AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

A. EFFECTIVENESS AND EFFICIENCY

Internal controls are intended to provide reasonable assurance that program goals and objectives are effectively and efficiently met; laws and regulations are complied with; resources are adequately safeguarded and efficiently used; and reliable data are obtained, maintained, and accurately and fairly disclosed in reports.

This section provides broad questions to help the agency determine whether it is achieving its mission, goals and objectives in an effective and efficient manner, and whether organizational changes may impact its ability to continue to do so. Definitions for some of the terms used in this section follow.

"Customers" are broadly defined as any/all users of the agency's external or internal services. "Customers" could include: the public, federal or state funding sources, other city agencies, other units within the same agency, etc.

"Inputs" are defined as measures of the quantity of resources used in achieving program goals and objectives (e.g., personnel, materials, etc.).

"Outputs" are defined as measures of the quantity of service (e.g., the number of 911 calls the Police Department responded to in a given period).

"Outcomes" are defined as measures of the accomplishments or results that occur because of the provided services- the outputs (e.g., a reduction in the crime rate for given period due to the efforts of the Police Department).

"Significant Deviations" may be defined as 10 percent or greater. Agencies that feel that this is an inappropriate definition, may define the term differently, but should explain their definition as a Note at the end of the checklist.

		Enter "X" below to indicate answer			
		Yes	No	Partial Compliance	Not Applicable
1.	Does the agency, division unit, etc., have a written mission statement (i.e., what it is expected to accomplish)?	X			
2.	Does the agency, etc. have a clear understanding of its mission?	X			
3.	Is the agency's mission's) carried out with the highest quality , at the lowest cost, and with integrity?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
4.		Does the agency's mission reflect its customers' expectations?	X			
	a)	Do the customers have a clear understanding of the agency's mission?	X			
	b)	Does the agency have a process for getting periodic customer feedback (i.e., suggestions, compliments or complaints)?	X			
	c)	Are customer complaints reviewed and addressed, when considered necessary?	X			
5.		Are the agency's goals/objectives defined in measurable terms?	X			
	a)	Are the agency's outcomes measurable?	X			
	b)	Does the agency have specific outcome measurements?	X			
	c)	Does the agency have specific output measurements?	X			
	d)	Are the agency's outputs measurable?	X			
6.		Has the agency achieved its defined goals and objectives for the year under review?			X	
	a)	Were there no or only insignificant deviations between the expected and actual goals and objectives?			X	
	b)	Were there no or only insignificant deviations between the expected and actual outcomes (if they are being measured)?			X	
	c)	Were there no or only insignificant deviations between the expected and actual outputs (if they are being measured)?			X	
	d)	Were any significant deviations between the expected and actual goals, objectives, outcomes or outputs investigated and appropriate action taken?	X			
7.		Do the indicators published in the Mayor's Management Report effectively reflect the agency's performance?	X			
	a)	Do the indicators reflect the agency's principal activities?	X			
	b)	Were any significant deviations investigated and appropriate action taken?	X			
8.		Are agency programs conducted in accordance with clearly defined management policies?	X			
	a)	Are these policies in writing?			X	
	b)	Are these policies in accordance with the intent of applicable laws and regulations?	X			
	c)	Are these policies properly communicated to the appropriate agency staff?			X	
	d)	Are these policies reflected in formal written operating procedures?			X	
	e)	Are these procedures communicated to the appropriate agency staff?			X	
	f)	Are these policies periodically reviewed and updated as needed?			X	
	g)	Are these procedures periodically reviewed and updated as needed?			X	
	h)	Have these policies and/or procedures remained substantially the same within the past year?	X			
9.	a)	Are agency programs evaluated according to specific criteria for performance measurement?	X			
	b)	Are marginal or unsatisfactory levels of performance investigated?	X			
10.		Are the agency's outputs compared to the agency's inputs through efficiency performance measures?	X			
11.		Are efficiency measures compared over time or among programs?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

		Enter "X" below to indicate answer			
		Yes	No	Partial Compliance	Not Applicable
12.	Are the agency's outcomes compared to the agency's inputs through effectiveness performance measures?	X			
13.	Are effectiveness measures compared over time or among programs?	X			
14.	Has there been less than a 10% turnover in personnel performing the same job, within the past year?			X	
15.	Has the contracting out of a significant percentage of the agency's workload (i.e., more than 10% of the agency's OTPS budget) resulted in more effective delivery of service?	X			
	At the same or less cost?	X			
16.	Have compensating controls been put into place to adjust for any significant organizational changes?				X
17.	Are there any significant unresolved audit findings that have been open for more then one year?		X		

TOTALS: 27 1 11 1

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
B.		**CASH RECEIPTS** CASH RECEIPTS refers to Currency, Checks, Money Orders, Credit Card payments, and Electronic Fund Transfers. Sources of cash receipts include: sales, grants, taxes, fees and refunds. Internal Controls should provide reasonable assurance that cash receipts will not be misappropriated or stolen. These controls should be commensurate with the value of the receipts that are to be safeguarded. Controls include adequate segregation of duties, ongoing reviews and monitoring functions, adequate security and timely reconciliations. Information pertaining to cash management can be found in Comptroller's Directive #11, "Cash Accountability and Control."				
1.		Segregation of Duties:				
	a)	Are responsibilities for cash receipt functions segregated from those of cash disbursement?	X			
	b)	Are responsibilities for billing, collecting, depositing, and accounting for receipts performed by different individuals?	X			
	c)	Are responsibilities for preparing and approving bank account reconciliations segregated from other cash receipts or disbursement functions?	X			
	d)	Does someone independent of processing and recording cash receipts follow-up on checks returned for insufficient funds?	X			
2.		Control Over Cash Receipts:				
	a)	Are cash receipts recorded immediately and deposited daily?			X	
	b)	If not, are the mitigating controls stated in Comptroller's Directive #11 followed?	X			
	c)	Do separate collection centers forward a timely notice of cash receipts to the agency's central accounting unit?	X			
	d)	Are electronic fund transfer transactions controlled in accordance with Directive #11				X
	e)	Is cash on hand properly secured (i.e., in a locked safe with a periodically changed combination known to few individuals)?	X			
	f)	Is a restrictive endorsement placed on incoming checks as soon as they are received?	X			
	g)	Are incoming checks listed when received by someone separate from the accounting unit?	X			
	h)	Is this list independently reviewed and compared to cash receipts and deposit slips?	X			
	i)	For sale, or other transactions with the public, are prenumbered receipts provided to payers?	X			
	j)	Are these receipts issued in numerical sequence and accounted for numerically, including those that are voided?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
	k)	Are these receipts matched to collection reports on a daily basis?	X			
	l)	Are non-cash methods of payment (e.g., credit cards, checks, money orders) promoted, whenever possible?	X			
	m)	Does someone ensure that all bank accounts are approved by the Department of Finance and registered with the Comptroller's Office?	X			
	n)	Does someone ensure that all bank account closings are routed through the Department of Finance and the Comptroller's Office?	X			
	o)	For bank deposits, are checks separately listed on the deposit slip and confirmed to the cash receipts record?	X			
	p)	Are deposit bags safeguarded (e.g., locked)?	X			
	q)	Are deposits made by authorized personnel?	X			
	r)	If deposits are made by courier service, is the service adequately insured and/or bonded?	X			
3.		Bank Reconciliations:				
	a)	Are all of the agency's bank accounts reconciled within 30 days of the statement date?	X			
	b)	Are outstanding checks and deposits in transit traced to the following month and followed up?	X			
	c)	Are copies of the June 30th reconciliations sent to the Comptroller's Office promptly?	X			
	d)	Are procedures for follow-up on checks returned for insufficient funds adequate?	X			
	e)	Are checks in excess of $25 which are outstanding over 6 months cancelled?		X		
		TOTALS:	**24**	**1**	**1**	**1**

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

		Enter "X" below to indicate answer			
		Yes	No	Partial Compliance	Not Applicable
C.	**IMPREST FUNDS (PETTY CASH)** IMPREST FUNDS (PETTY CASH) is a type of agency fund used for minor expenses incurred in daily operations, and is periodically replenished. Although large sums of money are not usually involved, and this is a cash disbursement function, this fund requires similar controls as those needed for the management of cash receipts, since funds may be easily misappropriated or stolen. For information about managing imprest funds, see Comptroller's Directive #3, "Procedures for the Administration of Imprest Funds".				
1.	Are the functions of authorizing purchases, disbursing petty cash, signing checks, signing vouchers, recordkeeping and bank reconciliations performed by different individuals in accordance with Directive #3?	X			
2.	Is a maximum limit established for the imprest fund?	X			
3.	Is a separate bank account maintained for the imprest fund?	X			
4.	Are controls in place to ensure that no individual purchase or disbursement exceeds $250, and that purchases are not split to circumvent the $250 limit?	X			
5	Are petty cash vouchers presented with all requests for reimbursement?	X			
6	Do invoices paid by petty cash reflect proof of purchase?	X			
7	Are cash invoices approved by a responsible person other than the petty cash custodian?	X			
8	Does a responsible employee check and verify all vouchers and supporting documentation for completeness and authenticity prior to replenishing the fund?	X			
9	Does someone, other than the employee in Item 7 examine and cancel paid vouchers to prevent duplicate reimbursement?	X			
10.	Are imprest funds promptly replenished?	X			
11.	Has a maximum amount been established that can be withdrawn from Petty Cash at one time?	X			
12.	Are independent, surprise counts of the petty cash fund and reconciliations to its records periodically conducted?	X			
13.	Is the petty cash secured in a locked safe with limited access?	X			
14.	Are petty cash slips pre-numbered?		X		
	TOTALS:	**13**	**1**	**0**	**0**

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
D.		**BILLINGS AND RECEIVABLES**				
		BILLINGS AND RECEIVABLES are related processes that are subject to manipulation for the purposes of misappropriation or theft of City funds. Internal Controls are intended to minimize the possibility of such improper actions. Billings involves sending out accurate and timely bills for services rendered or for monies due to the City. Receivables are accounts set up to record monies owed to the City, including unexpended advances to contractors, and the subsequent receipt of monies that reduce or eliminate the outstanding receivable. The receivables should be reviewed and aged periodically to determine if other collection actions should be taken or if accounts should be written off. For information regarding billings and receivables, refer to Comptroller's Directive #21, "Revenue Monitoring".				
1.		Segregation of Duties: Are receivable accounts maintained by employees who do not handle cash receipts?	X			
2.		Billing:				
	a)	Are fees for inspections, licenses, tuition, rent, permits and other revenues billed fully and promptly?	X			
	b)	Are unexpended advances to agency contractors promptly recouped as provided for in covering contracts?	X			
	c)	Are disputed billing amounts promptly investigated by an individual, independent of receivables recordkeeping?	X			
	d)	Do procedures provide for the prompt filing of liens on properties for nonpayment when permitted by law?	X			
3.		Receivables:				
	a)	Are all receivable accounts reconciled on a monthly basis as per Directive #21?	X			
	b)	Are accounts aged periodically?	X			
	c)	Is nonpayment of accounts followed up?	X			
	d)	Are there written collection procedures?	X			
	e)	Are they periodically re-evaluated by individuals of appropriate authority?	X			
	f)	Are adjustments to receivables accounts independently reviewed?	X			
	g)	Are overdue accounts transferred to the Law Department for litigation, or an outside collection agency, in accordance with Comptroller's Directive #21?	X			
4.		Write-Off Procedures:				
	a)	Do write-offs receive the proper level of authorization as required by Directive #21?			X	

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
	b)	Is a formal write-off policy established as required by Directive #21?			X	
5.		Claims for State and Federal Aid:				
	a)	Are all claims for State and Federal Aid filed by the agency within 30 days of the close of the period being claimed?	X			
	b)	Is the claim for nonpayment by State and Federal agencies followed-up within the required 30 or 45 days?	X			
	c)	Are disputed claims investigated promptly?	X			

TOTALS: 15 0 2 0

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

E. EXPENDITURES AND PAYABLES

EXPENDITURES AND PAYABLES are monies paid or owed by the City for the procurement of services or goods. Due to the many steps in the procurement process and the large sums of monies that are expended, the review, authorization and inspection controls are the most important. Ongoing monitoring reduces the risk of improper actions and misappropriation, and ensures that the City obtains quality goods and services at economical prices.

