ACTUARIAL SERVICES AND RISK MANAGEMENT SECTOR

INTERNAL SERVICES

Volume 16

OFFICE OF THE SENIOR VICE-PRESIDENT - ACTUARIAL SERVICES AND RISK MANAGEMENT SECTOR
CORPORATE INFORMATION SECURITY DEPARTMENT
PROJECT MANAGEMENT TEAM FOR RISK MANAGEMENT

LIST OF SERVICES

INTERNAL SERVICES **PAGE**

OFFICE OF THE SENIOR VICE-PRESIDENT – ACTUARIAL SERVICES AND RISK MANAGEMENT SECTOR

1. RECEIVING DOCUMENTS REQUIRING ACTION

This is specific to simple inquiries that can be addressed immediately, i.e., inquiry on benefits, accreditation. standards of care policy

Office/Division	Office of the Senior Vice Presodent - Actuarial Services and Risk Management Sector
Classification	Simple
Type of Transaction	G2C; G2B; G2G
Who may avail:	All

CHECKLIST OF REQUIREMENTS	**WHERE TO SECURE**
None	None

CLIENT STEPS	**AGENCY ACTION**	**FEES TO BE PAID**	**PROCESSING TIME**	**PERSON RESPONSIBLE (Position of Supervisor)**
1. Send Memorandum	1.1. Receive memorandum through personal service	None	2 minutes	Administrative staff
	1.2 Log and upload electronic copy in registry	None	3 minutes	Administrative staff
	1.3 Forward memorandum	None	1 minute	Administrative staff
	1.4. Review memorandum as to required action from the Senior Vice President	None	3-15 minutes	Executive Assistant
	1.5. Prepare recommendation on the appropriate course of action of the Senior Vice President, or prepare draft reply, whichever is applicable	None	3-15 minutes	Executive Assistant
	1.6 Evaluate the memorandum to determine the proper course of action which may be any of the following: (1) instruct to prepare reply or initiate conduct of study;	None	15 minutes	Senior Vice President

	(2) forward to PMT-RM/ CISD/ OA; (3) forward to the concerned offices outside the sector to request data or information; (4) return to sender to ask for additional data or information, or seek clarification			
	1.7. Instruct the Executive Assistant on the appropriate course of action	None	5 minutes; however actuarial reports and studies may take longer depending on the nature of the study	Senior Vice President
	1.8 Comply with the instruction of the Senior Vice President	None	15 minutes	Executive Assistant
	1.9 Review and sign the reply, report, endorsement, or memo which apprises the sender of the course of action taken and the expected TAT	None	10 minutes	Senior Vice President
	1.8 Release the reply-memorandum, report, or endorsement to sender; and appropriate offices, if applicable	None	3 minutes	Administrative staff
	TOTAL	**None**	**2 days**	

CORPORATE INFORMATION SECURITY DEPARTMENT

1. INFORMATION SECURITY INCIDENT MANAGEMENT (HIGHLY TECHNICAL)

Concerns the handling of incidents reported

Office/Division	Corporate Information Security Department (InfoSec)
Classification	Highly Technical
Type of Transaction	G2G - Government to Government
Who may avail:	Employees who experienced or discovered an information security incident

CHECKLIST OF REQUIREMENTS	**WHERE TO SECURE**
Incident report (IR) form (including proofs or pieces of evidence) (1 Original and Digital Copy Accepted)	Attached as Annex A to Office Order No. 0086-2015

CLIENT STEPS	**AGENCY ACTION**	**FEES TO BE PAID**	**PROCESSING TIME**	**PERSON RESPONSIBLE**
1.The employee/ initiator properly accomplishes the IR Form a. Attach pertinent documents to support the report b. Submit the report to InfoSec (walk-in, email, direct message)	1.1 Receive the incident report	None	5 minutes	Information Systems Analyst II, InfoSec Information Technology Officer III, InfoSec
	1.2 Update the incidents register	None	5 minutes	
	1.3 Review the incident report and classify	None	1 hour	
	1.4 Set meeting and convene, officers, and employees involved in the incident	None	2 days	
	1.5 Facilitate the resolution of the incident	None	5 days	
	1.6 Document the incidents as well as the agreements	None	1 day	
2. Expect a notification from the InfoSec Operations Division	2.1. Close the incident	None	5 minutes 5 minutes	
	2.2 Monitor the agreements.	None		
	2.3 Perform assessment if warranted.	None		
	Total	**None**	**8 days, 1 hour, 15 mins**	

