Committee(s)	**Dated:**
Digital Services Sub-Committee – For Information	**3rd July 2020**
Subject: IT Division – IT Service Delivery Summary	**Public**
Report of: The Chamberlain	**For Information**
Report author: Matt Gosden – Deputy IT Director Eugene O'Driscoll, Agilisys Client Director	

Summary

There was a total of 5 P1 and 2 P2 incidents for the City of London Corporation and City of London Police in May. These incidents were caused by external factors such as supplier works outside of the direct control of Agilisys.

Problem records have been created where appropriate to identify root causes and to manage improvements.

- There was **1** P1 incident for City of London Corporation and **4** for City of London Police.
- There were **0** P2 incidents for the City of London Corporation and **2** for City of London Police.
- **92%** of users reported a good or very good experience of the City of London Service Desk and **93%** of users reported the same for the City of London Police Service Desk.

Recommendations

Members are asked to note this report

Main Report

Service levels and exceptions

1. **City of London Police (CoLP) P1 incidents**

There were 4 P1 incidents

Affected Service	Duration	Reason	Resolution	Problem Management plan
Network	01:02	A failed change to exclude Snow Hill from the CoLP network caused a network loop	The change was reverted	Reviewed and second attempt was successfully implemented
PNC	17:45	A change to deploy a registry key to fix a Triple DES Vulnerability, which appeared to have caused the certificate auto enrolment issue on both servers upon restarting.	The keys were removed from the servers	Review and reschedule
Network (Security Zone)	OOH 07:18	CP6SEAP2 (VPN) Forcepoint firewall in Bishopsgate stopped responding and two DCs went offline	CP6SEAP2 firewall was restarted. This took several attempts.	Problem record
Pronto-Niche	OOH 00:45	Network change of New Street firewall caused routes not to be advertised as expected and network traffic was blocked.	Rollback of firewall change	Review and reschedule

2. **City of London Police P2 Incidents**

There were 2 P2 incidents

Affected Service	Duration	Reason	Resolution	Problem Management plan
HR Application Portal	OOH 60:08	Update error by 3rd party Capita	Resolved by 3rd party Capita	Supplier management
IL4 CoLPConf VPN client	16:00	Non-responsive firewall	The firewall was restarted	Problem record

3. City of London (CoL) P1 incidents

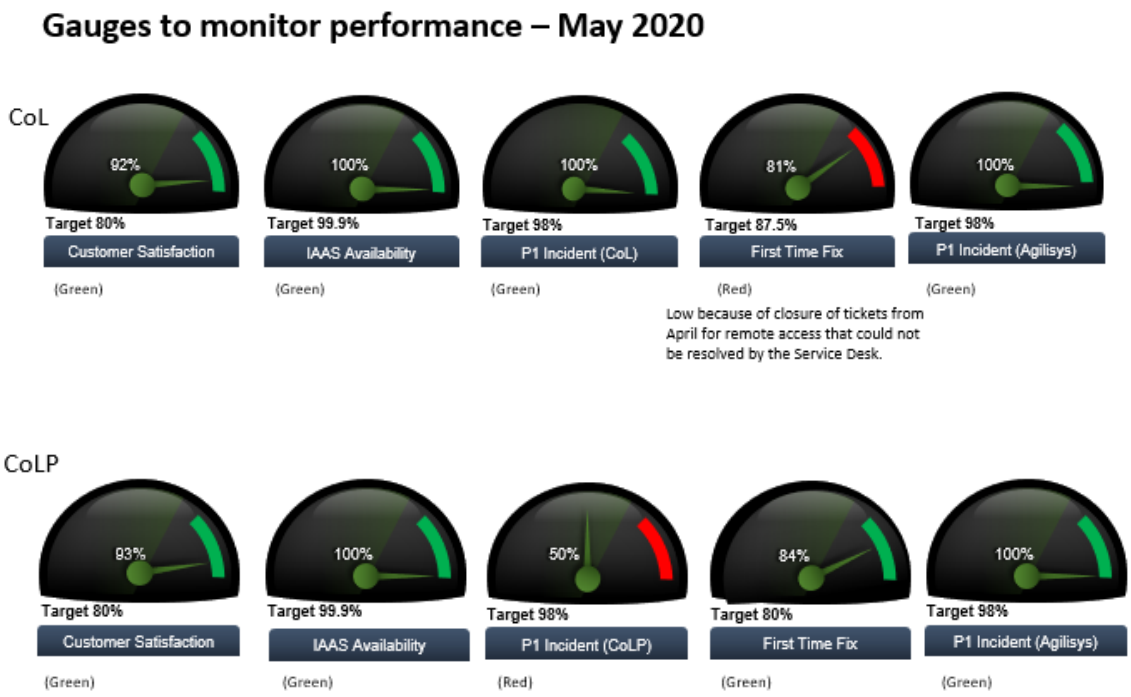
Affected Service	Duration	Reason	Resolution	Problem Management plan
Epilog Gower	00:12	The application became unavailable. No root cause discovered in incident.	Application services were restarted.	Problem record