See the Procurement Policy Board Rules (PPBR) and Comptroller's Directives # 2, 9, 24, and 29 about issues pertaining to expenditures and payables.

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
1.		Segregation of Duties: Are the functions of ordering, receiving, invoice processing and voucher preparation performed by different individuals?	X			
2.	a)	Procurement Practices: Are all purchases authorized by personnel of the proper level of responsibility?	X			
	b)	Have specific agency contract procedures been developed to ensure compliance with the City's Procurement Policy Board Rules (PPBR) for: i. Contract Formation?	X			
		ii: Vendor Source Selection?	X			
		iii: Contract Award?	X			
		iv: Contract Administration?	X			
		v. Dispute Resolution?	X			
		vi. Maintenance of Records?	X			
		vii. Contract Change Orders?	X			
	c)	Are competitive sealed bids/proposals used for purchases over $25,000 for goods, $50,000 for services, and $100,000 for construction or information technology in accordance with the PPBR?	X			
	d)	When competitive bidding is not used are "special case" determinations (per PPBR) documented and approved by the Agency Chief Contracting Officer (ACCO)?	X			
	e)	Was prior approval sought and received from the Comptroller and Corporation Counsel for emergency purchases (per PPBR)?	X			
	f)	Is follow up done for contracts that are not shown as registered with the Comptroller's Office?	X			
	g)	Are prequalified vendor lists maintained and updated?	X			
	h)	Are only bid submission forms that are typed or printed in ink (no erasures) accepted?	X			
	i)	Does someone, other than the individual requesting the procurement, review the City's VENDEX listing, and the contractor's stated qualifications and references, to determine if the contractor is qualified?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

		Enter "X" below to indicate answer			
		Yes	No	Partial Compliance	Not Applicable
j)	Does the agency's ACCO review the information obtained from VENDEX and related qualification/reference information, in making decisions regarding the contractor's qualifications?	X			
k)	Do all procurement personnel receive training in the PPBR as needed?	X			
l)	Are there formal procedures for purchasing items under $5,000 that are not required to be bid?	X			
m)	Are purchase orders for similar items under $5,000 from the same vendor reviewed to ensure that they are not split orders meant to circumvent the PPBR?	X			
n)	Is there contract monitoring and is information pertaining to the applicable program collected and evaluated periodically, to determine if the goals related to the contract are being met?	X			
o)	Is supplier performance evaluated at least once a year per PPBR and procedures established by the City Chief Procurement Officer (CCPO)?	X			
3.	Encumbrances: Are all encumbrances (contracts and orders) more than 90 days old reviewed monthly and adjusted as necessary to reflect the value of goods and services still to be received?	X			
4. a)	Accountability for Resources: Are quantities verified upon receipt of merchandise?	X			
b)	Is the merchandise examined or tested for quality as soon as possible after delivery?	X			
5. a)	Invoice and Voucher Processing Procedures: Are copies of purchase orders and receiving reports obtained directly from the issuing department?	X			
b)	Are purchase orders, purchase requisitions, and vouchers all prenumbered and recorded?		X		
c)	Are missing purchase orders and/or requisitions investigated?	X			
d)	Are invoice quantities, prices and terms compared with those indicated on purchase orders?	X			
e)	Are invoice quantities compared with those indicated on receiving reports?	X			
f)	Are invoices checked for clerical accuracy?	X			
g)	Do invoices above a set amount need additional approval?		X		
h)	Are all paid invoices marked "cancelled","paid", or "voided" to indicate that they have been processed for payment?	X			
i)	Are procedures in place to ensure that payment vouchers are approved by two agency assigned FMS users in accordance with Directive 24?	X			
j)	Are vouchers processed promptly for payment?			X	
k)	Are cash discounts taken?	X			
l)	Are exemptions from sales, Federal excise and other taxes claimed?	X			
m)	Are invoices and supporting documents furnished to and reviewed by the signer prior to signing a voucher?	X			
6. a)	FMS Reconciliation: Are agency expenditures and purchasing records reconciled on a timely basis to appropriate FMS reports for all funds?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
	b)	Do FMS reports reflect vouchers properly authorized by agency personnel?	X			
	c)	Does the agency have proper documentation to support all FMS vouchers?	X			
7	a)	Has the agency established controls and procedures to assure the accuracy and integrity of all information entered into the City-wide FMS payee/vendor database, in accordance with Directive 29, so that payee/vendors receive the appropriate 1099 forms(1099-MISC, 1099-INT)?	X			
	b)	Has the agency established controls and procedures to determine that a new payee/vendor has not already been validated in FMS?	X			
	c)	Has the agency established controls and procedures to assure that the information for a payee/vendor that you use is accurate?	X			
	d)	Has the agency established controls and procedures to assure that the VA99 report is promptly reviewed in accordance with Directive 29, and any erroneous information corrected?	X			
		TOTALS:	**42**	**2**	**1**	**0**

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
F.		**INVENTORY** INVENTORY primarily refers to items used by the Agency for its operations. However, it could also include items stored by the agency for disbursement to its branches or other agencies, or confiscated or obsolete goods that are being held for sale. Supplies and some non-capital assets are particularly susceptible to theft and misuse; while capital assets require specific procedures for their purchase, maintenance and disposal. All of these inventory items require strong controls to ensure accurate recordkeeping and good security. For information regarding Inventory issues, refer to Comptroller's Directives #10, 24, and 30.				
1.	a)	Supplies and Non-Capital Assets: (Supplies and Non-capital assets are charged to the expense budget. Excluding capital assets, all other assets fall under these two categories.) Are supplies and non-capital assets kept under the strict control of designated employees?			X	
	b)	Are detailed records maintained for supplies and non-capital assets?			X	
	c)	Is the responsibility for supervising the use of physical inventories of supplies and non-capital assets segregated from that for the maintenance of detailed records?			X	
	d)	Have inventory levels been established in such a manner as to prevent excess accumulations or unavailability of items?			X	
	e)	Are perpetual inventory records (if a perpetual system is maintained) compared to physical inventory taken, and significant variances investigated?			X	
	f)	Are physical inventories conducted and supervised by individuals independent of the departments maintaining the assets?		X		
	g)	Are government assets in a contractor's custody promptly retrieved and accounted for upon final termination of a contract with an agency contractor?	X			
	h)	Are expensive non-capital items (e.g., computers, cars) positively identified (tagged)?			X	
2.	a)	Capital Assets: Are responsibilities for initiating, evaluating, approving and recording capital expenditures, leases and maintenance or repair projects performed by different individuals?	X			
	b)	Is the responsibility for supervising the use of physical inventories for capital assets segregated from the maintenance of detailed records?	X			
	c)	Does an appropriate employee ensure that accurate and complete inventory records are maintained for all assets?			X	
	d)	For new projects, are the criteria in Directives 10 and 30 complied with when determining capital eligibility?			X	

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

	Enter "X" below to indicate answer			
	Yes	No	Partial Compliance	Not Applicable
e) For all capital projects, are the criteria in Directives 10 and 30 complied with when determining whether an expense is capital eligible?			X	
f) Are capital assets valued in accordance with Directive 30?		X		
g) Are all capital projects reflected in FMS in accordance with Directive 10 and Directive 30 requirements, and in a timely basis (i.e., FMS documents FI, FA, FB, FT, FC, FD)?			X	
h) Are assets monitored to determine that there is no permanent impairment as detailed in Directive 30?			X	
i) Are assets that have permanent impairments written down in accordance with Directive 30 requirements?			X	
j) Are assets that have no further utility disposed of in accordance with Directive 30 requirements?			X	
k) Are capital assets held for resale, for example foreclosed assets, recorded in the General Fund, at their appropriate value as required by Directive 30?			X	
l) Are assets classified as infrastructure included in the capital asset inventory if they meet the eligibility criteria in Directives 10 and 30?			X	
m) Is an annual physical inventory performed for all capital assets and the records maintained as required by Directive 30?			X	
n) Are the agency inventory records reconclied to both the FMS Capital Asset information and the agency's internal Capital Asset records?			X	
o) Are metal numbered tags or other means of positive identification used to identify motor vehicles, office furniture, and other equipment?			X	
p) Are assets maintained properly?	X			
q) Are adequate controls in place over the sale of scrap?	X			
TOTALS:	**5**	**2**	**18**	**0**

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
G.		**PAYROLL AND PERSONNEL** PAYROLL AND PERSONNEL management involves cyclical functions that begin by recording accurate personnel data such as employee's name and address, time worked, authorized expenses, correct wages, tax withholding information, etc. and ends with the paycheck distribution. Good internal controls in this area ensure that only those persons entitled to a paycheck obtain one; and each paycheck represents the correct amount of money that each person is entitled to. Accurate, earned leave balances should be accrued and recorded, and employees leaving city employment be paid for any unused leave in accordance with applicable requirements. For additional information on this topic, refer to Comptroller's Directives 13 (Payroll Procedures), 14 (Leave Balance Payments), and 19 (Recouping Payroll Overpayments to City Employees).				
1.		Segregation of Duties:				
	a)	Are responsibilities for supervision, timekeeping, personnel, payroll processing and disbursements all performed by different individuals?	X			
	b)	Are comparisons (reconciliations) of gross pay of current to prior period payrolls reviewed for reasonableness by knowledgeable persons not otherwise involved in payroll processing?	X			
	c)	Is payroll reviewed (including an examination of authorizations for any changes noted on the reconciliations) by an employee not involved in its preparation?	X			
2.		Payroll Processing:				
	a)	Does the Personnel or Human Resources Department ensure that all new employees are promptly placed on the payroll?	X			
	b)	Does the Personnel or Human Resources Department ensure that all employees who have retired, or resigned, or who are on leave without pay, etc., are promptly removed from the payroll?	X			
	c)	Does the Personnel Department ensure that all changes in employment (additions and terminations), salary/wage rates and payroll deductions are properly authorized, approved and documented?	X			
	d)	Are payroll records periodically checked against personnel records, and are any discrepancies investigated?	X			
3.		Timekeeping:				
	a)	Are appropriate records maintained for accumulated employee benefits (e.g., vacation)?	X			
	b)	Have adequate timekeeping procedures been established to insure that employees arriving late or leaving early are charged leave?	X			
	c)	Are leave balances/records periodically checked to source documents?	X			
	d)	Are negative leave balances properly investigated to determine the exact causes and appropriate action(s) subsequently taken?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

