

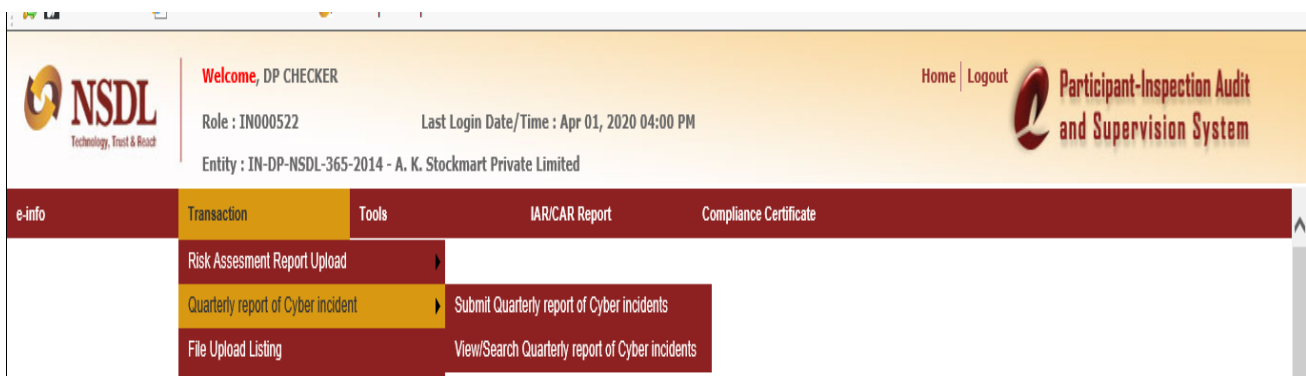
Annexure

Procedure of submission of Quarterly Report of Cyber Incidents through e-PASS

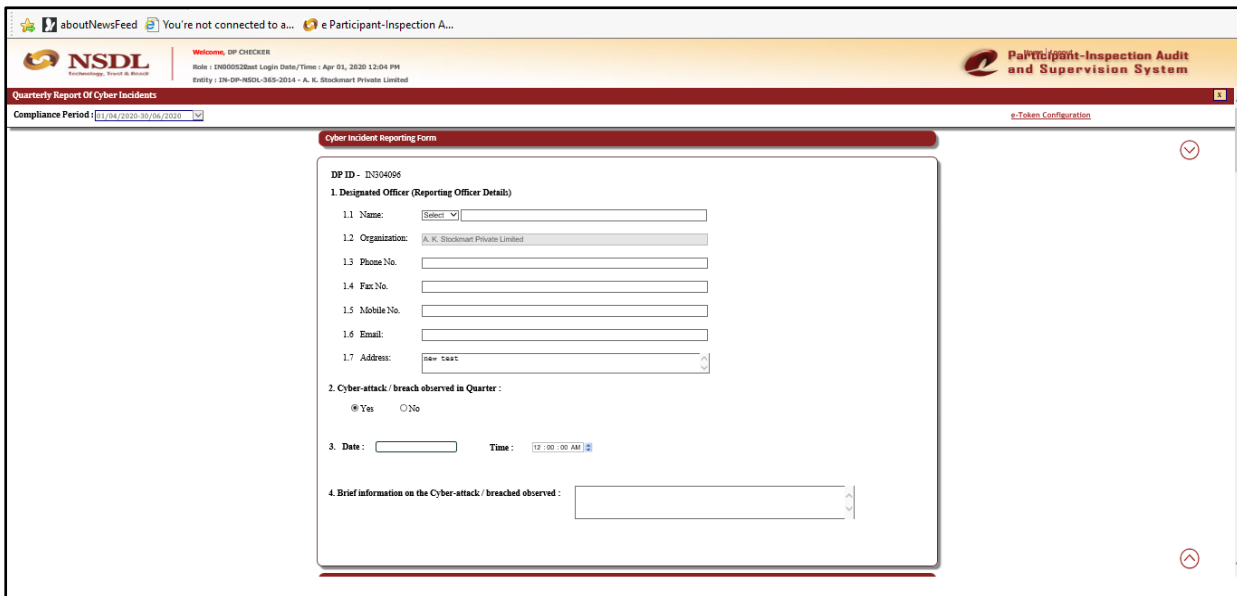
Participants are hereby informed that a new feature has been incorporated on e-Pass portal to facilitate participants to submit the quarterly report of cyber incidents. We have introduced new option viz., 'Quarterly Report of Cyber Incidents' under menu viz., 'Transaction'. On clicking this option, it will display two sub-menus as under:

- Submit Quarterly Report of Cyber Incidents: This section will enable user to capture/submit the Report.
- View/Search Quarterly Report of Cyber Incidents: This section will populate all reports submitted by the Participant.