There was 1 P1 incident, for Epilog Gower, which was resolved within 12 minutes.

4. City of London P2 Incidents

There were no P2 incidents in May

Service performance summary is detailed in the dashboard below:



Service improvements and highlights

5. City of London Police Improvements include:

- Discussions are under way to improve the PSN annual check process.
- Improved stability of the remote access solution, making it more resilient and providing an increase in capacity to accommodate the potential user numbers.

6. Corporation improvements include:

City of London has requested an extension of Sharepoint, Office365 and SQL database support from Agilisys for 3 months from September. This will support the City whilst it builds its own capabilities in these areas.

7. PSN summary

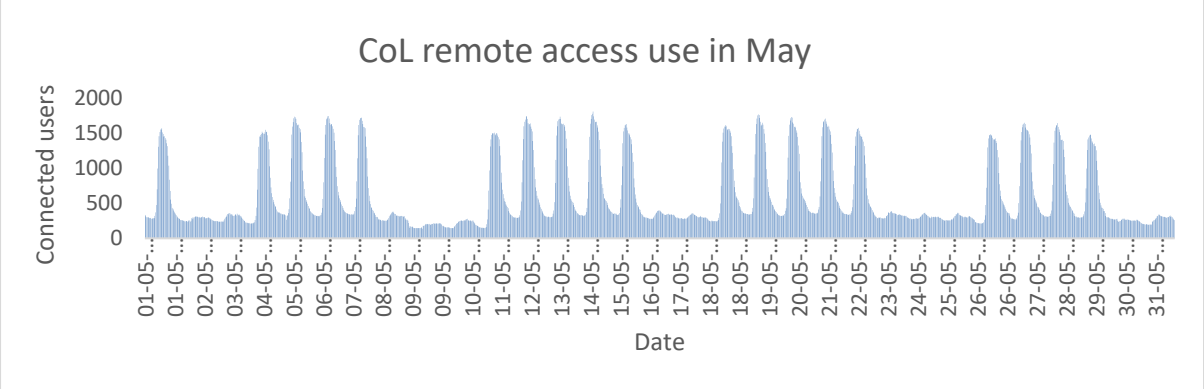
Ambitious targets to review and address every recommendation from the PSN annual check were achieved and 99% of the City of London vulnerabilities have been remediated or mitigated.

For City of London Police, there are no critical vulnerabilities, and the remaining 3 ‘high’ findings will be completed under the IT Modernisation Programme.