		Enter "X" below to indicate answer			
		Yes	No	Partial Compliance	Not Applicable
e)	Are periodic checks made to verify that non-managerial employees are accumulating and using sick and annual leave properly?	X			
f)	Are periodic checks made to verify that managerial employees are accumulating and using sick and annual time in accordance with Personnel Orders 88-5 and 97-2?	X			
g)	Are periodic checks made to verify that non-managerial compensatory time is authorized, accumulated and used properly?	X			
h)	Are procedures in place to ensure that employees whose personnel status changes (e.g., from non-managerial to managerial, or from part-time to full-time) are still accruing and using their leave balances appropriately?	X			
i)	Are all proposed managerial lump sum payments submitted to the Comptroller's Office for approval, prior to payment, per Directive #14?	X			
4.	Personnel:				
a)	Are periodic reconciliations made between all payroll records and central master records to ensure that all data is up-to-date?	X			
b)	Are notices of additions, separations, and changes in salaries, wages, and deductions reported promptly to the payroll processing function?	X			
c)	Is there a waiver (approval) on file for all employees that work for the City but live outside its limits? (Section 1127 which states employees will pay City taxes)	X			
d)	Are Federal and New York State withholding status forms on file?	X			
e)	Are there adequate controls to ensure that Form DP-1021 is submitted to the City's Personnel Department for each employee who is securing additional employment in any other civil service position in New York City or with any other governmental agency?	X			
f)	Are controls in place to ensure compliance with DCAS Personnel Services Bulletin # 440-10 (transmitted 6/30/97) regarding Jury Duty?	X			
5.	Disbursements:				
a)	Are paychecks inadvertently generated for persons no longer on the payroll, returned immediately to the Office of Payroll Administration?	X			
b)	Are all undistributed checks or payroll stubs for those receiving direct deposit, logged in and their disposition noted?	X			
c)	Are payroll registers adequately reviewed and approved before disbursements are made?	X			
d)	Are employees required to sign for their paychecks or payroll stubs for those receiving direct deposit?	X			
e)	Are all requests to hold a paycheck (or payroll stub for those receiving direct deposit) or to authorize someone else to claim it, in writing?	X			
6.	Supervision:				
a)	Is overtime properly authorized?	X			
b)	Are adequate supervisory controls, such as field observations and productivity standards, established with regard to persons working in the field?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
7.		PMS Reports:				
	a)	Are PMS reports, such as employee's leave, overtime, and absence control, reviewed periodically by management?	X			
	b)	Are there adequate controls to ensure that no paycheck will be released to an employee until a time card, approved by a supervisor has been submitted to the Payroll Department as required by PMS regulations?	X			
		TOTALS:	**31**	**0**	**0**	**0**

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

H. MANAGEMENT INFORMATION SYSTEMS (MIS): MAINFRAME/MIDRANGE

As the City stores increasing amounts of information in a computerized medium, it becomes increasingly important to assure that this data is reliable and adequately protected from unauthorized access, manipulation or destruction. An equally significant concern is whether the City is acquiring its computer hardware and software in a planned manner to ensure that anticipated future information processing, storage and retrieval needs are met.

The Department of Information Technology and Telecommunications (DoITT) has assumed the responsibility for information security policy formulation. It has published the Citywide Information Security Policies and Standards, which City agencies must comply with.
Some of these have been classified as public documents and are available at:
http://www.nyc.gov/html/doitt/html/business/business_it_security.shtml
Others are internal and are available to authorized users on the City’s intranet.
Comptroller’s Directive #18, "Guidelines for Computer Security and Control" provides additional guidance

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
1.	a)	Planning and Organization: Is there a MIS planning/steering committee?	X			
	b)	Has management established: i. A written long range MIS plan?			X	
		ii. A written short range MIS plan?	X			
	c)	Has management shared both its long range and short range plans with the appropriate field personnel?	X			
	d)	Has management established MIS policies, procedures and standards?			X	
	e)	Do these comply with DoITT Citywide Information Security Policies and Standards?			X	
	f)	Is there segregation of duties between MIS and the accounting and operating departments for which it processes data?	X			
	g)	Within the MIS organization are there separate and distinct groups responsible for: i. Operations?		X		
		ii. Applications Development?	X			
		iii. Applications Maintenance?		X		
		iv. Quality Assurance?	X			
		v. Technical Support?		X		
		vi. Systems Programming?		X		
	h)	Are there written MIS position descriptions?	X			
	i)	Is there an internal MIS audit group?			X	
		i. Reporting to MIS?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
		ii. Reporting to the Internal Audit Department?				X
	j)	Has any aspect of MIS been audited within the last four years? If so, please attach a list of the reports, organizations that issued them, and dates of issuance.	X			
	k)	Are computer processing services provided by: i. The Department of Information, Technology & Telecommunications?	X			
		ii. The Financial Information Services Agency?	X			
		iii. Inhouse personnel?	X			
		iv. Any other City agency?	X			
		v. Other vendors?	X			
2.		Systems Development Controls:				
	a)	Are new systems developed in accordance with DoITT's Systems Development Life Cycle (SDLC)?				X
	b)	Is there user involvement in systems development?	X			
	c)	Is a separate Quality Assurance function used to assess the adequacy and appropriateness of system enhancements and/or new systems, as they are being developed?			X	
	d)	Are the costs of system enhancements and/or new systems monitored and recorded on a system-by-system basis?		X		
3.	a)	Does the agency maintain a list of all systems currently being developed?				X
	b)	Does the list identify: how each was procured?				X
		i. Whether the system was approved (if applicable) by the Information Technology Steering Committee?				X
		ii. Whether the systemwas approved by the Citywide Chief Information Security Officer (CISO)?				X
		iii. Whether system maintenance was or will be purchased from an external vendor?				X
	c)	If the answer to a. is "Yes," please provide an agency contact for the list.				
		Agency contact:				
		Title:				
		Telephone #				
	d)	Please enclose a copy of the list with your Directive 1 submission. Have you submitted the requested copy?				X
4.		Application and System Software Maintenance:				
	a)	Are there written standards for the maintenance of applications software?	X			
	b)	Are application system modifications tested before implementation?	X			
	c)	Do operating departments approve the test results?	X			
	d)	Is application system documentation revised to reflect the changes?	X			
	e)	Is an independent group, other than those groups responsible for applications development or maintenance, responsible for changes to computer operating system software?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
5.		Documentation of Systems:				
	a)	Are there written standards for the documentation of computer applications?			X	
	b)	Do the documentation standards include: i. Data ownership and criticality classification?	X			
		ii. Data syntax rules (file naming conventions)?	X			
		iii. Security levels?	X			
		iv. Comparison of information architecture to similar organizations?		X		
	c)	Do these standards require that such documentation include: i. Application overview?	X			
		ii. Data dictionary?	X			
		iii. A description of paper or other input sources?	X			
		iv. User procedures?	X			
		v. System processing?	X			
		vi. Computer operations procedures?	X			
		vii. A description of the system's output?	X			
		viii. Instruction for report and output distribution?	X			
	d)	Are there written programming standards?			X	
	e)	Is adequate documentation maintained for computer operating systems software including: i. Version?	X			
		ii. Parameters selected?	X			
		iii. Modifications?	X			
		iv. Computer operations procedures?	X			
		v. Compliance with software licensing agreements and copyright laws?	X			
	f)	Is the documentation for all data processing systems adequate to ensure that the organization could continue to operate if key MIS employees, and/or key consultants leave?			X	
6.	a)	Does the agency maintain a list of all critical mainframe systems?	X			
	b)	Does the list provide a brief description of each system?	X			
	c)	If the answer to a) is "Yes," please provide an agency contact for the list. Agency Contact for List:	Joe Tuccillo			
		Title:	Computer Specialist			
		Telephone #	212-689-2737			
	d)	Please enclose a copy of the list with your Directive 1 submission. Have you submitted the requested copy?	X			
7.		Physical and Logical Security:				
	a)	Is physical access to computer operations facilities restricted to authorized personnel?	X			
	b)	Has all computer hardware been marked with, or can be identified by, the Agency Asset Identification number?	X			
	c)	Does policy prohibit MIS personnel from originating financial transactions?	X			
	d)	Is there an independent data security administrator?	X			
	e)	Is a general purpose security software product used to restrict logical access to data and to prevent data entry by unauthorized individuals?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
	f)	Do the users have the capability of dialing into the systems from a remote location?		X		
	g)	If so, are all such sessions authenticated by the system?				X
8.		Systems Operations Controls:				
	a)	Is a computer operations schedule used to ensure timely submission and control over work?	X			
	b)	Has that schedule been approved by: i. The operating departments?	X			
		ii. The MIS Department?	X			
	c)	Are there detailed written instructions for the operation of each system?	X			
	d)	Is there a log of computer operations activities?	X			
	e)	Are these logs maintained for at least one year?				X
	f)	Are these logs reviewed by MIS management?			X	
	g)	Are computerized records retained in accordance with an established schedule?	X			
	h)	Does the data retention schedule comply with applicable legal requirements (i.e., Department of Records and Information Services [DORIS])?	X			
9.	a)	Backup and Disaster Contingency Plans: Are backup copies of computerized records made on a regular schedule?				X
	b)	Are additional backup copies of computerized records kept at a secure off-site location?				X
	c)	Is there a written contingency and disaster recovery plan?				X
		When was it updated?				
	d)	Is the disaster recovery plan based upon an agency-wide information protection plan which assesses the agency's information risks and vulnerabilities?				X
	e)	Does the agency have its own user site contingency and disaster recovery plan?			X	
	f)	For agencies maintaining their own data processing facilities, is the plan tested semiannually?				X
	g)	For agencies whose processing facilities are supplied by an outside vendor or another NYC agency, has the agency participated in a semiannual disaster recovery test?			X	
	h)	Has the plan been tested within this calendar year?			X	
		If the answer is "Yes," please provide the date				
10.		Execution and Authorization of Transactions:				
	a)	Are there adequate controls over preparation and approval of input transactions by the operating departments?	X			
	b)	Is there adequate MIS editing and validation of data entry (i.e., testing dollar fields for numeric data, testing for duplicate numbers)?	X			
	c)	Are there adequate controls to assure that all transactions are accurately recorded and promptly posted?	X			
	d)	Are there reconciliation procedures for batch processing?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

	Enter "X" below to indicate answer			
	Yes	No	Partial Compliance	Not Applicable
e) Are rejected records corrected and reprocessed?	X			
f) Do user controls include reconciliation of input to output?	X			
g) Are system outputs reviewed for reasonableness?	X			
h) Do the system balancing procedures reconcile opening balances plus current input to the closing balances?	X			
i) Are source documents retained in accordance with an approved schedule?	X			
j) Do all transactions have a readily accessible source document?	X			
TOTALS:	**61**	**7**	**12**	**15**