2. INFORMATION SECURITY INCIDENT MANAGEMENT (SIMPLE)

Concerns the handling of incidents reported

Office/Division	Corporate Information Security Department (InfoSec)			
Classification	Simple			
Type of Transaction	G2G - Government to Government			
Who may avail:	Employees who experienced or discovered an information security incident			
CHECKLIST OF REQUIREMENTS		**WHERE TO SECURE**		
Incident report (IR) form (including proofs or pieces of evidence) (1 Original and Digital Copy Accepted)		Attached as Annex A to Office Order No. 0086-2015		
CLIENT STEPS	**AGENCY ACTION**	**FEES TO BE PAID**	**PROCESSING TIME**	**PERSON RESPONSIBLE**
1. The employee /initiator properly accomplishes the IR Form	1. Receive the incident report	None	5 minutes	Information Systems Analyst II, InfoSec
2. Attach pertinent documents to support the report	2. Update the incidents register	None	5 minutes	
3. Submit the report to InfoSec (walk-in, email, direct message)	3. Review the incident report and classify	None	1 hour	
4. Expect a notification from the InfoSec Operations Division	4. Address the incident	None		
	TOTAL	**None**	**3 hours, 10 mins**	

3. MONITORING OF INFORMATION SECURITY POLICY AND PROTOCOLS

Concerns with overseeing the implementation of security controls and measures, together with other Corporate units tasked to monitor and enforce them.

Office/Division	Corporate Information Security Department (InfoSec)
Classification	Highly Technical
Type of Transaction	G2G - Government to Government
Who may avail:	Business Process Units (BPUs), which require secure corporate information systems (people, process and technology). The BPUs in consultation and coordination with Corporate Information Security Department identify and assess information security risks. The Corporate Information Security Department, both as a BPU and as a responsible office for information security identify and assess information security risks

CHECKLIST OF REQUIREMENTS	WHERE TO SECURE
Anyone of the following: Risk information sheet (RIS) (1 Original Copy);	Reported through Risk Information Management System (RIMS)/For manual copy, RIS Form is an attachment of PhilHealth-SOP-01-02-002
Feedback through email/Report from Information Security Awareness Officer (1 Original copy)	No prescribed form
Assessed Information Security Incident Report (1 Original Copy); or	Received and assessed incident report by Security Operations Division (OpSec) of Corporate Information Security Department
Audit Findings and Recommendations Referred by Internal Audit Group and (Internal Audit Group/COA) (1 Original Copy)	Referred by Internal Audit Group and COA

CLIENT STEPS	AGENCY ACTION	FEES TO BE PAID	PROCESSING TIME	PERSON RESPONSIBLE
1. Implement information security controls and	1. Monitor policy compliance through the following avenues:	None	1/2 day	Information Systems Analyst

measures: a. RIS or RIMS; b. Feedback through email/Report from Information Security Awareness Officer; c. Assessed Information Security Incident Report; or d. Audit Findings and Recommendations (Internal Audit Group/COA)	a. Security Education, Training and Awareness (SETA) activity gathers feedback on policy implementation; b. Incident assessment results and self-assessment; c. Internal Audit Group's audit findings with its recommendations relating to Information Security and Data Privacy; d. Audit Findings and Recommendations (Internal Audit Group/COA)			II, InfoSec Information Systems Analyst III, InfoSec
	2. Reassess information security risks and their corresponding controls and measures (Guidelines, Policy and Standard Operating Procedure)	None	1 day	Information Systems Analyst II, InfoSec Information Systems Analyst III, InfoSec
	3. Revises the corresponding controls and measures (Guidelines, Policy and Standard Operating Procedures)based on the results of the reassessment and in accordance with PhilHealth-SOP-01-01-001 (Policy Formulation Process) and Office Order 0060, series of 2015	None	18days (Initial/Final Review of Concerned Offices/Approval and Signature of Sector Heads	Information Systems Analyst II, InfoSec Information Systems Analyst III, InfoSec