8. Remote access for users during Covid-19

City of London

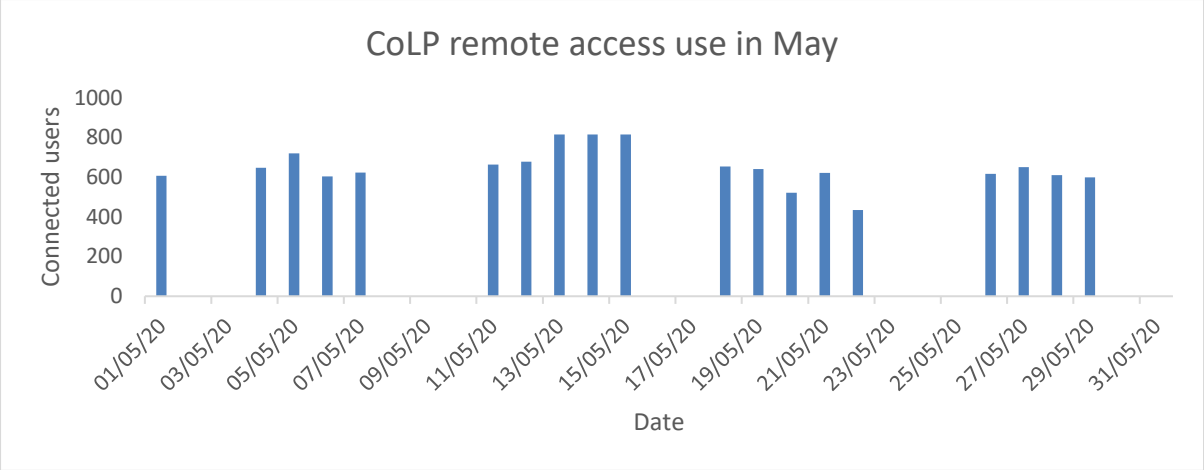
The City of London remote access service experienced a hardware failure which impacted on service stability in April. Since the faulty hardware was replaced and an additional server added to provide extra resilience, the service has been extremely stable and providing service to between 1500 and 1700 users per day.



Includes two Bank Holidays (8th and 25th May).

City of London Police

The average number of City of London Police remote access users in May was 650, with a high of 816 and a low of 435. Through March and April significant progress was made to stabilise VPN, make it more resilient and increase capacity to accommodate the potential user numbers.



9. Partnership improvements include:

In response to Covid-19, the City of London, London Councils and City of London Police greatly increased the proportion of the workforce which is working from home. Agilisys worked with the IT department in anticipation of a sudden change in workforce profile by provisioning additional laptops, prioritising remote working and working closely with the suppliers of the remote access service to improve performance. The majority of IT staff are also working from home, although Agilisys continues to provide a partial onsite capability to support City of London Police operational requirements.

Implementation of the new IT Service Management tool is under way and expected to complete by September. The new tool, called ServiceNow, will provide enhanced self-service capabilities for users and an improved Configuration Management database (CMDB) which will support CoL and CoLP's change management and asset management functions.

10. Public Services Network Submission

Our annual Public Services Network Submission has been made to the Cabinet Office with no Critical or High issues left to remediate from our last IT Heathcheck which was carried out by an independent IT security consultancy. (See Appendix 2 for further details).

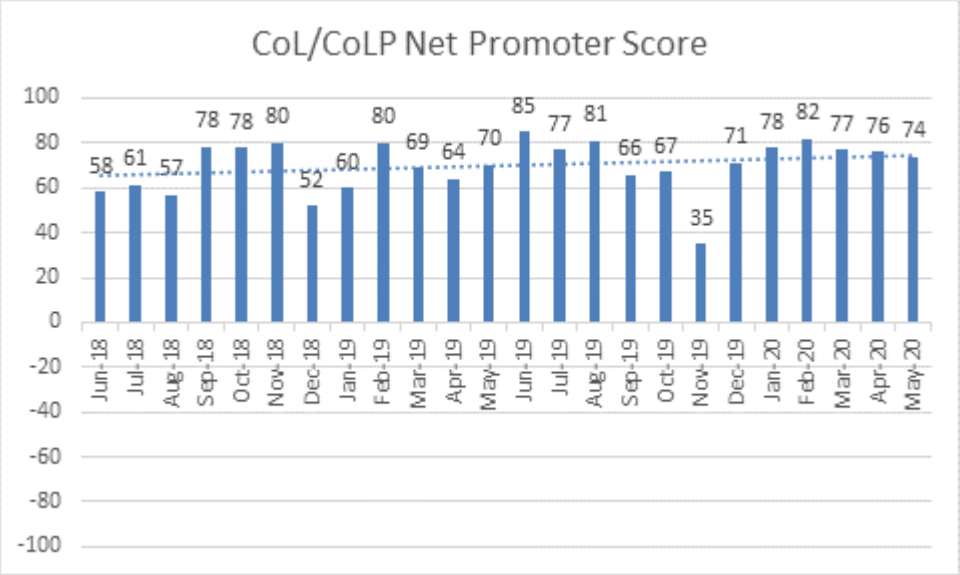
Matt Gosden and Eugene O'Driscoll
Deputy IT Director, Agilisys Client Director
E: Matt.Gosden@cityoflondon.gov.uk
Euegene.ODriscoll@cityoflondon.gov.uk