The quarterly report of Cyber Incidents can be submitted by Checker user. Checker user shall fill the report and submit the report by clicking on sub menu 'Submit Quarterly Report of Cyber Incidents' under the option viz., 'Quarterly Report of Cyber Incidents' as exhibited below.



On clicking on the sub menu viz., Submit Quarterly Report of Cyber Incidents, the system will be redirected into capture screen as exhibited below wherein User will be required to enter designated officer details and at point no. 2 Participant have to select 'Yes' or 'No' whether cyber attacks/breached observed in that quarter.



Quarterly Report Of Cyber Incidents

Compliance Period : 01/04/2020-30/06/2020

Cyber Incident Reporting Form

DP ID - IN304056

1. Designated Officer (Reporting Officer Details)

1.1 Name:

1.2 Organization:

1.3 Phone No.

1.4 Fax No.

1.5 Mobile No.

1.6 Email:

1.7 Address:

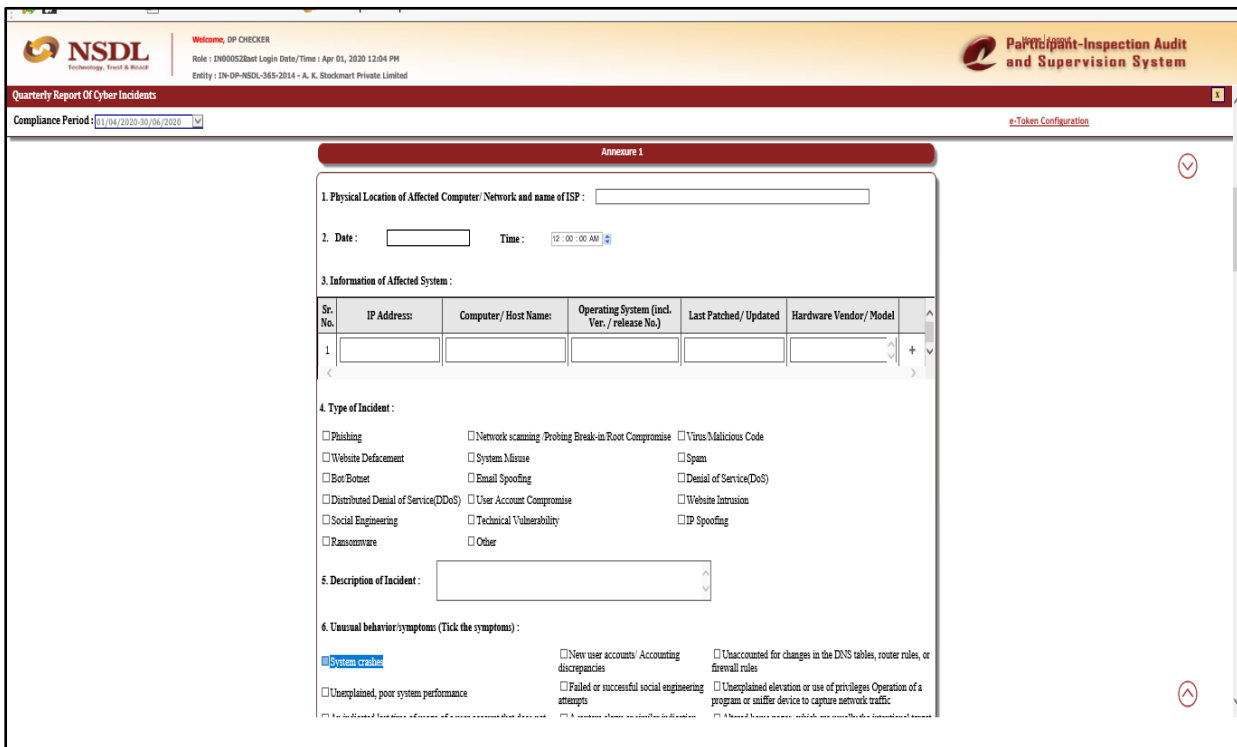
2. Cyber-attack / breach observed in Quarter :

Yes No

3. Date : Time : 12 : 00 : 00 AM

4. Brief information on the Cyber-attack / breached observed :

If User select 'Yes' in above Point 2, he will be required to enter Cyber Incident details as exhibited below:



Quarterly Report Of Cyber Incidents

Compliance Period : 01/04/2020-30/06/2020

Annexure 1

1. Physical Location of Affected Computer/ Network and name of ISP :

2. Date : Time : 12 : 00 : 00 AM

3. Information of Affected System :

Sr. No.	IP Address	Computer/ Host Name	Operating System (incl. Ver. / release No.)	Last Patched/ Updated	Hardware Vendor/ Model
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

4. Type of Incident :

Phishing Network scanning/ Probing Break-in/Root Compromise Virus/Malicious Code

Website Defacement System Misuse Spam

Bot/Botnet Email Spoofing Denial of Service(DoS)

Distributed Denial of Service(DDoS) User Account Compromise Website Intrusion

Social Engineering Technical Vulnerability IP Spoofing

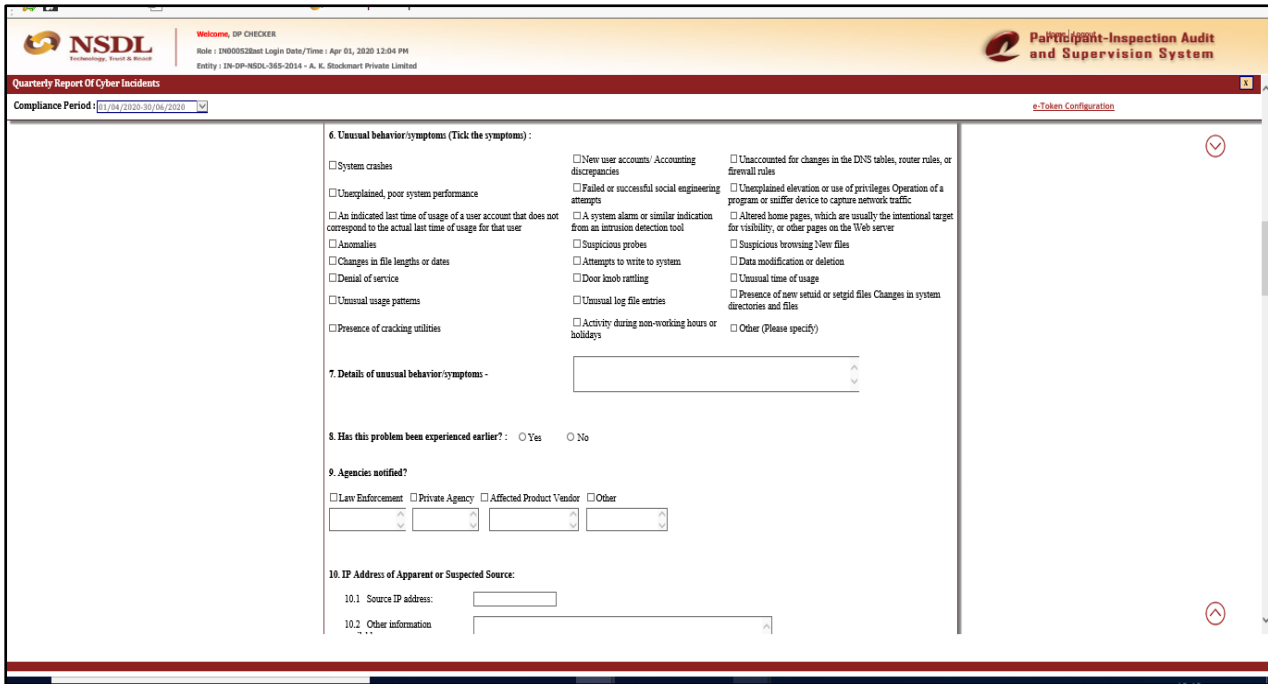
Ransomware Other

5. Description of Incident :

6. Unusual behavior/symptoms (Tick the symptoms) :

System crash New user accounts/ Accounting discrepancies Unaccounted for changes in the DNS tables, router rules, or firewall rules

Unexplained, poor system performance Failed or successful social engineering attempts Unexplained elevation or use of privileges Operation of a program or sniffer device to capture network traffic



NSDL Technology, Trust & Reach

Welcome, DP CHECKER

Role : IN0055282st Login Date/Time : Apr 01, 2020 12:04 PM
Entity : IN-DP-NSDL-365-2014 - A. K. Stockmart Private Limited

Participant-Inspection Audit and Supervision System

Quarterly Report Of Cyber Incidents

Compliance Period:

6. Unusual behavior/symptoms (Tick the symptoms) :

<input type="checkbox"/> System crashes	<input type="checkbox"/> New user accounts/ Accounting discrepancies	<input type="checkbox"/> Unaccounted for changes in the DNS tables, router rules, or firewall rules
<input type="checkbox"/> Unexplained, poor system performance	<input type="checkbox"/> Failed or successful social engineering attempts	<input type="checkbox"/> Unexplained elevation or use of privileges Operation of a program or sniffer device to capture network traffic
<input type="checkbox"/> An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user	<input type="checkbox"/> A system alarm or similar indication from an intrusion detection tool	<input type="checkbox"/> Altered home pages, which are usually the intentional target for visibility, or other pages on the Web server
<input type="checkbox"/> Anomalies	<input type="checkbox"/> Suspicious probes	<input type="checkbox"/> Suspicious browsing/ New files
<input type="checkbox"/> Changes in file lengths or dates	<input type="checkbox"/> Attempts to write to system	<input type="checkbox"/> Data modification or deletion
<input type="checkbox"/> Denial of service	<input type="checkbox"/> Door knob rattling	<input type="checkbox"/> Unusual time of usage
<input type="checkbox"/> Unusual usage patterns	<input type="checkbox"/> Unusual log file entries	<input type="checkbox"/> Presence of new sendid or setgid files Changes in system directories and files
<input type="checkbox"/> Presence of cracking utilities	<input type="checkbox"/> Activity during non-working hours or holidays	<input type="checkbox"/> Other (Please specify)

7. Details of unusual behavior/symptoms -

8. Has this problem been experienced earlier? : Yes No

9. Agencies notified?

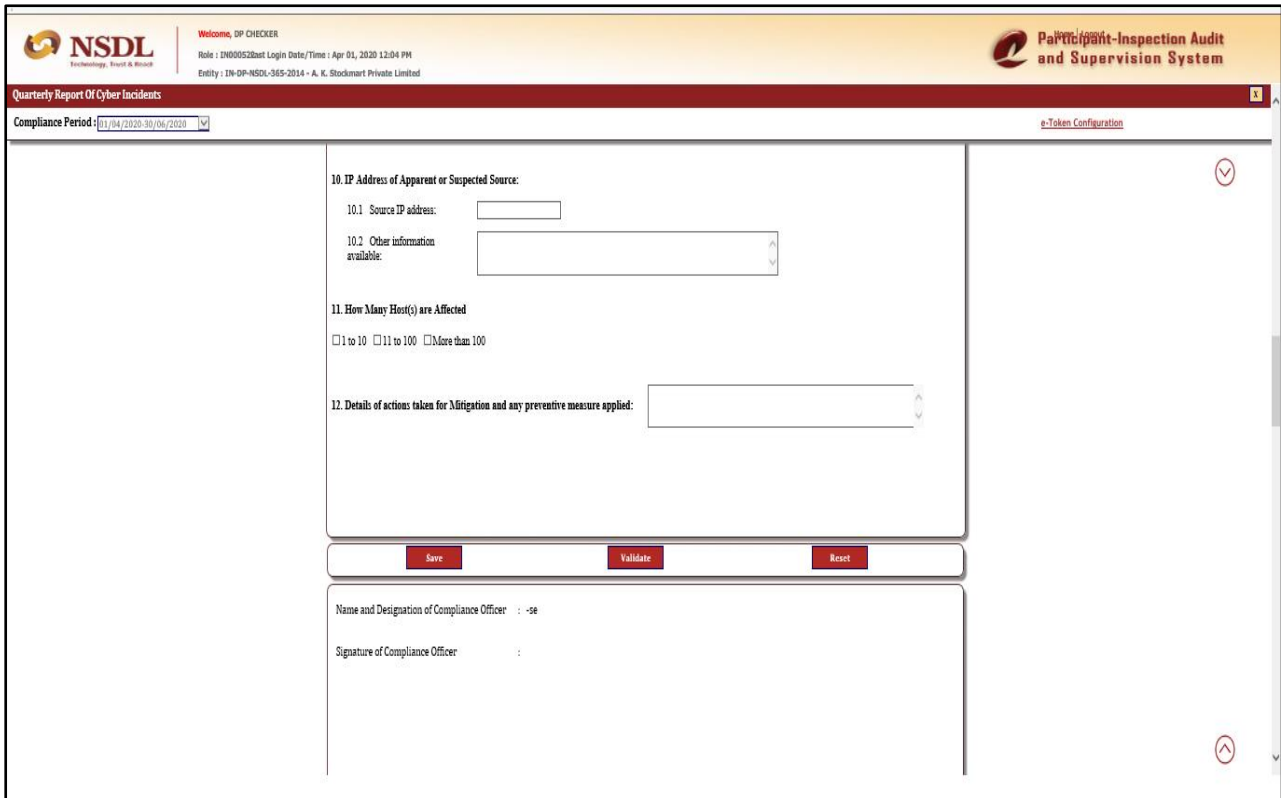
Law Enforcement Private Agency Affected Product Vendor Other