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
I.		**MANAGEMENT INFORMATION SYSTEMS (MIS):** **PERSONAL COMPUTERS/LOCAL AREA NETWORKS** This section raises the same concerns as Section H.				
1.		Personal Computer Procedures and Standards:				
	a)	Has management established agency wide policies, procedures and standards for the installation and use of Personal Computers (PC)?	X			
	b)	Do these comply with DoITT's Citywide Information Security Policies and Standards?			X	
	c)	Have all employees who access information systems received a copy of DoITT's User Responsibilities Policy?		X		
	d)	Have these policies, procedures, and standards been communicated to appropriate field personnel?	X			
	e)	Do these policies, procedures and standards address the following issues:				
		i. Standardization of software?	X			
		ii. Standardization of hardware?	X			
		iii. Data retention?	X			
		iv. Data recovery?	X			
		v. Data Security?	X			
		vi. Application development controls?	X			
		vii. Inventory of hardware?			X	
		viii. Inventory of software?	X			
		ix. Compliance with software licensing agreements and copyright laws?	X			
	f)	Do these policies, procedures and standards provide appropriate controls over the:				
		i. Use of the computers?	X			
		ii. Standardization of software?	X			
		iii. Periodic copying of programs and data?	X			
		iv. Acceptance and installation of new equipment?	X			
		v. Inventory of all hardware?	X			
		vi. Inventory of all software?	X			
		vii. Compliance with software licensing agreements and copyright laws?	X			
	g)	Have all PCs and related hardware been marked with an Agency Asset Identification number?			X	
2.		Local Area Network Procedures and Standards:				
	a)	Has management established agency wide policies, procedures and standards for the installation and use of Local Area Networks (LANS)?	X			
	b)	Do these comply with DoITT's Citywide Information Security Policies and Standards?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
	c)	Do these policies and procedures define an Agency Support Function and its associated responsibilities?	X			
	d)	Do these policies and procedures address adherence to copyright infringement terms and licensing agreements for leased and purchased LAN software?	X			
	e)	Do these policies and procedures address: i. Program testing?	X			
		ii. Documentation?	X			
		iii. Backup and recovery?	X			
	f)	Are the policies and procedures reviewed and updated to reflect changes in technology, the organizational structure, and management directives?	X			
	g)	Do the policies and procedures reflect the agency's position on employees' personal, non-business related use of agency workstations?	X			
	h)	Do the policies and procedures address the need for applicable training from either in-house or external consultants, as appropriate?	X			
3.		Agency Support Function:				
	a)	Is there a centralized group (or individual) designed to support end-user LAN installations?	X			
	b)	Is the support function adequately staffed?	X			
	c)	Are remote workstation processing locations provided with helpdesk consultation service for problems relating to workstation hardware and software?	X			
	d)	Are evaluations performed to avoid designing applications for LANs, for functions that can be performed more economically on the agency's mainframe computer?		X		
4.		Local Area Network Installations:				
	a)	Is there an inventory of all LANs currently installed throughout the agency?	X			
	b)	Are specific personnel assigned the functional responsibilities for LAN control and security?	X			
5.		LAN Hardware:				
	a)	Are procedures in place to ensure hardware maintenance is performed on a periodic basis?	X			
	b)	Are alternative vendors available to provide hardware support if the current vendor fails to provide adequate support?		X		
	c)	Are there procedures for the disposition of surplus hardware?	X			
6.		LAN Software:				
	a)	Is there a LAN purchased/leased software inventory list and is it kept current?	X			
	b)	Have procedures been developed and distributed to ensure compliance with software maintenance contracts and licensing agreements?	X			
	c)	Are LAN users knowledgeable of and in compliance with copyright infringement terms and licensing agreements for leased and purchased LAN software?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
	d)	Are network versions of LAN software being used?	X			
	e)	Do vendors of LAN software provide maintenance agreements which clearly define maintenance services and costs, and make source code available if the vendor goes out of business?	X			
	f)	Are backup copies made of all software before installation on the LAN?	X			
7.	a)	Does the agency maintain a list of all systems currently being developed?			X	
	b)	Does the list identify: how each was procured?			X	
		i. Whether the system was approved by the Information Technology Steering Committee (as applicable)?			X	
		ii. Whether the system was approved by the Citywide Chief Information Security Officer (CISO)?		X		
		iii. Whether system maintenance was or will be purchased from an external vendor?	X			
	c)	If the answer to a) is "Yes," please provide an agency contact for the list.				
		Agency contact:	Anuraag Sharma			
		Title:	Director of Business Re-engineering			
		Telephone #	212-313-5184			
	d)	Please enclose a copy of the list as part of your Directive 1 submission. Have you enclosed the requested copy?	X			
8.		Physical Security Controls:				
	a)	Are workstations physically secure during and after normal business hours?			X	
	b)	Do locations (e.g., individual workstations, file servers, etc.) have adequate fire detection and prevention facilities?			X	
	c)	Do workstations log-off when not attended during business hours, or after hours?			X	
	d)	Are passwords changed periodically?	X			
	e)	Is password modification: i. required by the Network operating system?	X			
		ii. manually controlled and enforced?		X		
		iii. if manual, are there procedures to ensure password changes?				X
	f)	Do policies and procedures prohibit user identification and confidential passwords to be written on or near the workstations or work areas?	X			
	g)	Are workstations with access to sensitive data shielded from view by unauthorized personnel?			X	
	h)	Are log-on system commands, and on-line transaction documentation manuals placed in a secure area when not in use?	X			
	i)	Has each user department designated a person to be responsible for controlling access to and use of the department's workstations?	X			
	j)	Is a log maintained of all departmental personnel authorized to use workstations?	X			
	k)	Are workstation IDs and passwords changed, when departmental personnel are terminated or transferred?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
	l)	Are there procedures to follow in order to move or acquire workstations?	X			
	m)	Is supervisory approval required in order to move or acquire workstations?	X			
9.		User Authorization and Identification:				
	a)	Are there specific additional, security-related procedures required to bring a workstation and the LAN on-line, outside of normal operating hours?	X			
	b)	Does the LAN security software uniquely identify each workstation and each workstation user?	X			
	c)	Can all workstation usage and transaction processing be identified to a specific individual?			X	
	d)	Are there software controls that limit the types of transactions/files/directories that are made available to individual users?	X			
	e)	Are there different levels of access restrictions that can be placed on agency workstations and users?	X			
	f)	Are all workstations protected by passwords or similar techniques?	X			
	g)	Do procedures prohibit the sharing of passwords by individuals in the same department?	X			
	h)	Does each user have his/her own password?	X			
	i)	Are there established procedures to set up passwords for individual workstation users?	X			
	j)	Are there documented procedures to follow when an authorized user forgets his or her password?	X			
	k)	Can all workstation users change their passwords at any time?	X			
	l)	Are workstation users precluded from personally deactivating their passwords?	X			
	m)	Does the security software detect and prevent repeated attempts to log-on to the network by guessing passwords?	X			
	n)	Are workstations that are left unattended for a specific period of time automatically logged off the network?			X	
	o)	Is automatic file or record locking available and being used by the LAN operating system to prevent simultaneous update?	X			
10.		Activity, Utilization, and Violation Reporting:				
	a)	Does the network operating system and/or security software report the following: i. Workstation activity?			X	
		ii. Workstation utilization?		X		
		iii. Access violations?	X			
	b)	Is there an individual responsible for following-up on workstation security violations?	X			
	c)	Are security violations promptly investigated and are the violator's superiors notified?	X			
	d)	Does the security software immediately report invalid access attempts?	X			
	e)	Are all workstation reports reviewed by independent data processing and/or user administrators on a weekly basis?			X	

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
11.		Network Operating System and Security Table Maintenance:				
	a)	Are security tables backed up frequently and rotated to an off-site storage location?	X			
	b)	Are there restrictions limiting access to the security table (e.g., additional passwords, codes, etc.)?	X			
	c)	Is there an audit trail that documents all parameter changes that are made to the network operating system and security tables?	X			
12.		Backup and Recovery:				
	a)	Are there documented procedures to guide LAN users in backing-up data from hard-disk drives and USBs?				X
	b)	Does a policy exist that defines adequate backup frequency and retention periods for backup data?	X			
	c)	Is track, disk, or server mirroring used to backup critical data?	X			
	d)	Do LAN software vendors provide backup and recovery training to LAN users?				X
	e)	Are there procedures to guide workstation users in recovering data from backup copies?				X
	f)	Are users responsible for their own hard disk backup if the information is not backed-up on a LAN?	X			
	g)	Is the LAN security administrator responsible for backing-up the file server(s)?	X			
	h)	Are there procedures for adequate in-house and off-site storage of backup data and programs?	X			
	i)	Is there an established source for replacing LAN hardware components when hardware failures occur?	X			
	j)	Is LAN hardware and software adequately insured against loss or damage?				X
	k)	Is recovery of LAN processing capabilities included in the agency's disaster recovery plan?			X	
	l)	Does your agency store e-mails in the event that this information may be used during litigation?	X			
	m)	Has your agency addressed the December 2006 electronic discovery-related amendments to the Federal Rules of Civil Procedure, (Rules 16, 26, 33, 34, 37, and 45, as well as Form 35) that electronically stored information must be produced during the discovery process?	X			
	n)	Has your agency created a policy and has a procedure been implemented that complys with the new regulation?	X			
	o)	Does your agency track e-mails?	X			
	p)	Are all incoming, outgoing, and internal e-mails captured and archived?	X			
13.		Software Acquisition and Application:				
	a)	Was agency MIS consulted to determine if desired software is: i. the most appropriate available?	X			
		ii. listed in the agency's application software catalog or endorsed by MIS?	X			
	b)	Was the warranty registration card filed with the vendor?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
14.		Documentation:				
	a)	Is there documentation for each recurring application (i.e., used more than once)?			X	
	b)	Is the application software catalog periodically updated?	X			
	c)	Do each of the applications have documentation?			X	
	d)	Does the documentation contain: i. a description of the application?	X			
		ii. a filename and backup filename?	X			
		iii. update frequency?	X			
		iv. sources of data including other filenames?	X			
		v. field definitions and names?	X			
		vi. a printout of formulas (especially for spreadsheet programs)?			X	
		vii. program execution instructions?	X			
		viii. backup instructions?	X			
		ix. copy of the software application?	X			
		x. sample printouts?	X			
		xi. distribution requirements?	X			
	e)	Are control, audit trail, and review procedures clearly set forth in software documentation?			X	
15.	a)	Does the agency maintain a list of all critical LAN/PC systems?	X			
	b)	Does the list provide a brief description of each system?	X			
	c)	If the answer to a) is "Yes," please provide an agency contact for the list. Agency Contact for List:	Anuraag Sharma			
		Title:	Director of Business Re-engineering			
		Telephone #	212-313-5184			
	d)	Please enclose a copy of the list as part of your Directive 1 submission. Have you enclosed the requested copy?	X			
16.		Communications:				
	a)	Has agency MIS been consulted prior to any communications networking?	X			
	b)	Are all network users and microcomputers uniquely identified?	X			
	c)	Are modems used on the network?				X
	d)	Is access to dial-up telephone numbers restricted (i.e., need-to-know basis only)?				X
	e)	Are dial-up lines monitored for repeated failed-access attempts?				X
	f)	Is the mainframe operator notified of repeated violations?				X
	g)	Is the line disconnected after repeated violations?				X
	h)	Is dial-up access restricted to only authorized users?				X
	i)	Are automatic call-back devices used where microcomputers can access the mainframe through a "dial-up" facility?				X
	j)	Is data that is transmitted over public lines encrypted?			X	
	k)	Do microcomputer users have access to sensitive data stored on other computers?			X	
	l)	Does the mainframe computer or LAN have a security software package that prevents unauthorized access to data?	X			
	m)	Have passwords been assigned to users?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
	n)	Are passwords kept confidential and changed periodically?	X			
	o)	Are computer logs available and reviewed by the appropriate supervisor?	X			
	p)	Can users upload or change data on the mainframe?	X			
17.		Physical Security - Hardware:				
	a)	Have all component serial numbers been recorded and stored in a secure location?	X			
	b)	Is the unit reasonably protected from unauthorized access?	X			
	c)	Are components secured, e.g., bolted down?			X	
	d)	Is the processing unit locked so that the cover cannot be removed and internal boards removed?		X		
	e)	Is there a policy requiring proper authorization before microcomputers are allowed to leave the property (e.g., night or weekend use)?	X			
	f)	Have adequate physical security policies for portable computers been developed, and distributed to users?	X			
18.		Physical Security - Data and Software:				
	a)	Has management identified those individuals authorized to use the microcomputer(s)?	X			
	b)	Have procedures been established for authorizing new users?	X			
	c)	Have critical or sensitive data files been identified?			X	
	d)	Are critical or sensitive data files protected from unauthorized access (by password)?			X	
	e)	Are critical or sensitive data files protected from unauthorized update?			X	
	f)	Are critical or sensitive data files encrypted?			X	
	g)	Are deleted or erased files really destroyed or overwritten so they cannot be recovered by utility programs?			X	
	h)	i. Are all accesses logged?			X	
		ii. Is the user uniquely identified?			X	
		iii. Is the date/time of access identified?			X	
		iv. Are the functions performed identified?			X	
		v. Is the microcomputer identified?			X	
	i)	Are private individual data sets secure from "browsing" by unauthorized network users?	X			
	j)	Have standardized file transfer formats been developed?	X			
	k)	Is critical data properly managed when downloaded?			X	
	l)	Is downloaded critical data used for analysis only, and not permanently stored on microcomputer storage media (e.g., USBs or hard drive units)?			X	
	m)	If data must be permanently stored in the microcomputer, is it encrypted or protected with password access?			X	
		TOTALS:	**114**	**7**	**35**	**12**