	(Creation, Revision and Use of Standard Operating Procedure)			Information Technology Officer III, InfoSec Senior Manager, InfoSec
		Total	**None**	**20 days**	

4. HANDLING OF COMPLEX INFORMATION SECURITY CONCERNS

Concerns with managing information security concerns across the PhilHealth Organization. It basically covers the formulation of security measures and controls based on the results of the identified and assessed risks on programs and projects.

Office:	Corporate Information Security Department (InfoSec)
Classification:	Complex
Type of Transaction:	Internal Service (G2G)
Who May Avail:	Business Process Units (BPUs), which require secure corporate information systems (people, process and technology). The BPUs in consultation and coordination with Corporate Information Security Department identify and assess information security risks. The Corporate Information Security Department, both as a BPU and as a responsible office for information security identify and assess information security risks

CHECKLIST OF REQUIREMENTS	**WHERE TO SECURE**
None	None

CLIENT STEPS	**AGENCY ACTION**	**FEES TO BE PAID**	**PROCESSING TIME**	**PERSON RESPONSIBLE**
1. Send query/feedback via letter/memo to InfoSec.	1.1. Received letter/memo.		5 minutes	Clerk III, InfoSec Senior Manager, InfoSec Information Technology Officer III, InfoSec Information Systems Analyst III, InfoSec Information Systems Analyst II, InfoSec
	1.2. Assessed received letter/memo.		4 hours	
	1.3. Evaluate and prepare response memo.		4 days	
	1.4. Review draft response memo and provide comments, if any.		1 day	
	1.5. Finalize reply, if with comments.		1 day	
	1.6. Sign finalized response letter.		2 hours	
	1.7. Release response letter to client.	None	5 minutes	
	TOTAL:		**6 days 6 hours and 10 minutes**	

5. HANDLING OF DATA PRIVACY CONCERNS

Handling of concerns involving processing of personal information and compliance with the Data Privacy Act

Office:	Corporate Information Security Department (InfoSec)			
Classification:	Highly Technical			
Type of Transaction:	Internal Service (G2G)			
Who May Avail:	Employees' and external stakeholder's concerns on probable violation of the Data Privacy Act			
CHECKLIST OF REQUIREMENTS		**WHERE TO SECURE**		
Submission/endorsement of documents, electronic mail, and other forms of reporting data privacy concerns		Attached as Annex A to Office Order No. 0086-2015		
CLIENT STEPS	**AGENCY ACTION**	**FEES TO BE PAID**	**PROCESSING TIME**	**PERSON RESPONSIBLE**
1. The employee/external stakeholder properly submits/endorses documents, electronic mail, and other forms of reporting data privacy concerns.	1. Receipt of the report/concern from Clerk III			Clerk III
				Information Systems Analyst II
2. Attach evidences to support the report/concern.	2. Evaluation and assignment of the report/concern to the appropriate Information Systems Analyst		5 minutes	Information Systems Analyst III
			4 hours	Information Technology Officer III
3. Submit the report/concern to InfoSec through established means of communication (walk-in, email, snail mail, business correspondence).	3.1. Conduct of technical assessment, research and/or meetings with relevant Business Process Owners (BPOs) in aid of addressing the report/concern.	None	16 days	

	3.2. Crafting of memoranda and/or other forms of documentation as well as the agreements that addressed the report/concern.		2 days	
	3.3. Technical review of documentation that addressed the report/concern.		2 days	
4. Expect a notification/response from the InfoSec Data Privacy Division.	4. Submission to the Office of the Senior Manager for approval		5 minutes	
	TOTAL:		**20 days, 4 hours, 10 mins**	

6. HANDLING OF HIGHLY TECHNICAL INFORMATION SECURITY CONCERNS

Concerns with managing information security concerns across the PhilHealth Organization. It basically covers the formulation of security measures and controls based on the results of the identified and assessed risks on programs and projects.