Appendices

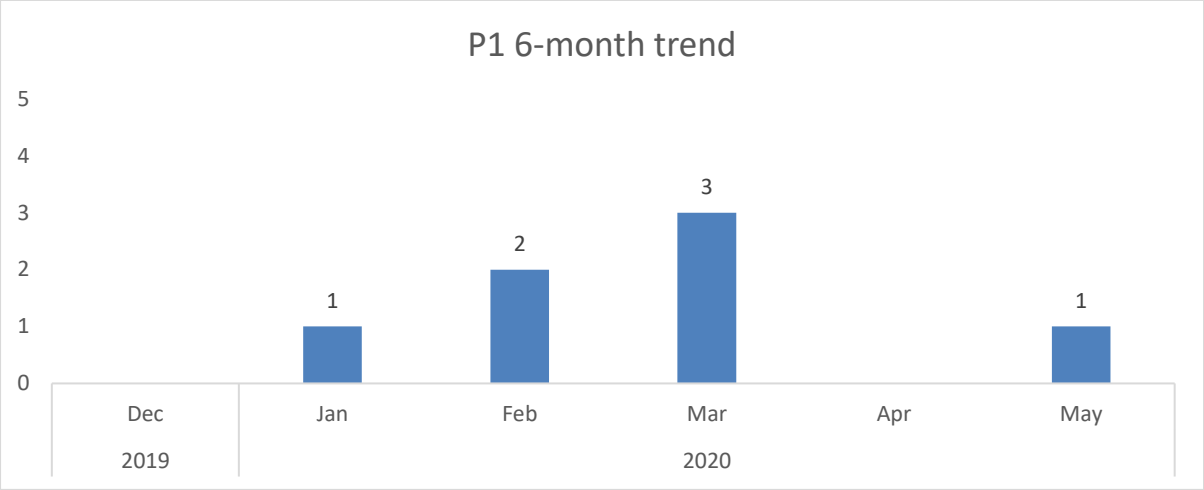
- Appendix 1 – Trend Graphs
- Appendix 2 – IT Health Check Actions