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

		Enter "X" below to indicate answer			
		Yes	No	Partial Compliance	Not Applicable
J.	**INTERNET CONNECTIVITY** The City makes use of the Internet to communicate, retrieve information, and provide information via City websites. It becomes increasingly important to assure that City data is reliable and adequately protected from unauthorized access, manipulation or destruction. The Department of Information Technology and Telecommunications (DoITT) has assumed the responsibility for information security policy formulation. It has published the Citywide Information Security Policies and Standards, which City agencies must comply with. Some of these have been classified as public documents and are available at: *http://www.nyc.gov/html/doitt/html/business/business_it_security.shtml* Others are internal and are available to authorized users on the City's intranet. Comptroller's Directive #18, "Guidelines for Computer Security and Control" provides additional guidance				
1.	Does your agency obtain Internet Connectivity through DoITT's central internet connection?	X			
2.	Does your agency use DoITT's centralized web content filtering?		X		
3.	Does your agency host internet applications?	X			
4.	Have the applications been accredited by the Citywide Chief Information Security Officer (CISO)?			X	
	If the answer is "Yes," please attach a list of each application including the date accredited				
5.	Has your agency designated a Chief Information Security Officer (CISO) and informed the Citywide CISO of same?	X			
	Name of individual:	Stanley Trepetin			
	Title:	Chief IT Security Officer			
	Telephone #:	212-313-5126			
6.	Have all employees who access information systems received a copy of the User Responsibilities Policy?		X		
7.	Are usernames and password required?	X			
8.	Do usernames and password comply with the User Account Management directive?	X			
9.	Are digital Certificates used?	X			
10.	Are tokens used?	X			
11.	Are SSL/HTTPS used?	X			
	i. Are they secured?	X			
12	Has your agency encrypted all data stored on disks, removable drives, tapes, flash memory cards, CDs, USB memory devices, laptops, smart telephones, and PDAs ?			X	
13.	Is all hardware inventoried?			X	
14	Is hardware protected from theft?			X	
15.	Are Virtual Private Networks used?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

		Enter "X" below to indicate answer			
16	Are consultants permitted to download City information?			X	
	If the answer is "Yes," describe the controls in place to prevent unauthorized actions (e.g.,misuse, theft of data).	We have comprehensive controls outlined in our security and private policies that			
17.	Are penalties defined in consultant contracts for the unauthorized downloading of City information?			X	
18.	Are firewalls used?	X			
	i. Are they in accordance with DoITT directives?	X			
19.	Are all applications monitored and configured to log system events?			X	
20.	Are intrusion detections systems in place?	X			

TOTALS: 13 2 7 0

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

K RISK ASSESSMENT, DATA CLASSIFICATION, AND INFORMATION SECURITY

The Department of Information Technology and Telecommunications (DoITT) has assumed the responsibility for information security policy formulation. It has published the Citywide Information Security Policies and Standards, which City agencies must comply with.
Some of these have been classified as public documents and are available at:
http://www.nyc.gov/html/doitt/html/business/business_it_security.shtml

Others are internal and are available to authorized users on the City's intranet.

DoITT's Data Classification Policy places responsibility on the agency head or designee for ensuring that agency information assets are appropriately categorized and protected. The value of the information must therefore first be assessed to determine the requirements for security protection. Data may be classified according to four levels: public, sensitive, private, confidential. The Data Steward is responsible for conducting this assessment.

		Enter "X" below to indicate answer			
		Yes	No	Partial Compliance	Not Applicable
1.	Has your agency conducted a data classification assessment in accordance with the Data Classsification Policy?		X		
2.	Has your agency classified data in accordance with the levels prescribed by the policy?		X		
3.	Has the Data Steward function been established and a Data Steward desginated?			X	
	If a data classification assessment has been conducted, please provide the document				
	Name of individual who conducted the asssessment:				
	Title:				
	Telephone #:				
4.	Can your agency's information transactions be reconstructed?			X	
5	Have access control measures been imposed on information and processes?			X	
6.	Are user activity logs in place to provide accountability?			X	
7.	Are city information users assigned different levels of access (system privileges) depending on their function and responsibilities?	X			
	TOTALS:	1	2	4	0

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

		Enter "X" below to indicate answer			
		Yes	No	Partial Compliance	Not Applicable
L.	**INCIDENT RESPONSE**				
	Despite an organization's best efforts, an information technology (IT) security incident may occur. When an incident occurs, the incident response process helps the affected organization respond to the event and resume normal operations as quickly as possible. Throughout the incident response process, the organization must have adequate controls to ensure that the following goals are achieved: determine the scope of the incident, maintain and restore data and evidence, maintain and restore services, determine how and when the incident occurred, determine the causes of the incident, prevent escalation and further incidents, prevent negative publicity, penalize or prosecute the attackers, and report the incident depending on its severity to appropriate agency management (i.e., CISO).				
1.	Has your agency developed an incident response procedure as defined by DoITT's Incident Response Policy?			X	
2.	Does the procedure classify incidents in accordance with DoITT's policy?			X	
3.	Are system compromises defined and how these events are to be handled and reported described?	X			
4.	Are information compromises defined and how these events are to be handled and reported described?	X			
5	Is unauthorized access defined and how these events are to be handled and reported described?	X			
6.	Is denial of service defined and how these events are to be handled and reported described?	X			
7.	Is the misuse of IT resources defined and how these events are to be handled and reported described?	X			
8.	Are hostile probes defined and how these events are to be handled and reported described?	X			
9.	Is suspicious network activity defined and how these events are to be handled and reported described?	X			
10.	Is excessive junk mailing defined and how these events are to be handled and reported described?	X			
11.	Is mail spoofing defined and how these events are to be handled and reported described?	X			
12.	Has an Agency Response Team been created and its responsibilities defined?	X			
13.	Have Procedures for this team been developed?	X			
14.	If your agency has procedures do they include: incident detection, incident containment, incident resolution, incident handling, incident logging, and incident prevention?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

		Enter "X" below to indicate answer			
15.	Please attach the latest version of your incident response procedure and any written procedure/descriptions addressing questions 3 through 14. Have you attached the requested documentation?			X	
	TOTALS:	12	0	3	0

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

		Enter "X" below to indicate answer			
		Yes	No	Partial Compliance	Not Applicable
M	**SINGLE AUDIT** The City receives federal funding and therefore must comply with the Federal Single Audit Act Amendments. These establish uniform requirements for audits of federal awards administered by states, local governments, and not-for-profit organizations (NPOs). Federal OMB Circular A-133, "Audits of States, Local Governments and Non-Profit Organizations" is the regulation issued by OMB to implement the Amendments. A-133 is effective for fiscal years beginning after June 30, 1996 and requires audits when an entity spends over $500,000 in federal awards for fiscal years ending after 12/31/03				
1.	Was the agency/covered authority audited by the City's external auditors as part of the FY 2007 New York City Single Audit (i.e., external auditors conducted fieldwork at the agency)?	X			
2.	Was the agency/covered authority audited by external auditors in FY 2007 who subsequently issued a separate Single Audit report on the agency/covered authority?	X			
3.	Did the agency spend more than $500,000 in federal awards in FY 2008?	X			
4.	Have all federal grants and other federal assistance been identified by federal funding source (CFDA#), including federal revenues, agency expenditures, and any adjustments?	X			
5.	Does the agency maintain a list of all subrecipients who receive federal funding through the agency?	X			
	If the answer is "Yes," please provide an agency contact for the list. Agency Contact for List:	Wilmer Ortiz			
	Title:	Director of Grants Administration			
	Telephone #:	212-788-4772			
6.	Does the agency maintain a list of vendors who received payments for goods and services that were federally funded?	X			
	If the answer is "Yes," please provide an agency contact for the list. Agency Contact for List:	Marissa Maziotta-Cohen			
	Title:	Director of Claiming			
	Telephone #:	212-232-2425			
7.	Does the agency receive federal funds which it transfers/passes through to other city agencies/covered authorities?	X			
	If the answer is "Yes," please provide an agency contact for this information. Agency Contact:	Wilmer Ortiz			
	Title:	Director of Grants Administration			
	Telephone #:	212-788-4772			
8.	Does the agency receive federal funds from other city agencies/covered authorities?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

		Enter "X" below to indicate answer			
		Yes	No	Partial Compliance	Not Applicable
	If the answer is "Yes," please provide an agency contact for this information. Agency Contact:	Wilmer Ortiz			
	Title:	Director of Grants Administration			
	Telephone #:	212-788-4772			
9.	Has the agency established a process for determining the difference between federal subrecipients and vendors in accordance with the Single Audit Act?	X			
	If the answer is "Yes," has the agency documented the process through written procedures?	X			
	If the answer is "Yes," please provide an agency contact for the written procedures. Agency Contact for written procedures:	Marissa Maziotta-Cohen			
	Title:	Director of Claiming			
	Telephone #:	212-232-2425'			
10.	Has a specific individual been assigned to monitor all federal funding & applicable agency expenditures?	X			
	If yes, give name of individual:	Marissa Maziotta-Cohen			
	Title:	Director of Claiming			
	Telephone #:	212-232-2423			
11.	Has a specific individual been assigned to monitor Single Audit/A-133 compliance? Please identify below, if the individual is different from the one identified in Question 10.	X			
	Name of individual:	Sara Packman			
	Title:	ASSISTANT COMMISSIONER			
	Telephone #:	212-219-5044			
12.	Is a list maintained of subrecipients who directly contract for A-133 Audits themselves?	X			
	If the answer is "Yes," please provide an agency contact for the list. Agency Contact for List:	Sara Packman			
	Title:	ASSISTANT COMMISSIONER			
	Telephone #:	212-219-5044			
13.	Does the agency follow-up on all A-133 related audits to ensure appropriate and timely corrective action (e.g., issue management decisions on audit findings within six months of receiving the report)?	X			
	If the answer is "Yes," has the agency assigned this responsibility to a single individual or unit? Please identify below, if the individual is different from the one identified in Question 12. Name:	Sara Packman			
	Title:	ASSISTANT COMMISSIONER			
	Telephone #:	212-219-5044			
14.	Apart from A-133 requirements, does the agency employ CPA firms to conduct audits of agency funded services (i.e., delegate agency audits/Comptroller's Directive #5)?	X			
15.	Are the Procurement Policy Board Rules and Comptroller's Directive #5 followed in procuring these additional audits?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

		Enter "X" below to indicate answer			
		Yes	No	Partial Compliance	Not Applicable
16.	Does the agency have procedures/practices to monitor agency expenditures apart from those covered by A-133 and delegate agency CPA audits?	X			
17.	Has the responsibility for implementing and monitoring the effectiveness of the procedures in Question 16. been assigned to a specific individual?	X			
	If yes, give name of individual:	Andrew Rein			
	Title:	COO/Executive Deputy Commissioner			
	Telephone #:	212-788-5347			

TOTALS: 18 0 0 0

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
N		**LICENSES/PERMITS** The key elements are to ensure that licenses and permits are appropriately issued, accurately recorded, and any applicable fees received are promptly deposited and accurately recorded.				
1.		Segregation of Duties:				
	a)	Are responsibilities for the authorization, preparation, issuance and recording of licenses segregated?	X			
	b)	Are the responsibilities for application review, recording cash receipts and inspection segregated?	X			
	c)	Are all new license/permit applications reviewed for completeness?	X			
2.	a)	Recordkeeping: Are all application and renewal fees promptly recorded in FMS and deposited?	X			
	b)	Are individuals promptly notified if their applications are rejected?	X			
	c)	Is a permanent record of all issued licenses/permits maintained?	X			
	d)	Is the disposition of all licenses/permits, including voids, maintained in a current log?	X			
	e)	Are post issuance checks performed on samples of approved licenses/permits to verify that all approval requirements had been met?				X
3.		Safeguarding of Assets:				
	a)	Are required bonds properly recorded and invested in interest-bearing accounts through the City Treasury?				X
	b)	Are the blank, imprinted licenses/permits properly stored and secured?	X			
	c)	Is a periodic inventory of blank licenses/permits made?	X			
	d)	Are the blank license/permit forms pre-numbered?	X			
	e)	Are the blank pre-numbered license/permit forms accounted for numerically, including voids?	X			
4.		Control Procedures:				
	a)	Does the Licensing Department review all licenses/permits prepared by the Data Processing Department on a daily basis?	X			
	b)	Is the number of employees who are authorized to print licenses/permits restricted?	X			
	c)	Is there a daily reconciliation of the printed licenses/permits to the authorized licenses/ permits?			X	
		TOTALS:	**13**	**0**	**1**	**2**