Office:	Corporate Information Security Department (InfoSec)
Classification:	Highly Technical
Type of Transaction:	Internal Service (G2G)
Who May Avail:	Business Process Units (BPUs), which require secure corporate information systems (people, process and technology). The BPUs in consultation and coordination with Corporate Information Security Department identify and assess information security risks. The Corporate Information Security Department, both as a BPU and as a responsible office for information security identify and assess information security risks

CHECKLIST OF REQUIREMENTS	**WHERE TO SECURE**
None	None

CLIENT STEPS	**AGENCY ACTION**	**FEES TO BE PAID**	**PROCESSING TIME**	**PERSON RESPONSIBLE**
1. Send query/feedback via letter/memo to InfoSec.	1.1. Received letter/memo.		5 minutes	Clerk III, InfoSec Senior Manager, InfoSec Information Technology Officer III, InfoSec Information Systems Analyst III, InfoSec Information Systems Analyst II, InfoSec
	1.2. Assessed received letter/memo.		1 day	
	1.3. Evaluate and prepare response memo.		15 days	
	1.4. Review draft response memo and provide comments, if any.		2 days	
	1.5. Finalize reply, if with comments.		2 days	
	1.6. Sign finalized response letter.		2 hours	
	1.7. Release response letter to client.	None	5 minutes	
	TOTAL:		**20 days 2 hours and 10 minutes**	

7. HANDLING OF SIMPLE INFORMATION SECURITY CONCERNS				
Concerns with managing information security concerns across the PhilHealth Organization. It basically covers the formulation of security measures and controls based on the results of the identified and assessed risks on programs and projects				
Office/Division	Corporate Information Security Department (InfoSec)			
Classification	Simple			
Type of Transaction	Internal Service (G2G)			
Who may avail:	Business Process Units (BPUs), which require secure corporate information systems (people, process, and technology).			
CHECKLIST OF REQUIREMENTS		**WHERE TO SECURE**		
None		None		
CLIENT STEPS	**AGENCY ACTION**	**FEES TO BE PAID**	**PROCESSING TIME**	**PERSON RESPONSIBLE (Position of Supervisor)**
1. Send query/feedback via letter/memo to InfoSec.	1.1. Received letter/memo.	None	5 minutes	Clerk III, InfoSec Senior Manager, InfoSec Information Technology Officer III, InfoSec Information Systems Analyst III, InfoSec Information Systems Analyst II, InfoSec
	1.2. Assessed received letter/memo.		3 hours	
	1.3. Evaluate and prepare response memo.		1 day	
	1.4. Review draft response memo and provide comments, if any.		1 day	
	1.5. Finalize reply, if with comments.		1 day	
	1.6. Sign finalized response letter.		1 day	
	1.7. Release response letter to client.		5 minutes	
	TOTAL	**None**	3 days 4 hours and 15 minutes	

8. INFORMATION SECURITY INCIDENT MANAGEMENT (COMPLEX)

Concerns the handling of incidents reported

Office/Division	Corporate Information Security Department (InfoSec)			
Classification	Complex			
Type of Transaction	G2G - Government to Government			
Who may avail:	Employees who experienced or discovered an information security incident			
CHECKLIST OF REQUIREMENTS		**WHERE TO SECURE**		
Incident report (IR) form (including proofs or pieces of evidence) (1 Original and Digital Copy Accepted)		Attached as Annex A to Office Order No. 0086-2015		
CLIENT STEPS	**AGENCY ACTION**	**FEES TO BE PAID**	**PROCESSING TIME**	**PERSON RESPONSIBLE**
1.The employee/ initiator properly accomplishes the IR Form a. Attach pertinent documents to support the report b. Submit the report to InfoSec (walk-in, email, direct message)	1.1 Receive the incident report	None	5 minutes	Information Systems Analyst II, InfoSec Information Technology Officer III, InfoSec
	1.2 Update the incidents register	None	5 minutes	
	1.3 Review the incident report and classify	None	1 hour	
	1.4 Set meeting and convene, officers, and employees involved in the incident	None	1 day	
	1.5 Facilitate the resolution of the incident	None	2 days	
	1.6 Document the incidents as well as the agreements	None	4 hours	
2. Expect a notification from the InfoSec Operations Division	2.1. Close the incident	None	5 minutes	
	2.2 Monitor the agreements.	None		
	2.3 Perform assessment if warranted.	None	5 minutes	
	Total	**None**	**3 days, 5 hours, 15 mins**	

9. INFORMATION SECURITY POLICY AND PROTOCOLS DEVELOPMENT

Concerns with managing information security across the PhilHealth Organization through corporate policy development. It basically covers the formulation of security measures and controls based on the results of the identified and assessed risks, and assessed security incidents.