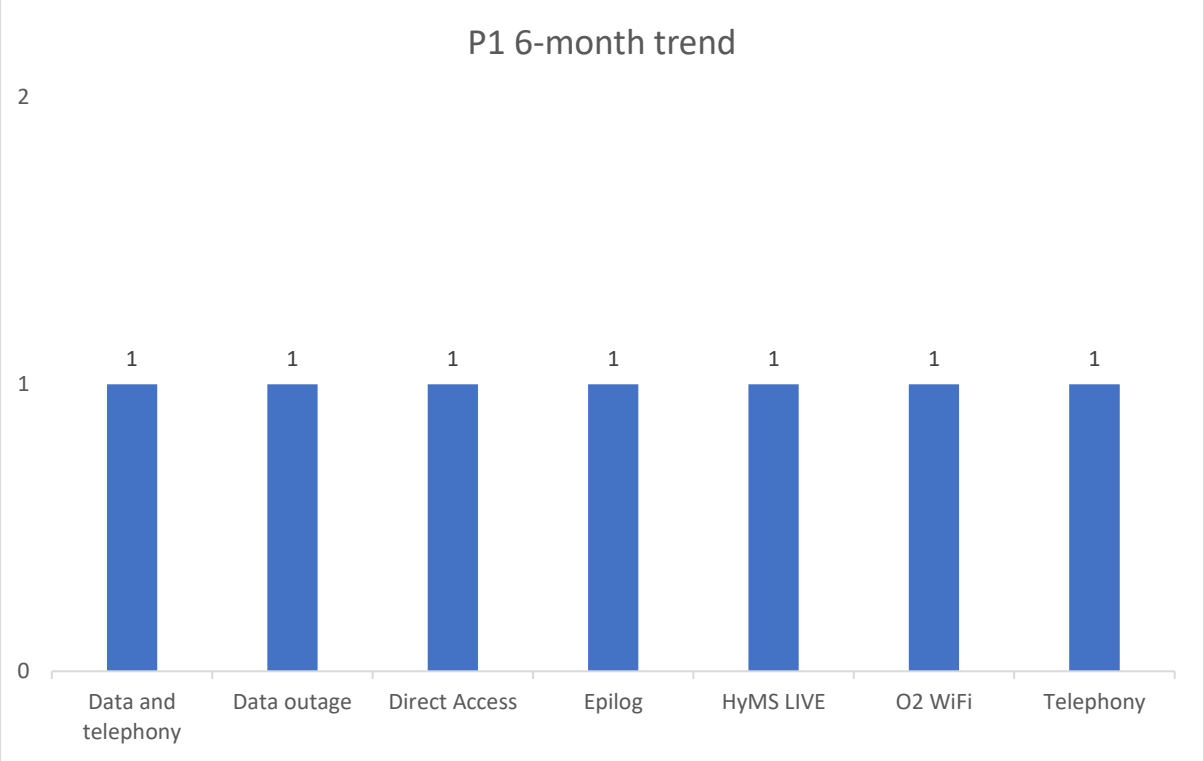
Appendix 1 – Trend Graphs

CoL and CoLP Net Promoter Score (scores above 50 are 'very good').