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

		Enter "X" below to indicate answer			
		Yes	No	Partial Compliance	Not Applicable
O	**VIOLATIONS CERTIFICATES** Violations should be appropriately issued and recorded promptly and accurately. Inspection and collection procedures should be adhered to and monitored. Following up on outstanding violations is important and may be the most significant control feature in the entire process.				
1.	Segregation of Duties: Is the responsibility for issuing violation notices separated from the responsibilities for processing the notices or collecting the violation fees?	X			
2.	Monitoring Procedures:				
a)	Are violation notices followed up in a timely manner when a violator fails to appear at a hearing?	X			
b)	Is timely legal action taken when a violator fails to pay civil penalty fines?			X	
c)	Is an accurate, up-to-date log maintained showing the status of each violation notice?	X			
d)	Do controls over violation notices allow processing and collection of violation fines on a timely basis?	X			
e)	Are controls in place and followed to ensure that Field Inspectors are following Agency Standard Operating Procedures in preparing violation notices?	X			
f)	Are Field Inspectors prohibited from receiving cash/check payments for violations?	X			
g)	If Inspectors are allowed to accept cash/checks, are there controls that would mitigate the improper disposition of the cash/check?	X			
h)	Are field Inspectors' routes periodically rotated?	X			
	TOTALS:	**8**	**0**	**1**	**0**

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

		Enter "X" below to indicate answer			
		Yes	No	Partial Compliance	Not Applicable
P	**LEASES/CONCESSIONS/FRANCHISES** LEASES/CONCESSIONS/FRANCHISES - Agencies that have Lease, Concession and/or Franchise agreements should closely monitor the lessees', concessionaires' or franchisees' compliance with these agreements. Agencies must also follow the requirements established by the City Charter, section 371, and the Franchise and Concession Review Committee. Fulfilling legal and monitoring requirements will enhance internal controls in this area.				
1.	Is certification obtained that the proposed lessor has fully satisfied all tax obligations outstanding as of the date of the lease?	X			
2.	Are copies of lease/concessions maintained with a current name and address of the party to whom the billings are to be sent?	X			
3.	Are proposed authorized resolutions submitted to the Mayor for all franchises after 1/1/90?	X			
4.	Are all franchises after 1/1/90 reviewed and approved by the Franchise and Concession Review Committee?	X			
5.	Do all concessions after 1/1/90 comply with the procedures established by the Franchise and Concession Review Committee?	X			
6.	Are all concessions after 1/1/90 that differ from the procedures established by the Franchise and Concession Review Committee (except those not subject to renewal and with a term of less than 30 days) reviewed and approved by the Committee?	X			
7.	When franchise agreements after 1/1/90 include rights of renewals, are the renewals less than an aggregate of 25 years?	X			
8.	Was a public hearing held, before each franchise contract, in accordance with the regulations of the City Charter, Section 371?	X			
9.	Has a copy of each concession agreement been registered with the Comptroller?	X			
10.	Are formal standards used to prepare estimates for alteration costs of leased space?	X			
11.	Does management formally review and approve cost estimates for alteration costs of leased space?	X			
12.	Are all bids that are obtained by the lessor for alteration costs reviewed by the agency?	X			
13.	Is compliance to prior contract requirements verified, before authorizing contract renewals?	X			
14.	Does this compliance check include follow up to determine if any additional assessments per audit have been collected?	X			
	TOTALS:	**14**	**0**	**0**	**0**

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

Q. INTERNAL AUDIT FUNCTION

The existence of an internal audit function in an agency is an aid in establishing and monitoring internal control procedures. The Internal Audit group should be familiar with GAO's yellow book requirements (generally accepted government auditing standards - GAGAS, July 2007 Revision) and may be required to follow its requirements if the agency or the function/program to be audited is federally funded. The key requirements are that the staff be independent, trained, competent and provide the agency with audit/review results and recommendations.

The head of the internal audit function traditionally reports administratively to the head of the organization and functionally to the Audit Committee (if one exits).

The "Audit Committee" may be defined as a body charged with the responsibility of providing oversight of the entity's financial reporting process (including the internal control environment). The Audit Committee's responsibilities generally include:

- Ensuring the independence of the external auditors, and the adequacy of their audit scope

Approving the scope of the internal audit plan, ensuring the quality of the internal audit Function by requiring adherence to professional standards, and responding to issues that may be raised by the internal audit Function
- Setting the tone for integrity in the financial reporting process, and
- Ensuring that any reports to external regulators are accurate and filed in a timely manner.

		Enter "X" below to indicate answer			
		Yes	No	Partial Compliance	Not Applicable
1.	Does the agency have an internal audit function to examine and evaluate the adequacy and effectiveness of its policies and procedures?	X			
2.	If the agency has no formal internal audit function: a)are built-in internal checks in place?				X
	b) are self assessments or management reviews conducted at least annually?				X
	c) are risk assessments or management reviews discussed with officials/managers who are authorized to take action on findings/conditions and proposals/recommendations?				X
3.	Does the internal audit function follow Generally Accepted Government Auditing Standards (GAGAS), i.e., the GAO Yellow Book?				X

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
4.		Does the internal audit function adequately cover all of your audit concerns?			X	
5.		Has your internal audit function been affected by any recent organizational changes: Unaffected?	X			
		Positively affected?	X			
		Negatively affected?		X		
6.		Has the number of reports or the scope of completed audits been affected by any recent organizational changes: Unaffected?		X		
		Positively affected?		X		
		Negatively affected?		X		
7.		Has the contracting out of a significant internal audit workload resulted in more effective audit coverage?				X
		At the same or less cost?				X
8		General Audit Standards:				
	a)	Are there adequate controls to ensure that the internal audit staff collectively possess adequate professional proficiency for the tasks required?	X			
	b)	Is the internal audit unit organizationally independent of the staff or line management function of the audited entity?	X			
	c)	Does the internal audit unit follow up on findings and recommendations from previous internal and external audits that could have an effect on the current audit objectives?	X			
	d)	Has the internal audit unit established a system of internal quality control to provide reasonable assurance that it is following prescribed audit policies and procedures, and that it has adopted and is following applicable auditing standards?		X		
	e)	Has the internal audit unit established procedures to determine whether the staff assigned had any personal impairments that could prevent them from reporting audit findings impartially?	X			
9.		Field Work Standards:				
	a)	Does the unit prepare an annual audit work plan based on a risk assessment analysis?	X			
	b)	Was a written audit program prepared for each audit assignment?	X			
	c)	Does the audit program detail the audit steps, procedures, and methodologies to be followed by the assigned staff?	X			
	d)	Does the unit maintain adequate controls to ensure that its audit staff is properly supervised?	X			
	e)	In conducting the audit, does the audit team make an assessment to determine if the audited entity is complying with applicable laws and regulations?	X			
	f)	In conducting the audit, does the audit team assess the effectiveness of the audited entity's internal control structure relating to the audit objectives?	X			

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

			Enter "X" below to indicate answer			
			Yes	No	Partial Compliance	Not Applicable
	g)	Is the audit designed to provide reasonable assurance of detecting abuse or illegal acts that could significantly affect the audit objectives?	X			
	h)	Are there adequate controls to ensure that the audit team collect sufficient competent evidential matter to afford a basis for an opinion?	X			
10.		Reporting Standards:				
	a)	Are written reports prepared detailing the audit findings and recommendations?	X			
	b)	Are audit reports issued on a timely basis?	X			
	c)	Are audit reports distributed to officials/ managers who requested the audit and/or who are authorized to take action (s) on audit findings and recommendations?	X			
11.		Does the head of the Internal Audit Function report to the chief executive of the agency?		X		
		If not, please identify the agency executive to whom the head of Internal Audit does report. Name:	Andrew Rein			
		Title:	COO/Executive Deputy Commissioner			

Additional questions follow; see note below.

TOTALS: 18 6 1 6

NOTE: The remaining questions - # 12 through # 17 - only apply to agencies that issue their own financial statements; i.e., independent agencies. If this describes your agency, enter "X" in the box below and continue. Otherwise, STOP HERE.

➔ □ Independent agency issuing own financial statements

12.		Is your agency responsible for issuing its own financial statements?				
13.		If your agency is responsible for issuing its own financial statements, does your agency have an Audit Committee?				
14.		Are a majority of the Audit Committee members independent of agency senior management?				
		Are some members totally independent of the agency?				
		Are some members totally independent of the City?				
15.		Is there a written Charter specifying the Audit Committee's responsibilities, administrative structure, and rules of operation?				
16.		Is the Audit Committee responsible for:				
	a)	overseeing the agency's financial reporting process?				
	b)	participating in the selection of the agency's external auditing firm?				
	c)	ensuring the independence of the external auditors?				
	d)	ensuring the adequacy of their audit scope?				
	e)	approving the scope of the agency's Internal Audit Plan?				
	f)	ensuring the quality of the Internal Audit Function by requiring adherence to professional standards?				

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

		Enter "X" below to indicate answer			
		Yes	No	Partial Compliance	Not Applicable
g)	addressing issues raised by the internal audits?				
h)	monitoring compliance with the agency's governing Board policies?				
17.	Does Internal Audit report its audit findings to the Audit Committee?				

TOTALS:

NOTE: Cells in the "Explanation" column will automatically expand as needed to accommodate entered text.

AGENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

AGENCY'S EXPLANATION OF ALL "NO" AND "PARTIAL COMPLIANCE" RESPONSES

Part Letter	Question #	Explanation
Part A	6. a-c	Partial. Although DOHMH continues to achieve most targets for goals/outcomes/outputs, certain programs have not fully met stated expectations.
Part A	8. a,c-g	Partial. Periodically, in the course of reviews of operational and administrative processes and outcomes, the need to revise outdated policies and procedures is identified. Through establishing an internal audit unit, DOHMH is conducting more frequent risk surveys/assessments and audits to ensure that policies and procedures throughout the agency are up-to-date, and that they have been communicated appropriately. Policies and procedures are also regularly updated to reflect new technologies and new best practices.
Part A	14	Partial. DOHMH works to actively recruit and retain qualified personnel, and to address areas of high turnover in particular. In 2008 the agency had an overall turnover rate of 10.29%. Turnover rates vary significantly across units.
Part A	17	No. There are no DOHMH unresolved audit findings that are "significant".
Part B	2a	Partial. Office of Vital Records window receipts are processed by the Cashiering Unit, picked up by the armored car service, for deposit on the next business day. Checks received in the mail for certified copies of birth and death certificates are locked in a secure cabinet until they are reviewed and processed for deposit. In FY'08, checks by mail were deposited by an average of 3.1 calendar days for birth certificates and 11.9 calendar days for death certificates after receipt.
Part B	2f, g, h	Yes with explanation. Office of Vital Records receives a very large volume of mailed-in requests that are places unopened in a secure cabinet until the requests are reviewed, and the checks endorsed and processed. The Cash Management System operators endorse checks and money orders when they process them, which is separate from the accounting unit. Checks are listed and grouped on the deposit slips by amount, and receipts are reconciled to deposit slips. An armored car picks up the checks for delivery to the bank within 24 hours of processing.
Part B	2i	Yes with explanation. Receipts are given for all transactions; receipt numbers are generated by the Vital Records Cash Management System as applications are electronically cashiered.
Part B	2i	Yes with explanation. Receipts are given for all transactions; however payments made to the lock boxes do not receive receipts.
Part B	2o	Yes with explanation. The high volume of checks received by Vital Records precludes preparing an individual checklist. Checks are listed and grouped on the deposit slips by amount.
Part B	3. e	No. For checks under $25, they are cancelled. Checks over $25, stop payment orders are issued.
Part C	14	No. Petty Cash slips are not prenumbered. Petty Cash slips are downloaded directly from the intra-net.
Part D	4 a,b	Partial. A formal write-off procedure has been developed for the Administrative Tribunal fines and is currently being developed for other receivables.
Part E	5. b	No. FMS Purchase Order and Purchase Requisition forms are not pre-numbered. Purchase Orders are assigned sequential, unique numbers by the Procurement Office. The F.M.S. system automatically assigns a unique number to the voucher when processed by the Internal Accounting Office.
Part E	5. g	No. Additional approval is not needed as long as invoices are in agreement with the approved purchase orders.
Part E	5. j	Partial. Approval for payment in a timely manner is contingent upon the timely receipt of the receiving report and inspection report from the receiving unit.
Part F	1a-2q	Note, for this entire section (F) DIIT is responding to the following types of equipment: PC, Laptop, Printer, Server and Infrastructure Devices. DIIT is not answering on behalf of small-cost items like $2 cables or $8 USB drives.
Part F	1a	Partial. DIIT enhanced the inventory policy and is communicating it to all relevant employees.

