IT SYSTEMS CHECKLIST
Periodical Situation Analysis

1	General Responsibilities	Evaluation	☺	😐	☹	Remarks	AVG
1.1	The IT Manager is responsible for ALL of the following Information Systems: PMS, B/O, POS, LAN & S&C (through discussion)	Satisfied		75			90.00%
1.2	The IT Manager is responsible for all other Information Systems used within the hotel which include: PABX, Call Accounting, Voice Mail, In-Room Entertainment, Personnel, Payroll, Engineering & Locking Systems (not the day-to-day running) (through discussion)	Very Satisfied	100				
1.3	There is a designated back-up person for each system in 1.1 + 1.2 to take responsibility in the IT Manager's absence (talk to designated back-up person)	Very Satisfied	100				
1.4	If yes to 1.3 confirm if they are trained and/or have experience in the essential tasks (e.g. back-ups, trouble shooting, contact support, etc.) (see training records)	Very Satisfied	100				
1.5	A 3 year computerisation plan for the hotel has been prepared by the IT Manager (with budgetary figures) in order to provide compliance & adequate replacement (based on hardware inventory) & upgrade. Plan has been agreed with GM & Financial Controller & funds are included in the FF&E budget. (5-year plan & FF&E Budget)	Satisfied		75			
1.6	The IT Manager takes responsibility for his own department budget and is able to explain any deviation to the budgeted figures (Financial statement on file. IT Manager to explain deviation(s))						
2	**Administrative Tasks**	**Evaluation**	☺	😐	☹		**AVG**
2.1	A full up-to-date inventory exists for all Hardware, incl. modems, hubs, monitors etc. detailing Purchase date & Price, Serial Number, Model Number, expected replacement dates, & maintenance where applicable. This is to include all telecommunications related computer equipment. (Inventory list, spot check)	Satisfied		75			61.11%
2.2	A full listing exists, backed up by original licenses or invoices, detailing all software licenses including purchase date & price (where applicable), license code, release number & maintenance (where applicable) (Operating systems, Opera, Fideliol, SUN, Vision, FBM, Office Applications etc.) (Inventory list, spot check)	Very Satisfied	100				
2.3	A full inventory exists detailing, per PC, all software applications installed including location & release number (Inventory list, spot check)	Satisfied		75			
2.4	An up-to-date schematic diagram exists, identifying all main systems including interfaces, Millennium Oniline ,e-Mail, Call & Internet Billing System, Network Firewall etc. (excluding individual network pc's) (Schematic diagram)	Dissatisfied			50		
2.5	An up-to-date schematic diagram or floor plan exists, identifying all cabling routes & all cables are clearly labeled (Schematic diagram or floor plan)	Dissatisfied			50		
2.6	An up-to-date diagram or listing exists identifying all patching information for the IT Patch Panel(s) (This can be a part of the above diagrams or hardware listings) (Diagram or listing)	Dissatisfied			50		
2.7	An up-to-date IT Emergency Plan exists which has been agreed with all HOD's & covers all critical systems. Relevant parts of the plan are available in departments. (Emergency plan, spot check departments)	Dissatisfied			50		
2.8	Full set of manuals exist in the IT department (Systems + Telephone Systems) & copies of relevant user manuals are available and accessible to users (Manuals in IT , spot check availability of User manuals in departments)	Dissatisfied			50		
2.9	IT Mgr must be familiar with and have on file all IT relevant policies & Procedures (Policies & Procedures file)	Dissatisfied			50		