Office/Division	Corporate Information Security Department (InfoSec)
Classification	Highly Technical
Type of Transaction	G2G - Government to Government
Who may avail:	Business Process Units (BPUs), which require secure corporate information systems (people, process and technology). The BPUs in consultation and coordination with Corporate Information Security Department identify and assess information security risks. The Corporate Information Security Department, both as a BPU and as a responsible office for information security identify and assess information security risks

CHECKLIST OF REQUIREMENTS	WHERE TO SECURE
Anyone of the following: Risk information sheet (RIS) (1 Original Copy);	Reported through Risk Information Management System (RIMS)/For manual copy, RIS Form is an attachment of PhilHealth-SOP-01-02-002
Feedback through email/Report from Information Security Awareness Officer (1 Original copy)	No prescribed form
Assessed Information Security Incident Report (1 Original Copy); or	Received and assessed incident report by Security Operations Division (OpSec) of Corporate Information Security Department
Audit Findings and Recommendations Referred by Internal Audit Group and (Internal Audit Group/COA) (1 Original Copy)	Referred by Internal Audit Group and COA

CLIENT STEPS	AGENCY ACTION	FEES TO BE PAID	PROCESSING TIME	PERSON RESPONSIBLE
1. Identify information security risk/ information security	1. Assessed received: a. RIS;	None	1/2 day	Information Systems Analyst

issue/ concern and report through any of the following: a. RIS or RIMS; b. Feedback through email/Report from Information Security Awareness Officer; c. Assessed Information Security Incident Report; or d. Audit Findings and Recommendations (Internal Audit Group/COA)	b. Feedback through email/Report from Information Security Awareness Officer; c. Assessed Information Security Incident Report; or d. Audit Findings and Recommendations (Internal Audit Group/COA)			II, InfoSec Information Systems Analyst III, InfoSec
	2. Develop information security controls and measures (Guidelines, Policy and Standard Operating Procedure) in accordance with PhilHealth-SOP-01-01-001 (Policy Formulation Process) and Office Order 0060, series of 2015 SOP (Creation, Revision and Use of Standard Operating Procedure)	None	17 1/2 days (Initial/Final Review of Concerned Offices/Approval and Signature of Sector Heads)	Information Systems Analyst II, InfoSec Information Systems Analyst III, InfoSec
	3. Communicate information security controls and measures through Outlook and SETA (Guidelines, Policy and Standard Operating Procedure		1 day	Information Systems Analyst II, InfoSec Information Systems Analyst III, InfoSec Information Technology Officer III, InfoSec Senior Manager, InfoSec
	Total	**None**	**20 days**	

10. RETRIEVAL OF BACK-UP TAPES

Concerns the tape vault storage retrieval of back-up tapes

Office:	Corporate Information Security Department (InfoSec)			
Classification:	Simple			
Type of Transaction:	Internal Service (G2G)			
Who May Avail:	Information Technology Management Department			
CHECKLIST OF REQUIREMENTS		**WHERE TO SECURE**		
Consolidated Vault Inventory List (2 Original Copies)		Information Technology Management Department / Information Management Sector		
Vault access request/ endorsement of back-up tape for storage (2 Original Copies)		Information Technology Management Department / Information Management Sector		
Approved withdrawal of tapes request (2 Original Copies)		Information Technology Management Department / Information Management Sector		
CLIENT STEPS	**AGENCY ACTION**	**FEES TO BE PAID**	**PROCESSING TIME**	**PERSON RESPONSIBLE**
1. Prepare letter request / back-up tape retrieval.	1.1. Receive and log all letter request.		5 minutes	Clerk III, InfoSec Senior Manager, InfoSec Information Technology Officer III, InfoSec Information Systems Analyst II, InfoSec Information Systems Analyst III, InfoSec
	1.2. Coordinate with PRID on the availability of service vehicle to Media Library.		3 days	
2. Endorse approved letter request to CISD	2.1 Identify back-up tapes for retrieval.		4 hours	
	2.2. Update Vault Inventory List		2 hours	
	2.3. Retrive back-up tapes.		15 minutes	
	2.4. Ensure that vaults and Media Library are locked.	None	5 minutes	
	TOTAL:		**3 days, 6 hours, 25 mins**	