Part Letter	Question #	Explanation
Part F	1b	Partial. Going forward into 2009, the enhanced policy described in F.1(a) will be used here. For example, Programs will not be able to purchase equipment until DIIT's approval, which will enable DIIT to keep accurate inventory.
Part F	1 c	Partial. In the laboratories, storeroom personnel have responsibility for both stock and recording functions and are monitored by the supervisor. In the separate pharmaceutical and vaccines/ biologics distribution units, the pharmacists have responsibility for supervising stockroom staff and maintaining the detailed records.
Part F	1d	Partial. By virtue of the policy in F.1 (a) going forward into 2009, purchases will require DIIT's approval, and only appropriate inventory will be allowed to be maintained.
Part F	1e	Partial DIIT has asked for summer interns to do the inventory counts for computer inventory. DIIT has completed inventory counts of 4 Programs/Bureaus in 2008 and plans to complete the remainder in 2009. Public Health Laboratories is currently centralizing and organizing inventory items by type/use to improve tracking ability.
Part F	1.f	No. Consumable inventories are conducted by supply staff combined with other warehouse staff and/or laboratory staff. Staffing constraints limit the ability to segregate tasks. Supervision at the sites is provided by bureau managers and supervisors, or the pharmacists in the pharmaceutical and the vaccines/ biologics distribution units. An automated inventory management system is being implemented to improve controls over vaccines and pharmaceuticals. For DIIT, an initial survey of equipment was necessary to build an inventory. Physical inventory management is being improved by acquisition of new automated technology that will provide "real time" inventory management and by the creation of internal processes that allow for independent monitoring of inventory by staff that are not part of the program being audited.
Part F	1.h	Partial.-Not all computer equipment is tagged. See (I) 1.e.
Part F	2. c - m	Partial. The agency is reviewing its inventory records and will be modifying its practices and procedures to bring operations into compliance with the recently issued requirements for Directive 30. DOHMH staff has been meeting with Office of the Comptroller Accountancy personnel to address a variety of issues concerning capital assets. In addition, DOHMH has obtained approval from OMB to establish a new computerized inventory record keeping system, which eventually will greatly enhance controls over agency inventories. For computer equipment, some mapping between physical inventory and inventory records takes place via Help Desk calls wherein calls are generated on behalf of specific hardware and serial numbers. These can be associated back to inventory records.
Part F	2k	N/A with explanation. None of the City owned IT equipment is allowed for re-sale.
Part F	2k,q	N/A because we do not do any sales of capital assets.
Part F	2n	Partial. Fiscal Management sent out Quarterly Fixed Assets Crystal Reports to programs for their reconciliations.
Part F	2.n	Partial. Fiscal Management sent out Quarterly Fixed Assets Crystal Reports to programs for their reconciliations
Part F	2o	N.A with explanation. Metal Tag for IT equipment purchased by Capital Fund was not distributed by the Procurement Office since 2005.
Part F	2o	Partial. See (I) 1. e. regarding tagging.
Part F	2q	N/A with explanation. All IT equipment deliveries made to our premises are in proper protection by vendors. Manufacture warranty ensures return policy for complete satisfaction.
Part H	1b.i	Partial. DIIT does focus on long-term infrastructure issues. The goals include centralizing the IT infrastructure, reducing IT complexity, consolidating the servers, and utilizing improved identity management tools. With regard to software/applications, DIIT responds, evaluates, and implements applications based on Bureaus' requests. Since it is unclear what Bureaus will request there is less of a long-term plan for applications per se, but primarily responses to requests.
Part H	1d	Partial . The Governance, Change Control, and Inventory Control policies and procedures will be updated and implemented.
Part H	1e	Partial. Every appropriate attempt is made to conform to DOITT policy. As these change, DOHMH discusses with DOITT the best way to proceed. Sometimes DOHMH will utilize an equivalent, but different, security policy or architecture.
Part H	1.i	Partial. An IT security audit group was started in the Office of the Chief IT Security Officer in 2007. The purpose is to provide IT security audit and assessment services for Programs during application/service procurement or new development.
Part H	1. g.i, iii, v, vi	No. There are no separate applications maintenance or systems programming groups. Instead, there is one pool of software developers which get assigned to these different tasks as needed.
Part H	2a	N/A with explanation. We are not doing new systems development in the mainframe environment as DIIT has moved to a web-application environment, which is more flexible and for which expertise is more readily available. Hence, no need to follow DOITT's policies in this case.

Part Letter	Question #	Explanation
Part H	2c	Partial. A formal Quality Assurance function is not required because we have limited new mainframe development. Instead, we thoroughly test including "user acceptance" testing.
Part H	2d	No. The mainframe enhancements are too small to record the costs for them.
Part H	3a, b, c, d	N/A with explanation. We are not doing new systems development in the mainframe environment as DIIT has moved to a web-application environment, which is more flexible and for which expertise is more readily available.
Part H	5a	Partial. Each mainframe application has their own approach regarding documentation.
Part H	5. b.iv	No. When these mainframe applications were developed, comparisons were not required. Furthermore, mainframe applications are being phased out for DOHMH in favor of web applications.
Part H	5. d	Partial. Some mainframe applications are over 15 years old. For "newer" mainframe applications, there are programming standards, but not for the "older" ones. We don't plan to update standards because mainframe applications are being phased out.
Part H	5. f	Partial. We recognize the documentation of older systems is not extensive. To mitigate the risk of loss of mainframe specialists, we plan to explore bringing in consultants to document and/or maintain systems and pursue our initiatives of migrating systems off the mainframe by mid 2010.
Part H	7. b	Yes with explanation. Most mainframe equipment belongs to, and is physically located at DOITT facilities. The few mainframe assets which DOHMH does own are tagged.
Part H	7. f	No. This capability does not exist for the mainframes DIIT works with.
Part H	8. e	N/A with explanation. We believe DOITT maintains detailed logs to analyze system operations and performance but it is unclear for how long.
Part H	8.f	Partial. The basic information available from the mainframe via console or some of the printouts available is sufficient for DOHMH needs. For detailed analysis regarding particular problems, DIIT management does not have access to DOITT's mainframe logs but can contact DOITT to request that log information be relayed to DIIT.
Part H	9.a-d, f	N/A with explanation. DOHMH does not maintain its own mainframes, which are housed at DOITT. Hence, these questions, regarding mainframe disaster recovery, should primarily be addressed by DOITT. However, see answers to questions (H) 9.e and g-h below.
Part H	9.e	Partial. DOITT handles disaster recovery issues for DOHMH mainframes although we have some ability to do recovery with respect to our mainframe operators and users. For example, if terminals fail we can emulate terminals on a PC.
Part H	9.g-h	Partial. DOHMH is ready to participate with DOITT when the latter drives disaster recovery testing. We are not privy to a set schedule, e.g. semi-annual or otherwise, when DOITT creates such tests. DOHMH last participated in DOITT-driven disaster recovery testing in late 2005 and/or early 2006.
Part I	1.b	Partial. The answer here is similar to that of (H) 1.e. We comply to some degree; not all policies have been completed; and questions of whether deviations can be accepted or mitigated in other ways will be discussed with DOITT. Contact Stanley Trepetin at 212-313-5126 with questions.
Part I	1.c	No. This answer is similar to (H) 1.e. However, DOHMH has its own set of acceptable use and confidentiality policies which require controls which are quite similar to those of DOITT's User Responsibilities Policy. We are compliant with our own policies.
Part I	1.e.vii	Partial. Inventory of enterprise and DIIT-managed hardware and software is in place. The inventory management system implemented in 2006 to allow for distributed management of hardware and software continues to be used. In 2008, 100% of DOHMH hardware purchases were approved through DIIT. 80% were delivered through DIIT and thus DIIT had control over the inventory and tracking information. The other 20% of the hardware was delivered to the Bureaus directly. In this case, DIIT’s inventory is updated when DIIT receives a service call for installation and configuration. Additional clarifications on who will be managing which type of Inventory will be discussed within Agency in 2009.
Part I	1.g	Partial. This is engraved by the vendor of the PCs and related hardware or distinctively labeled through other means. In 2006, 25% of Agency equipment was labeled this way, and all future purchased equipment will be so labeled. We also use the equipment's serial number to track the equipment when its owner contacts the help desk for service. DIIT does not track mice, monitors, printers, or keyboards, however.
Part I	3.d	No. DOHMH does not own a mainframe computer, although DOITT has mainframe capability. However, new DOHMH functionality is not being designed for the mainframe due to the flexibility of web-based applications.

Part Letter	Question #	Explanation
Part I	5.b	No. DOHMH IT purchases all necessary IT equipment always based on the State OGS or the Fed's GSA contracts, therefore, the risk has been very minimum in the past. However, due to the current nationwide economy difficulties, some contracted vendors filed Chapter 11. Gateway is one of them that directly affects the DOHMH as we still have 900 PCs and 30 servers that are under its extended warranty but out of support and maintenance.
Part I	7.a	Partial. Such a list exists for large-scale or enterprise-wide applications within DOHMH but not necessarily for the smaller applications developed or acquired by Bureaus on their own. We will address some of the disconnect between Bureau software development and DIIT awareness in 2009 by enforcing the IT Governance process, introduced in 2007.
Part I	7.b	Partial. Same reasoning as (I) 7.a
Part I	7.b.i	Partial. As per the new IT governance process, depending on the monetary value of the project, the Information Technology Steering Committee, office of the Chief Operating Officer, or DIIT may get involved in deciding whether a new IT project is to proceed. The greater the value of the project (e.g. Total Cost of Ownership over 5 years > $ 1million for Bureau/Program-managed projects), the higher the level of management must get involved in approval. However, this is not always reflected in the list, especially for systems which begun to be developed before the governance process was put in place. Nevertheless, DIIT and senior DOHMH management is aware of the progress of current systems.
Part I	7.b.ii	No. As indicated in comments like (H) 1.e, DOITT has not always made clear for which applications accreditation must be accomplished. For the bulk of our new applications, per DOITT guidelines, accreditation should not be necessary. One DOHMH application, Animal Licensing, has been accredited by DOITT.
Part I	8.a	Partial. Program offices are locked, and there is building-level security. Equipment is not always bolted. Smaller data centers have 24x7 video monitoring (lights left on at all times) and have key card access. In 2008, a new centralized data center with high security features was built and most DOHMH servers were moved to that location.
Part I	8.b	Partial. The new data center will have such facilities. As various equipment migrates to the new data center, key servers, workstations, etc. will have such protection. Further, most confidential and critical data are typically backed up nightly from network drives. Even if a workstation were to be damaged, its data should often be recoverable.
Part I	8.c	Partial. They "lock" via an automatic screen saver, but users are not logged off automatically. Users must do that themselves.
Part I	8.e.ii	No. These procedures are not manual and are enforced at the network level.
Part I	8.g	Partial. This practice is usually in place, including the use of protective monitor screens, although DOHMH does not monitor compliance. As budgetary limitations give way to permit more auditing of DOHMH facilities, any deviation from compliance in this regard will be noticed and an action plan will be put in place to install additional controls at those workstations which permit sensitive data to be casually seen by unauthorized passerby's.
Part I	9.c	Partial. For local use of applications (e.g. Microsoft Word) it is not possible to monitor each usage. Logins are monitored, and individual server-managed applications maintain their own transaction logs.
Part I	9.n	Partial. See response to (I)8.c.
Part I	10.a.i	Partial. Under Microsoft Active Directory, monitoring individual workstations is no longer possible. Activities such as checking for installed software, assessing memory usage, assessing CPU utilization, and other workstation monitoring cannot be easily done. Microsoft does provide a workstation monitoring tool (SMS), which we have purchased but not yet implemented. Having such monitoring is not required but does improve the ability to ensure appropriate policies are followed.
Part I	10.a.ii	No. Under the Microsoft Active Directory infrastructure it is not possible to monitor more detailed workstation activities other than just basic network activities. Again, monitoring workstation utilization across the Agency is not required. If there is a problem, the user can call the help desk to address the problem. Servers are monitored more closely.
Part I	10.e	Partial. The user is not required to review any workstation reports, and there is no central (Agency-wide) available tool to readily do this. However, servers along with the critical data they contain are often monitored. From a security point of view, if there is a problem, recognized by the user or DIIT, we can get the help desk or the local technician to address it. We do run the Qualys tool, which on a monthly basis captures any security vulnerabilities on the workstation, but not all of them.
Part I	12.a, d, e	N/A with explanation. To avoid security risk, we have users store all files on the server (not locally or on removable media) and handle backup centrally. The end result is that most important data are on centrally-managed and secured network drives. There is no need for users to backup their own storage, and hence no need to train them on recovery.