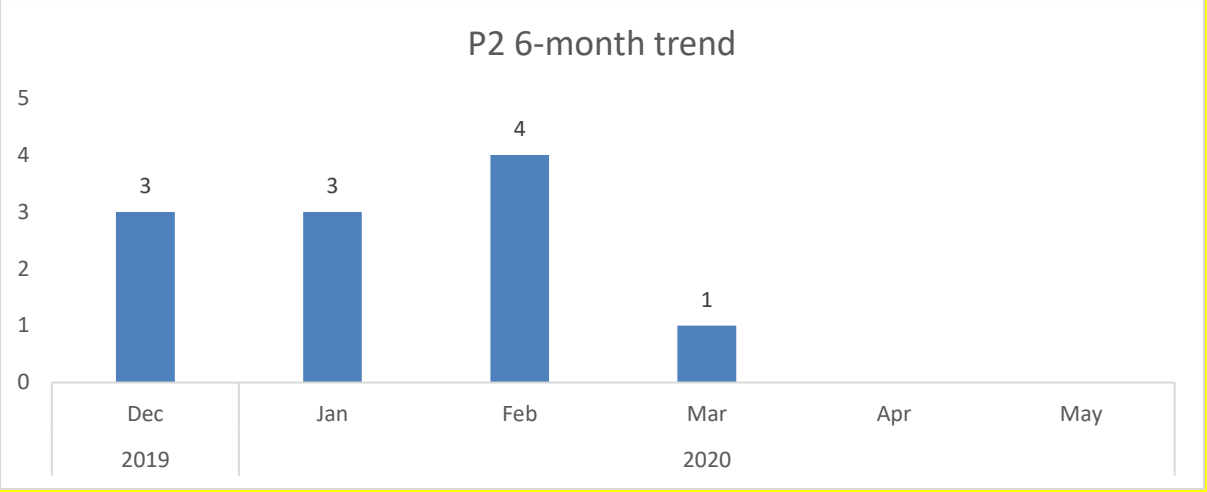


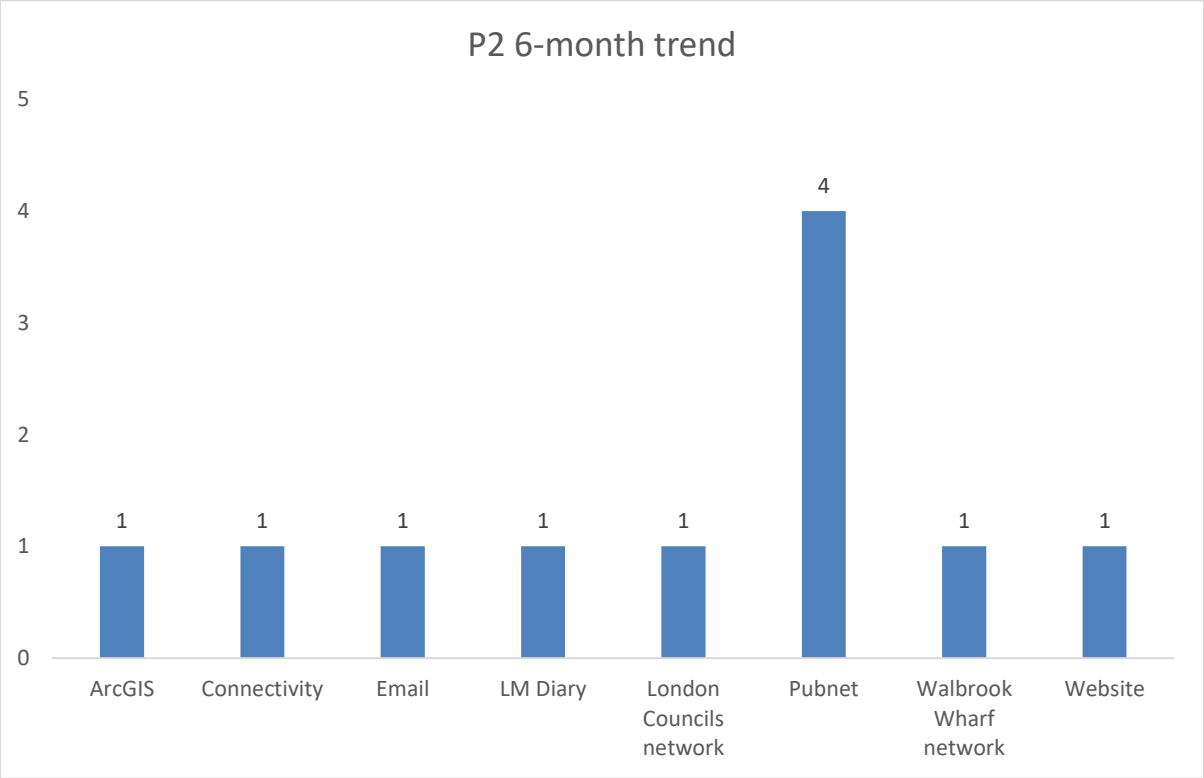
CoL Priority Incident trending – 6-month view





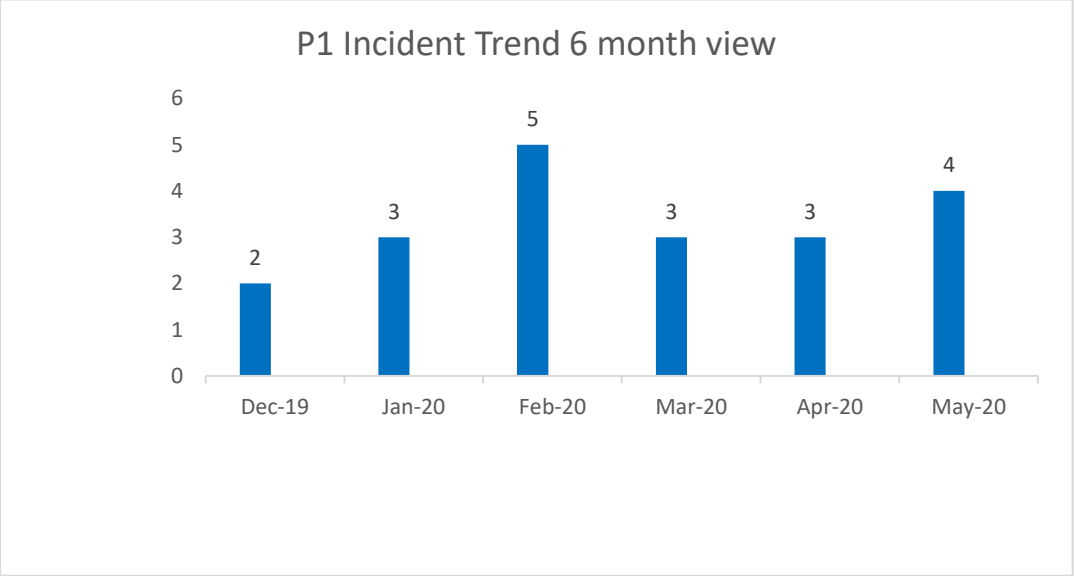
1 x P1 incident for Agilisys in the last 6 months (resolved within 16 minutes).