3	Physical Security	Evaluation	☺	😐	☹		AVG
3.1	The computer & Communicatoin rooms are locked & access restricted to authorised personnel; (physical check)	**Very Satisfied**	100				85.42%
3.2	The PABX room is locked & access restricted to authorised personnel; (physical check)	**Very Satisfied**	100				
3.3	Temperature/Fire/Smoke alarms and appropriate extinguishers are in place in the Computer Rooms & alarms are located in a central area with 24 hrs/day, 7 days/week staff coverage (e.g. telephone operators...) (physical check)	**Satisfied**		75			
3.4	All critical equipment (which is a minimum of all Servers, Night Audit station, Interfaces, Call Accounting) are protected by a UPS & the UPS must itself be connected to the power generator of the hotel (physical check / discussion)	**Very Satisfied**	100				
3.5	Minimum 1 Front Desk PC & printer is protected by UPS & power generator (Physical check / discussion)	**Very Satisfied**	100				
3.6	The PABX is to be supported by it's own independent battery back-up as well as by the emergency generator (physical check / discussion)	**Very Satisfied**	100				
3.7	Where a modem is used, dial-in capability is restricted (physical spot check)						
3.8	The hotel should have clear desk policy to be applied by employees which will include Instruction for safe guarding of documents and diskettes in locked desk Using key and or password to prevent unauthorised use of personal computers	**Satisfied**		75			
3.9	IT equipments should not be taken away without proper authorization and IT property that is used outside the premesis of the hotel should be well protected	**Satisfied**		75			
3.10	Backup printers are attached to the folowing ssytem and documents exist explaining how to process printed equipments (physical check & documents) or else you can use a PC to buffer the data	**Satisfied**		75			
3.11	PRI Line	**Satisfied**		75			
3.12	Internet Billing	**Satisfied**		75			
3.13	Pay-TV system						
3.14	PABX	**Satisfied**		75			

4	Systems Maintenance	Evaluation	☺	😐	☹		AVG
4.1	Maintenance agreements provide adequate cover for critical equipment & are reviewed annually (discussion/contracts)	**Dissatisfied**			50		61.36%
4.2	Where a central UPS is used to protect IT equipment, the UPS should be covered by a maintenance contract. For de-centralised UPS', written procedures should be in place to ensure uninterrupted operation & replacement as per manufactures instructions (maintenance contract and/or written procedures)	**Satisfied**		75			
4.3	All major problems should be properly documented and filed for reference purposes (min. description of problem, location & action taken) (problem log file)	**Dissatisfied**			50		
4.4	Problem Managements should be defined in terms of responsibilities and procedures should be in place in case of incidents.Logging the following: System malfunction, Downtime of the system, Errors resulting from incomplete or inaccurate operational data, Breaches of confidentiality.	**Dissatisfied**			50		
4.5	All maintenance calls which have not been properly attended to by the maintenance company should be documented and included in the monthly status report (documentation & Monthly status report)	**Dissatisfied**			50		
4.6	The Call-Out procedure numbers are documented and accessible to relevant staff (view document)	**Dissatisfied**			50		
4.7	The Diskspace on all servers (Micros, Windows, SUN) is checked at appropriate frequency and action is taken if required (spot check/discussion)	**Satisfied**		75			
4.8	Cleaning tapes are available and used per manufacturers recommendations (physical check)	**Satisfied**		75			
4.9	The Hotel should have an arrangement allowing for restoration of computer processing power in the event of emergency	**Satisfied**		75			
4.10	Change Management procedure regarding replacing hardware,defining,prioritizing. Assessing the possible consequences of such a change. Informing the employees of such a change.	**Dissatisfied**			50		
4.11	The Hotel should have adequate controls against viruses and right means to automatically update all the PC in the network	**Satisfied**		75			