Part Letter	Question #	Explanation
Part I	12.j	N/A with explanation. The city is self-insured but it is unclear to what degree small items are covered under such a policy.
Part I	12.k	Partial. Disaster recovery capabilities are spread out over several documents within DOHMH and there is no current comprehensive document. In 2009, a new disaster recovery document should be produced. Please contact Don Weiner at 212-313-5122 for details.
Part I	14.a, c	Partial. Older applications may not have sufficient documentation.
Part I	14.d.vi	Partial. The documentation may not always have it but some formulas can be readily made available.
Part I	14.e	Partial. A number of current applications have audit trails and they are used if there is a problem or to understand what led to a particular event. However, they are not monitored to systematically track for anomalies, and are more used on an exception basis. Documentation on the audit trails and usage rarely exists, though. In 2008 and going forward we introduced a process for creating audit logs for newly-developed web applications which will be incorporated into the Software Development Lifecycle. This process much more specifically defines what kind of logs must exist and when and how they will be monitored.
Part I	16.k	Partial. In general, workstations are set up and Programs make sure only certain individuals get access to others confidential data. However, this is not always fully enforced across the entire Agency. DOHMH has put in a request for capital funds to purchase Data Leak Prevention software in 2008, and should do so if the money is approved. We hope this will happen in 2009.
Part I	16.j	Partial. For "public" data, there is no concern. For sensitive data, this is a requirement in DOHMH policy. However, whether all applications in the Agency comply with this requirement is not always clear. The Chief IT Technology Officer (CISO) conducts assessments of new applications and major application changes, and if confidential data are to be transmitted over a public network like the Internet, encryption is required. But the CISO has not been able to audit the dozens if not hundreds of small and large applications in the Agency for compliance. As in I.16(k), we have applied for capital funds to purchase a Data Loss Prevention platform in 2008 but so far it has not been approved. Also, we have applied for capital funds for email encryption to prevent the transfer of unencrypted sensitive data over the Internet. So far, it has not been approved.
Part I	17.c	Partial. Program offices are locked, and there is building-level security. Equipment is not always bolted. Smaller data centers have 24x7 video monitoring (lights left on at all times) and have key card access. In 2008, a new centralized data center with high security features was built and most DOHMH servers were moved to that location.
Part I	17.d	No. For the machines DIIT purchases today (and in general for all PCs today), it is not easy to prevent someone from opening the cover and removing some of the innards.
Part I	18.c	Partial. As indicated in H.16(k), DITT plans to purchase a Data Leak Prevention solution which would identify where the sensitive data are.
Part I	18.d, e	Partial. DOHMH 's policy requires employees to protect sensitive data and to keep all passwords secured. Password protection is used to prevent unauthorized access to DOHMH's systems, and passwords are periodically updated for all personnel changes. DOHMH is also exploring ways to enforce DOHMH's Confidentiality Policy for safeguarding system data, and has applied for the purchasing of a Data Loss Prevention platform.
Part I	18.f	Partial. It is the policy of DOHMH to encrypt laptops that may contain sensitive data. However, some programs data may not be encrypted.
Part I	18.g	DOHMH's policy is to expunge datasets and files when they are no longer needed by the program. The electronic expunging is carried out by DIIT in coordination with the program. However, each program has its own protocol for when data will be expunged.
Part I	18.h.i-v	Partial. Most applications have an audit trail capability. Access to workstations is controlled by password implemented by Windows' logging controls. To improve controls, the agency is considering the procurement of a Data Loss Prevention platform.
Part I	18.k-m	Partial. "Critical" data can be downloaded for both analysis and transportation. There are agency-wide policies that prohibit and permit various uses of critical data. The agency has purchased encrypted USB drives so that if critical or sensitive data may be transported to another location, it can be encrypted, and must be encrypted per policy.
Part J	2	No. DIIT utilizes its own web content filtering, Websense.
Part J	4	Partial. One DOHMH application, Animal Licensing, has been accredited by DOITT. For applications requiring accreditation, DIIT is pursuing accreditation. For older applications, which are still in use, DIIT has not pursued accreditation. DIIT continues to discuss with DOITT on how to identify applications that need to be accredited.
Part J	6	No. See I.1(c)

Part Letter	Question #	Explanation
Part J	12	Partial. Some of the media, such as many of the Agency's laptops, the USB drives that have been recently purchased, and a few databases across the Agency do have and use encryption capability. It is also Agency policy that all future laptops and transportation of sensitive data across facilities use these encrypted USB drives. Older laptops and some other media are not so encrypted. As the Chief IT Security officer conducts assessments of Bureau programs and applications, these are discovered and rectified.
Part J	13	Partial. Most hardware is inventoried, but some programs purchase their own hardware without obtaining DIIT's approval. As indicated above, new purchase procedures are being implemented throughout the agency to address this concern.
Part J	14	Partial. See I.8(a).
Part J	16	Partial. DIIT has controls in place relating to use and access sensitive data by consultants/contractors. Other Bureaus especially those dealing with very sensitive medical data, also have such controls. Public data does not require a significant security as sensitive data. For sensitive data, DIIT uses VPNs, require encryption of data in motion, and require other controls related to this data, including the signature of confidentiality agreements. DIIT also has comprehensive controls outlined in our security and privacy policy.
Part J	17	Partial. New contracting language has been created in 2008 and will be introduced into actual contracts in 2009 to make vendors/consultants more accountable to DOHMH from a security perspective. Earlier DOHMH contracts do not always consistently detail DOHMH security and policy.
Part J	19	Partial. See I.14(e).
Part K	1	No. Classifying all existing data at DOHMH is a mammoth undertaking. There are literally millions if not tens of millions or more documents, files, databases, voicemails, etc. DOHMH addresses data classification on a project by project basis. At that time, the CISO will take into account the nature of the data involved and classify the data. In addition, DOHMH is considering the purchase of a Data Loss Prevention solution, which would facilitate such classification.
Part K	2	No. As indicated in K.1, DOHMH addresses data classification on a project by project basis. DOHMH has its own data classification that it has been following when considering security controls for application development and/or upgrades.
Part K	3	Partial. When the CISO gets involved in a security assessment, he becomes the Data Stewart (from DOITT's perspective), with input from the business owner.
Part K	4	Partial. DOHMH has robust database platforms supporting many databases that can support transaction reconstruction for various failing conditions, such as database-down. While most applications have audit trail, they are not monitored and/or systematically tested.
Part K	5	Partial. As indicated before in I.16(k) and I.18(d) and (e), security policies have been established. However, access to applications and data use is within programs' responsibilities.
Part K	6	Partial. For new application, audit logs are created to provide accountability. Other applications may have audit trail capabilities, they are not always monitored and/or systematically testing for user's activities.
Part L	1	Partial. A basic incident response process is already in place. DOHMH has hired the firm Foundstone to write a more robust set of Incident Response procedures. It is expected to roll out in 2009. Foundstone should be finishing writing the procedures in early 2009.
Part L	2	Partial. The procedures are being developed by Foundstone and will incorporate some level of DOITT's classification of incidents as well as DOHMH's classification criteria.
Part L	3,4,5,6,7,8,9,10,11	Yes with explanation. Once these procedures are written by Foundstone, these elements should all be defined.
Part L	12,13	Yes with explanation. Once these procedures are written by Foundstone, the Response Team will be defined and its protocols specified.
Part L	14	Yes with explanation. These should be in the written procedures.
Part L	15	Partial. We have attached the current incident response procedures related to confidentiality loss. (See pp.16-20 in particular in the "DOHMH Agency-wide confidentiality policy").
Part N	4c	Partial. CAMIS system (City Agencies Management Information System) at City Department of Consumer Affairs allows the license/ permit documents to be printed when a proper authorization code is entered by an authorized staff person and only if the payment has been processed prior to this. Therefore, the necessary controls are in place to prevent unauthorized approval of license/ permit documents. However, the licenses/ permits issued for DOHMH at DCA are not separately reconciled daily to the applications authorized and printed.
Part O	2b	Partial. DOHMH refers certain civil penalty fines to a contracted vendor for collection. The vendor has authority to docket cases in NY State Supreme Court. DOHMH will take measures to ensure legal action is pursued on a timely basis.

Part Letter	Question #	Explanation
Part Q	3	N/A. The internal audit unit is not required to follow GAGAS. Nevertheless, the audit unit utilizes the Yellow Book as a guide in the performance of its internal audits and reviews.
Part Q	4	Partial. Audits are selected based on risk assessments with the intention of addressing major issues on a multi-year cycle.
Part Q	8 d	Partial. The internal audit unit has a system of supervisory oversight to ensure that audit work follows agreed-upon-procedures. Certain audit procedures incorporate standards from the Yellow Book that help ensure that the audit findings are adequately documented and reasonably reflect the system of controls found during the review/audit. In addition, reports disclose audit findings to senior officials, incorporate management's response, and planned actions to close the issues.
Part Q	11	No. The internal audit function reports to COO/Executive Deputy Commissioner, Andrew Rein.D16

Part Letter	Question #	Explanation

Pages 51 through 59 Not Used

ENCY: Department of Health and Mental Hygiene

NEW YORK CITY COMPTROLLER'S OFFICE
CALENDAR YEAR 2008 CHECKLIST
AGENCY EVALUATION OF INTERNAL CONTROLS
DIRECTIVE # 1

RESULTS OF EVALUATION

		Yes	No	Partial Compliance	Not Applicable
Part A	Effectiveness and Efficiency	27	1	11	1
Part B	Cash Receipts	24	1	1	1
Part C	Imprest Funds	13	1	0	0
Part D	Billings and Receivables	15	0	2	0
Part E	Expenditures and Payables	42	2	1	0
Part F	Inventory	5	2	18	0
Part G	Payroll and Personnel	31	0	0	0
Part H	MIS - Mainframe and Midrange	61	7	12	15
Part I	MIS - PCs and LANs	114	7	35	12
Part J	Internet Connectivity	13	2	7	0
Part K	Risk Assessment, Data Classification & Information Security	1	2	4	0
Part L	Incident Response	12	0	3	0
Part M	Single Audit	18	0	0	0
Part N	Licenses and Permits	13	0	1	2
Part O	Violations Certificates	8	0	1	0
Part P	Leases, Concessions, Franchises	14	0	0	0
Part Q	Internal Audit Function	18	6	1	6
GRAND TOTALS:		**429**	**31**	**97**	**37**