*subject to approval of blanket CPO regarding Authority to Travel to Media Library (submitted every first month of the year) and availability of service vehicle

11. RETRIEVAL TAPE VAULT STORAGE

Concerns the tape vault storage retrieval of back-up tapes

Office/Division	Corporate Information Security Department (InfoSec)			
Classification	Simple			
Type of Transaction	G2G - Government to Government			
Who may avail:	Information Technology Management Department			
CHECKLIST OF REQUIREMENTS		**WHERE TO SECURE**		
Consolidated Vault Inventory List (2 Original Copies)		Information Technology Management Department / Information Management Sector		
Vault access request/ endorsement of back-up tape for storage (2 Original Copies)		Information Technology Management Department / Information Management Sector		
Approved withdrawal of tapes request (2 Original Copies)		Information Technology Management Department / Information Management Sector		
CLIENT STEPS	**AGENCY ACTION**	**FEES TO BE PAID**	**PROCESSING TIME**	**PERSON RESPONSIBLE**
1. Prepare letter request / back-up tape retrieval.	1. Receive and log all letter request.	None	5 minutes	Clerk III, InfoSec Information Systems Analyst III, InfoSec
2. Endorse approved letter request to CISD	2. Identify back-up tapes for retrieval.	None	5 minutes	
	3. Update Vault Inventory List	None	5 minutes	
	4. Coordinates with codes custodian and physical key custodian.	None	5 minutes	
	5. Retrieve back-up tapes.	None	5 minutes	
	Total	**None**	**25 minutes**	

12. SAFEKEEPING BACK-UP TAPES

Concerns the tape vault storage, safekeeping of back-up tape

Office:	Corporate Information Security Department (InfoSec)
Classification:	Simple
Type of Transaction:	Internal Service (G2G)
Who May Avail:	Information Technology Management Department

CHECKLIST OF REQUIREMENTS	WHERE TO SECURE
Consolidated Vault Inventory List (2 Original Copies)	Information Technology Management Department / Information Management Sector
Vault access request/ endorsement of back-up tape for storage (2 Original Copies)	Information Technology Management Department / Information Management Sector
Approved withdrawal of tapes request (2 Original Copies)	Information Technology Management Department / Information Management Sector

CLIENT STEPS	AGENCY ACTION	FEES TO BE PAID	PROCESSING TIME	PERSON RESPONSIBLE
1. Document/Label Back-up tapes.	1.1. Receive, encodes and prepares Vault Inventory List based on Endorsement Letter from ITMD.		5 minutes	Clerk III, InfoSec Senior Manager, InfoSec Information Technology Officer III, InfoSec Information Systems Analyst II, InfoSec Information Systems Analyst III, InfoSec
	1.2. Coordinate with PRID on the availability of service vehicle to Media Library.		3 days	
2. Prepare consolidated list of inventories/back-up tapes for transport and storage.	2. Validates the endorsed inventories. Checks the completeness and documentation of the endorsed inventories/back-up tapes.		4 hours	
3. Prepare memorandum to Department Manager CISD.	3.1. Receives back-up tapes based on Vault Inventory List.		15 minutes	
	3.2. Signs and completes signatories of Vault Inventory List by ITMD Representative.		15 minutes	
	3.3. Deposit/Store back-up tapes.	None	5 minutes	