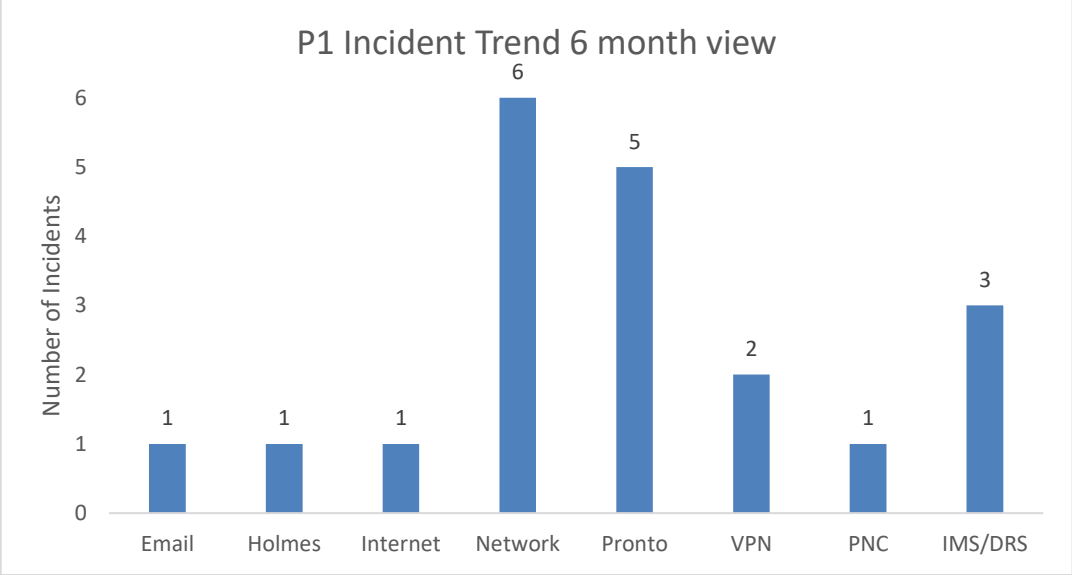


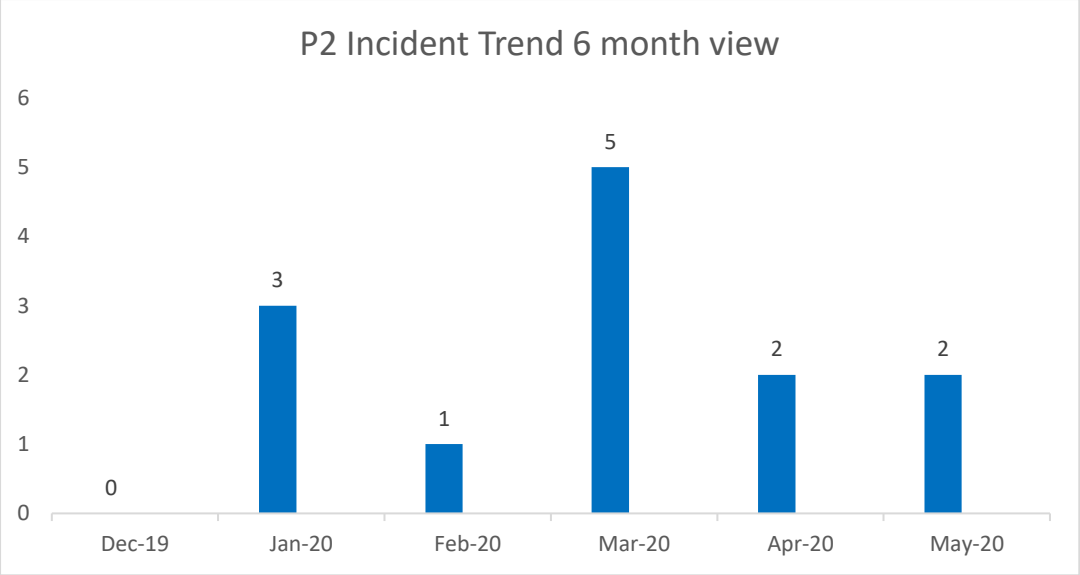


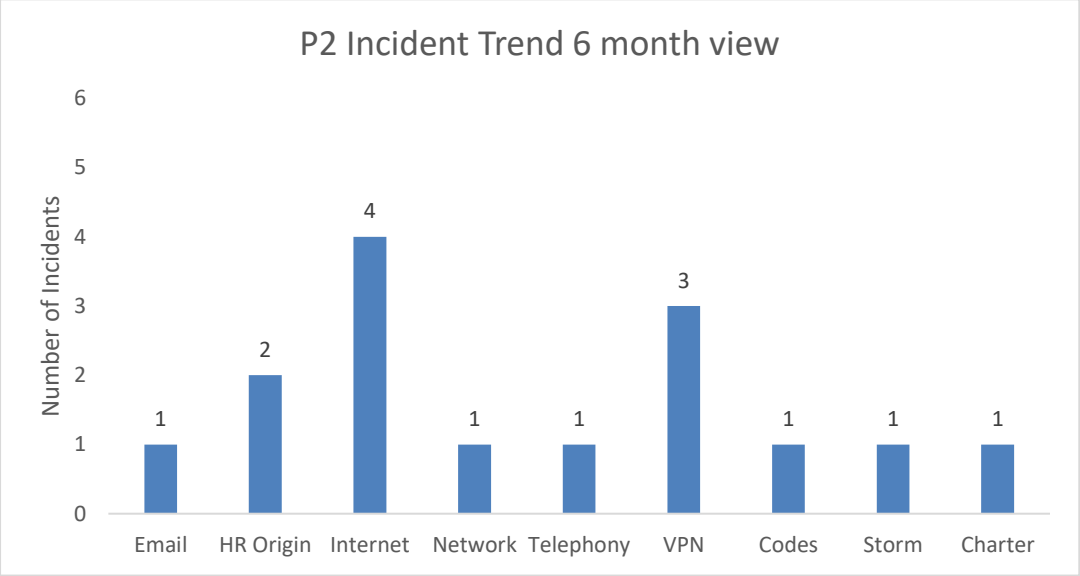
No P2 incidents for Agilisys in the last 6 months.

CoLP Priority Incident trending – 6-month view






P2 Incident Trend 6 month view
6
5
4
3
2
1
0
0
3
1
5
2
2
Dec-19
Jan-20
Feb-20
Mar-20
Apr-20
May-20


P2 Incident Trend 6 month view
Number of Incidents
6
5
4
3
2
1
0
1
2
4
1
1
3
1
1
1
Email
HR Origin
Internet
Network
Telephony
VPN
Codes
Storm
Charter

Appendix 2 – Summary IT Healthcheck Remediation

For the 2019/20 submission, of the 3 CRITICAL and 23 HIGH vulnerabilities identified in the IT health check report, there remain 2 HIGH category vulnerabilities that need remediating and are in progress to being fully resolved. Additional details are below and in the attached Remediation Action Plan (RAP.)

These will be remediated by the following actions, being delivered by in-flight projects and have resources assigned, plans developed and are in progress.

Details below:

CRITICAL: (3)
All 3 CRITICAL vulnerabilities have been remediated.

HIGH: (23)
21 HIGH vulnerabilities have been remediated.
2 HIGH vulnerabilities have not been remediated and the Corporation is asked to accept the risk of these vulnerabilities as these will be resolved when Citrix is decommissioned at the end of June 2020, following the Revenues and Benefits departments project to migrate to Capita Services in the Cloud in mid-June 2020 - as detailed in the attached Remediation Action Plan.

MEDIUM: (162)
109 MEDIUM vulnerabilities have been remediated and 53 mitigated – details in the attached Remediation Action Plan.

LOW & INFO: (74)
37 LOW vulnerabilities remediated and 20 mitigated.
8 INFO vulnerabilities remediated and 9 mitigated.