10. IP Address of Apparent or Suspected Source:

10.1 Source IP address:

10.2 Other information:

User can click “Save” button to save the draft at any point in time while filling the report. The user can view the saved quarterly report under ‘view/search reports’ option. Further, user can click “Reset” button to reset the filled quarterly report [as exhibited below].



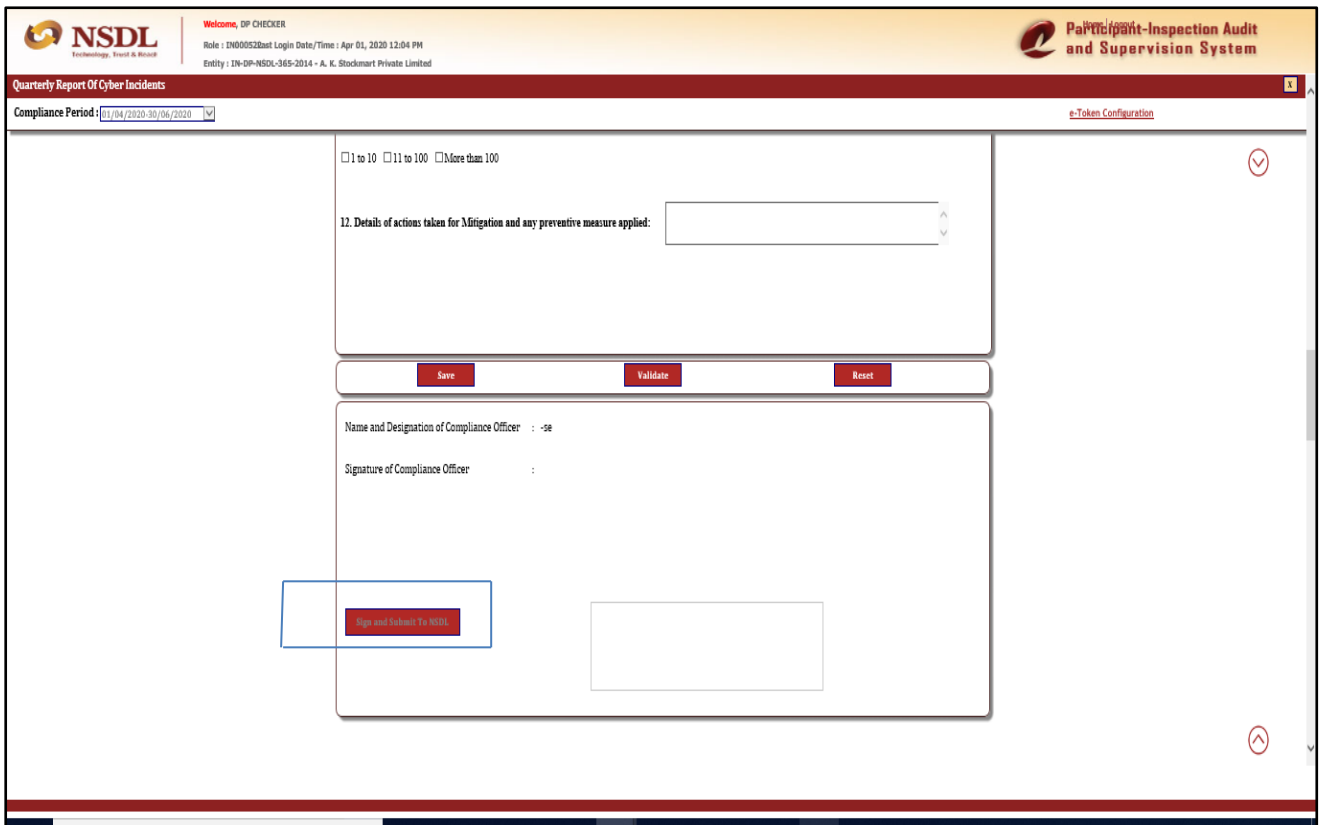
The screenshot shows the 'Quarterly Report of Cyber Incidents' form in the NSDL Participant-Inspection Audit and Supervision System. The form is titled 'Quarterly Report of Cyber Incidents' and includes a 'Compliance Period' dropdown set to '01/04/2020-30/06/2020'. The form is divided into several sections:

- 10. IP Address of Apparent or Suspected Source:**
 - 10.1 Source IP address: [Text input field]
 - 10.2 Other information available: [Text input field]
- 11. How Many Host(s) are Affected**
 - 1 to 10 11 to 100 More than 100
- 12. Details of actions taken for Mitigation and any preventive measure applied:** [Text input field]

At the bottom of the form, there are three buttons: 'Save', 'Validate', and 'Reset'. Below the form, there are two fields for the Compliance Officer: 'Name and Designation of Compliance Officer' and 'Signature of Compliance Officer'. The form also features a 'e-Taken Configuration' link in the top right corner and a 'Close' button in the top right corner of the form area.

Once the report is filled completely, the user will need to click on 'validate' button. If there are any error/s the same would be highlighted which are required to be corrected by the user and once again click on button 'validate'.

Once Quarterly Report of Cyber Incidents is validated successfully then the user is required to digitally sign the same and submit the Quarterly Report of Cyber Incidents to NSDL by clicking on "Sign and submit to NSDL" button.



NSDL | Welcome, DP CHECKER
Role : IN000522 Last Login Date/Time : Apr 01, 2020 12:04 PM
Entity : IN-DP-NSDL-365-2014 - A. K. Stockmart Private Limited

Participant-Inspection Audit and Supervision System

Quarterly Report Of Cyber Incidents

Compliance Period: 01/04/2020-30/06/2020

1 to 10 11 to 100 More than 100

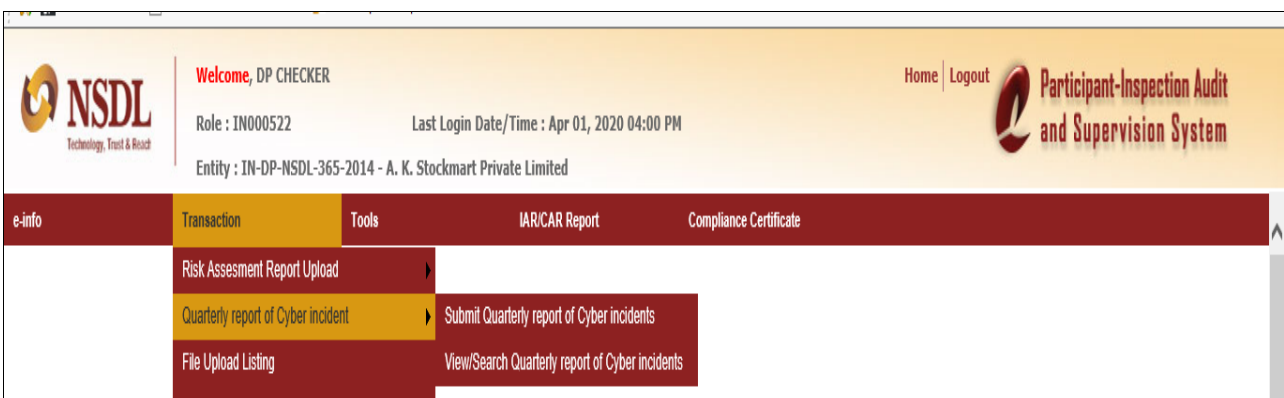
12. Details of actions taken for Mitigation and any preventive measure applied:

Save Validate Reset

Name and Designation of Compliance Officer : -se
Signature of Compliance Officer :

Sign and Submit To NSDL

Once the report get submitted, user will be able to view the report on link 'View/Search Quarterly Report of Cyber Incidents' provided under option viz., 'Quarterly Report of Cyber Incidents' as exhibited below.



NSDL | Welcome, DP CHECKER
Role : IN000522 Last Login Date/Time : Apr 01, 2020 04:00 PM
Entity : IN-DP-NSDL-365-2014 - A. K. Stockmart Private Limited

Home | Logout **Participant-Inspection Audit and Supervision System**

e-info	Transaction	Tools	IAR/CAR Report	Compliance Certificate
	Risk Assesment Report Upload			
	Quarterly report of Cyber incident		Submit Quarterly report of Cyber incidents	
	File Upload Listing		View/Search Quarterly report of Cyber incidents	