII data restricted to need-to-see/know (number one audit failure point).	
	Users (internal and external) granted need-to-know access have been vetted / credentialed including criminal and credit checks. Re-vetting occurs	





	regularly and routinely.	
	No generic ID's, each user must have unique ID that is never shared. (Batch processing ID's must be approved and monitored and used for no other purpose.)	
	Strong passwords in use and changed regularly (no vendor defaults must ever be retained).	
	Physical access to Data Center restricted and monitored.	
	Electronic access to PII data (in databases or other forms) tracked via audit trails.	
	Electronic access points must be logged off automatically if left unattended for more than a reasonable / appropriate amount of time.	
	Removal of PII data from premises and/or systems is monitored (if allowed or not);, includes access to printers, PDF versions, or via removable media, etc.	
	Policies exist on distribution of PII data (internally and externally) and is monitored.	
	Access terminated upon transition out of need-to-know role or termination.	
	Develop and maintain PII security policies with applicable sanctions for violations.	
	Regularly assess risks (existing and new) and update policies and procedures as appropriate.	
	Suspicious / unauthorized access attempts or entries must be reported and investigations begun immediately and remediated as quickly as possible.	
	Training in PII security policies implemented and for employees and contractors and refreshed regularly.	
	PII controls audited regularly by internal audit.	



HIPAA (Heath Insurance Portability and Accountability Act):

HIPAA controls revolve around the use and storage of personal medical information (a.k.a. Protected Health Information or PHI). The controls are not as clearly specified for HIPAA as for PCI and PII but, in general, they seem to be very similar (which makes sense). Clearly, a main focus of the HIPAA controls is access audit trails so it can be determined by whom a record(s) was accessed. One source on this subject that had some clarity is at: http://www.netwrix.com/download/Compliance/NetWrix_HIPAA_Compliance.pdf.

Value	Item	Response
	In addition to the above Network/Data Security and Access controls (assumed as a common-sense baseline):	
	Audit trails/logs must exist for each and every access of a PHI record (s). If non-electronic then a manual log must exist with appropriate information.	
	Audit trails/logs must include who, what, when and where. This includes administrative and user activity, such as:	
	Changes to critical data and/or security settings	
	Password changes + change authentication.	
	Access rights granted and terminated.	
	Audit trails/logs must be reviewed on a regular basis by appropriate authorized personnel.	
	Retention of all records and audit trails/logs for an extended period of time allowing reconstruction.	

Safe Harbor (European PII Data Safeguards):

If, your company deals with the European Union and if you store any PII information about folks in Europe on your computer systems that was collected in Europe, whether personal or business related (the definition is very broad), you may need to comply with Safe Harbor regulations. Below is a high level overview. More information may be found at: <http://www.export.gov/safeharbor/eu/index.asp>.

Value	Item	Response



	There are seven principles behind Safe Harbor:	
	Notice – notices must be sent to EU members describing what the data is used for	
	Choice – EU members must be allowed to choose whether their PII data may be used for the purposes described above in Notice	
	Onward Transfer – EU member data may not be transferred to another system unless adequate safeguard protections exist	
	Security – the company must take reasonable precautions to protect the EU data from misuse, loss, etc. [Note: no definition of “reasonable” exists so in the recent past the presumption has been that a proper implementation of the PII controls satisfy the requirement. Confirm with your Legal / Audit groups.]	
	Data Integrity – the data must be accurate, complete and relevant to the use(s) described in the Notice.	
	Access – the EU member has the right to view their information stored in the non-EU system and request any incorrect/incomplete information be corrected.	
	Enforcement – the company possessing the EU data must implement mechanisms to address and resolve any EU member complaints about their data, to ensure the Safe Harbor principles are implemented and to remedy any compliance failures. This includes providing self certification letters.	

Business Information Security Levels:

Finally, after protecting everyone else’s information you also need to protect your own company’s. A security level scheme somewhat like that below may be appropriate. Each level is defined, primarily, by the level or degree of access permitted and distribution allowed:





Value	Item	Response
	Level 1 – Public Information / Broad Distribution	
	Level 2 – Company Access / Limited External with approval. Contains low level proprietary and/or day-to-day information not generally distributed to the public. May be distributed to vendors / partners with approval.	
	Level 3 – Confidential Information / No External Distribution, Limited Need-To-Know Internal Distribution. Contains confidential information that could have adverse affects on the company if prematurely released or made known in an inappropriate manner.	
	Level 4 – Restricted Access / No External Distribution, Very Limited Need-To-Know Internal Distribution. Contains substantial, critical proprietary information and or far-reaching plans and projects that could have a detrimental effect (financial, PR, legal, etc.) on the future of the company if released prematurely or in an inappropriate manner.	

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

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