5	Access Security	Evaluation	☺	😐	☹		AVG
5.1	A procedure exists for issuing/canceling passwords for starters/leavers with notification within 7 days of departure (procedure/discussion with HR)	**Satisfied**		75			73.08%
5.2	Only current employees are set up in the system (spot check)	**Satisfied**		75			
5.3	All employees only have access to the system(s) at an appropriate level for their duties (, Active Directory, Opera, SUN, FBM) (spot check /discussion)	**Satisfied**		75			
5.4	Master passwords for ALL systems are kept in separate sealed envelopes in a safe accessible to the Duty Manager. Passwords are changed when an envelope is opened (physical check & spot check password validity)	**Dissatisfied**			50		
5.5	Where Internet Access is available, procedures must be in place to ensure maximum data security. (If Internet P&P/standards have been issued, they should be followed) (procedures/discussion)	**Satisfied**		75			
5.6	All PC's & Servers are protected by antivirus software which will be updated regularly - minimum every 2 days (spot check)	**Satisfied**		75			
5.7	All USB ports & CD-ROMs must be physically locked or disabled. Any exception must be documented & justified	**Very Satisfied**	100				
5.8	All employees, as part of the induction programme, have signed the IT policies & procedures & are advised of any possible disciplinary action in case of violation (P&P to minimum contain information about data security, unauthorised or illegal software usage & virus protection) (IT P&P document / check employee file)	**Satisfied**		75			
5.9	The Hotel should have formal procedure that deals with breach of IT security	**Dissatisfied**			50		
5.10	Employee should immediately report softwares failures using defined procedures	**Satisfied**		75			
5.11	All Applications should have owners who are responsible for defining and monitoring access control rights	**Satisfied**		75			
5.12	User access to an application should be according to present access rights and users should be monitored	**Satisfied**		75			
5.13	All employees should be part of induction program, have signed the IT policies & procedures and are advised of any possible disciplanary action in case of voilations (P&P to minimum contain information about data security,unauthorised or illegal software usage and virus protection	**Satisfied**		75			

6	Back-Ups	Evaluation	☺	😐	☹		AVG
6.1	Critical back-ups are stored in a fireproof safe (physical check)	**Satisfied**		75			75.00%
6.2	Downtime reports are printed at timed intervals (minimum every 6 hours) & kept at the Front Desk, easily accessible (physical check)	**Satisfied**		75			
6.3	Backups of data files should be performed regularly and minimum as follows: PMS - 3 times daily - 1 time daily on 7 rotating tapes or similar backup media, POS - 1 time daily on 7 rotating tapes or similar backup media, SUN - 1 time daily on 5 rotating tapes, SUN - 1 time monthly on 3 rotating tapes, FBM - 1 time daily on 7 rotating tapes or similar backup media, All other - on an appropriate frequency. (physical check/discussion)	**Satisfied**		75			
6.4	For the IT Manager to demonstrate an ability to restore from back-ups.	**Satisfied**		75			
6.5	Off-Site – outside the property – back-up on a monthly basis.	**Satisfied**		75			

7	Training & Development	Evaluation	☺	😐	☹		AVG
7.1	All outlets / departments have a complete and up to date standards manual which contains:- Job breakdowns - list of tasks for each position in the department and standards (review department manual)	**Dissatisfied**			50		78.13%
7.2	Pre course questionnaires are used regularly and effectively - discussion takes place between attendee and manager for both internal & external programmes (meet with 3 employees who attended off job training courses and review quality of questionnaire)	**Satisfied**		75			
7.3	The IT Manager or his Assistant hold a Craft Trainer Certificate (Check off job training records and certificate)	**Satisfied**		75			
7.4	The IT Manager or his Assistant have completed the three day Managing Training & Development programme (check training records & post course workbook)	**Satisfied**		75			
7.5	The IT Manager has had an appraisal within the last 12 months (appraisal form)	**Satisfied**		75			
7.6	An individual Training & Development plan exists for the IT Manager and his assistant identified from the succession plan, listing development needs (review Development Plan: name, current position, date in current job, date from last appraisal, training & development needs, comments and is implemented and actioned)	**Very Satisfied**	100				
7.7	A systematic training needs analysis is carried out for all computerised systems at the hotel and training is planned effectively for one year. The plan should contain: SMART objectives, development methods, review methods (review needs analysis and computer training plan)	**Satisfied**		75			
7.8	Computer Training plan is effectively implemented. All aspects of the plan have been actioned except where justifiable reasons exist (for example change of business environment) (review Computer Training plan, training records, attendance list)	**Satisfied**		75			
7.9	The IT Manager meets with the Training Manager once per two months to review Computer Training & development plan (review minutes of meeting & action plan)	**Satisfied**		75			
7.10	The IT Manager and his Assistant have attended fire security & bomb training in the last twelve months or in line with legal requirements (whichever is greater) (review training records) Health & safety training is scheduled and run in the departments for all employees a minimum of once per year (review training records and training modules)	**Satisfied**		75			
7.11	A monthly activity report is produced by the IT Manager & distributed to the GM and Area Director of IT or CVP of IT (status report)						
7.12	The IT Manager must attend operational/departmental/Executive meetings & provide regular updates on systems activities to Department / Executive Heads in the form of verbal & written presentations (discussions, meeting minutes & presentations)	**Very Satisfied**	100				
7.13	The IT Manager stays informed about and follows up on problems / request of the End-users through direct verbal communication (daily rounds, attending departmental meetings, problems / requests logged in logbook) (discussion, talk to staff, check logbook)	**Very Satisfied**	100				
7,14	The IT Manager provides an induction training for key personnel (Dept. Heads, Supervisors) (minimum systems overview & relevant emergency plan) (discussion / talk to 3 new staff, see training records)	**Very Satisfied**	100				
7.15	A detailed handover plan exists for the IT Manager's successor (View Handover Plan)	**Dissatisfied**			50		
7.16	Soft and hard copy of IT Handover Book to be maintained and updated bi-annually.						
7.17	IT Manager to maintain social and team collaboration activities to promote a positive and motivational spirit amongst his team.	**Satisfied**		75			
7.18	Evaluate the strengths and weaknesses of the achievements of the IT Manager with reference to his Annual Performance Review.	**Satisfied**		75			