	3.4. Ensure that vaults and Media Library are locked.		5 minutes	
	TOTAL:		**3 days, 4 hours, 45 mins**	

*subject to approval of blanket CPO regarding Authority to Travel to Media Library (submitted every first month of the year) and availability of service vehicle

13. SAFEKEEPING TAPE VAULT STORAGE

Concerns the tape vault storage, safekeeping of back-up tape

Office/Division	Corporate Information Security Department (InfoSec)			
Classification	Highly Technical			
Type of Transaction	G2G - Government to Government			
Who may avail:	Information Technology Management Department			
CHECKLIST OF REQUIREMENTS		**WHERE TO SECURE**		
Consolidated Vault Inventory List (2 Original Copies)		Information Technology Management Department / Information Management Sector		
Vault access request/ endorsement of back-up tape for storage (2 Original Copies)		Information Technology Management Department / Information Management Sector		
Approved withdrawal of tapes request (2 Original Copies)		Information Technology Management Department / Information Management Sector		
CLIENT STEPS	**AGENCY ACTION**	**FEES TO BE PAID**	**PROCESSING TIME**	**PERSON RESPONSIBLE**
1. Document/Label Back-up tapes.	1. Receive, encodes and prepares Vault Inventory List based on Endorsement Letter from ITMD.	None	5 minutes	Clerk III, InfoSec Information Systems Analyst III, InfoSec
2. Prepare consolidated list of inventories/back-up tapes for transport and storage.	2. Validates the endorsed inventories. Checks the completeness and documentation of the endorsed inventories/back-up tapes.	None	5 minutes	
3. Prepare memorandum to Department Manager CISD.	3. Receives back-up tapes based on Vault Inventory List.	None	5 minutes	
	4. Signs and completes signatories of Vault Inventory List by ITMD Representative and Guard on duty	None	5 minutes	
	5. Coordinates with codes custodian and physical key custodian.	None	5 minutes	
	6. Deposit/Store back-up tapes	None	5 minutes	
	Total	**None**	**30 minutes**	

PROJECT MANAGEMENT TEAM FOR RISK MANAGEMENT

1. ISSUANCE OF RISK ASSESSMENT CERTIFICATION (RAC) FOR NEW AND AMENDED PROGRAMS, PROJECTS AND POLICIES

As part of Completed Staff Work (CSW) requirements, the Risk Assessment Certification is issued to ensure the risk management process is carried out and applied by the proponent in the course of developing new and amended programs, projects, and policies.

Office/Division	Project Management Team for Risk Management (PMT-RM)
Classification	Complex
Type of Transaction	G2G- Government to Government
Who may avail:	All PhilHealth Head Offices (Proponent)

CHECKLIST OF REQUIREMENTS	WHERE TO SECURE
Draft program, project, or policy (1 photocopy)	Proponent Office
Risk Self-Assessment Questionnaire (1 original)	Proponent Office
Risk Information Sheet (RIS) (1 photocopy)	Proponent Office
Risk Registry (1 photocopy)	Proponent Office

CLIENT STEPS	AGENCY ACTION	FEES TO BE PAID	PROCESSING TIME	PERSON RESPONSIBLE
1. Submit required documents for initial assessment and verification	1.1. Receive required documents and check for completeness	None	2 hours	Clerk/ Administration Services Assistant C (ASA C), PMT-RM
	1.2. Record documents in logbook	None		
	1.3. Endorse documents to technical staff of PMT-RM	None		
	1.4 Check documents contents for completeness	None	4 working days	Project Development Officer III, PMT-RM
	1.5 Review, evaluate and validate submitted documents	None		
	1.6 Sign Risk Self-Assessment Questionnaire (RSAQ)	None		
	1.7 Prepare certification	None		

	1.8 Review documents and sign the Risk Self-Assessment Questionnaire (RSAQ) and Risk Assessment Certification (RAC)	None	1/2 working day (4 hours)	Senior Manager, PMT- RM
2. Receive signed RSAQ and RAC	2.1. Record the RAC Reference No.	None	2 hours	Clerk/ Administration Services Assistant C (ASA C), PMT-RM
	2.2. Release signed RSAQ and RAC	None		
	TOTAL		**4 Days, 1 Hour and 15 Minutes**	