8	IT Miscellaneous	Evaluation	☺	😐	☹		AVG
8.1	The number of software licenses match the number of concurrent users that have access to the applications (software licenses that match the copyright requirements (licenses / spotcheck)	**Satisfied**		75			75.00%
8.2	IT Manager must have good knowledge about Oracle Data Base Administration, cable of providing first line support for the Opera system	**Satisfied**		75			
8.3	The IT Manager must stay up-to-date with the latest IT developments through computer magazine subscriptions & visits to computer fairs (subscriptions / discussion)	**Satisfied**		75			
9	**Guest Services**	**Evaluation**	☺	😐	☹		**AVG**
9.1	Guests are able to use MS Office applications in the Business Center or Public area, including printing facilities (Word, Excel, Powerpoint) (physical check)	**Satisfied**		75			75.00%
9.2	Guests can establish a RJ45 ethernet based connection in the room.	**Satisfied**		75			
9.3	Guests are able to make data connections wired or wireless connnection in Business Center or public area (physical check)	**Satisfied**		75			
9.4	Document exists, explaining data connection features and relevant staff are familiar with it (document & spot check)	**Satisfied**		75			
9.5	Internet access is available to guests in room, Business Center or public area (physical check)	**Satisfied**		75			
9.6	Full set of power/data converters & adapters is available for guest use, where legally allowed (physical check)	**Satisfied**		75			
9.7	Guest failure to connect to internet is logged and reported to the IT Department. Investigation takes place and issue is rectified.	**Satisfied**		75			
9.8	Variety of IT services and promotions offered to the Guest all year round.	**Satisfied**		75			

10	I.T Security Policy & Organization	Evaluation	☺	😐	☹		AVG
10.1	The Hotel should have an IT Security Policy which should be documentes in a manual that is avaialable to all employees.	**Dissatisfied**			50		68.75%
10.2	The Hotel should have an IT Security and steering committee to guide and supervise how IT can support the goals of the organization and implement IT security according to the overall IT security policy	**Satisfied**		75			
10.3	The responsibility regarding the protection of confidential and sensative data should be well described in a privacy policy for protection of sensative data	**Satisfied**		75			
10.4	Third Party access to the IT envioronment should be only possible after this party signs a contract describing the conditions for the access.	**Satisfied**		75			
11	**Business Contingency Plan**	**Evaluation**	☺	😐	☹		**AVG**
11.1	Procedures that deal with the development and maintenance of business contingency plans should be in place which contains: • Specification and priortization of critical business cycles • Identification of calamities with respect to critical business cycles • Estimation of the possible consequences of the identified calamities • Specification and approval off all resposibilities of employees involved • Documention of all emergency procedures • Training of employees • Testing the business contingency plan • Updating the business contingency plan	**Dissatisfied**			50		50.00%
11.2	All Business contingency plan should be regularly tested						
11.3	Business contingency plan should be adjusted periodically as result of changes in the internal and external surroundings of the Hotel.						