THE CHIEF CONSTABLE OF NORTH YORKSHIRE

Service Operations

FINAL

Internal audit report: 11.19/20

9 March 2020

RSM

CONTENTS

Debrief held	12 December 2019	**Internal audit team**	Daniel Harris, Head of Internal Audit
Draft report issued	20 January 2020		Angela Ward, Senior Manager
Responses received	9 March 2020		Philip Church, Client Manager
			David Morris, Technology Assurance Director
			John Bradshaw, Managing Consultant
Final report issued	9 March 2020	**Client sponsor**	Managing Director
		Distribution	Interim Head of ICT
			Managing Director

1 EXECUTIVE SUMMARY

1.1 Background

A review was performed to enable the Force to take assurance over IT service operations with focus on the service desk covering governance, incident and problem management, continual service improvement and third-party management.

The IT department consists of approximately 60 staff supporting 2,200 users. The IT infrastructure is in the process of transitioning from an on-premise server and storage to an Office 365 Windows 10 environment. A VMware horizon five-year licence has been extended for a further year to allow time for the transition to complete. A Citrix environment is expected to continue to support two unique policing applications. A further upgrade is expected in moving the existing telephony system to a Microsoft Skype solution as part of Office 365.

A change in the IT service desk staffing profile is also planned in the near future to change the structure from 10 staff (six permanent and four agency) that is split by first-line support (provides the basic common assistance and call logging) and second-line support (provides support for more complex tasks) into a consolidated 'user support engineer' group of six staff reporting to one line manager. It is hoped that this will provide a more effective and resilient IT service support capability.

1.2 Conclusion

Our main concern is that the service delivery team, including service desk staff, have been operating reactively to the influx of IT service desk calls. The supporting procedures covering service delivery have not been formally reviewed since their last publication date of 2013. There is no documented problem management process in place to manage the lifecycle of all problems to prevent incidents from recurring and to minimise the impact of incidents that cannot be prevented.

Testing of active accounts identified a significant number had not been accessed for over two months. This is of particular concern for individuals who have moved roles within the Force but potentially have access to information that is no longer suitable for their new roles and responsibilities.

Service desk measurement and monitoring has not yet matured. The team had been unable to derive meaningful service desk data from the ticketing tool to drive analysis of incidents to identify trends in incidents to identify potential problems and opportunities for continual improvement. Similarly, management reporting does not appear to be fully established with gaps noted in their production and distribution.

We also noted the following weaknesses:

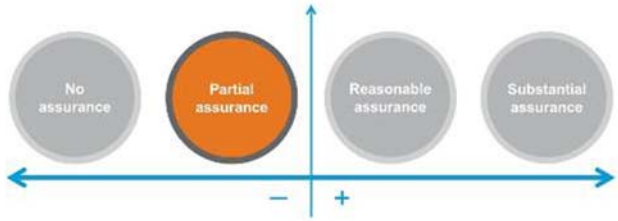
- There are monthly snapshots of tickets logged and resolved by month, but there is no available report to show ticket resolution performance across the year to determine if there is any observable impact due to staff capacity shortfalls.
- There is no service desk staff utilisation data available for review; and
- It was stated by the Service Desk Supervisor that staff do not always complete timesheets in a consistent manner to show hours worked. We were not able to corroborate this as the Service Desk Supervisor did not have access to such data reporting.

There appears to be no agreed method for knowledge capture and sharing. We noted that little use had been made of the ticketing system tool's knowledge management. The Manager of Digital Delivery stated that many 'low-level' repeatable issues had been raised on his team for remediation when the expectation is that they should have been addressed by the Service Desk Engineers as part of support.

We have agreed **two high** and **seven medium** priority management actions as a result of our findings. Further details of our findings and actions can be found in section two of this report.

Internal audit opinion:

Taking account of the issues identified, the Chief Constable can take **partial assurance** that the controls to manage this risk are suitably designed and consistently applied.
Action is needed to strengthen the control framework to manage the identified risk.



1.3 Key findings

We have summarised our **high** and **medium** management actions below:

Account Access

- We recorded 861 internal IT accounts that had no identified activity in more than two months. We sampled four randomly selected staff leavers in the past year to confirm that their corresponding Active Directory access had been disabled. We found that all four accounts continued as 'active' with the same passwords in use during the leaver's employment. There is a risk that a proportion of these accounts may carry sensitive data that continues to be available to individuals who have left their current role and moved to another role or another force for which they are no longer authorised. **(High)**

Service Governance

- One of the processes reviewed was the major incident service delivery document that showed communication flows to roles. It was not clear from the workflow how an incident was diagnosed, repaired and recovered. The diagram did not indicate the key staff assigned to the roles. There is a risk that staff may not be aware of the order to their responsibilities in a major incident that introduce delays in restoring the service. **(High)**

- Service desk procedures covering service delivery team's activities have not been reviewed or updated since 2013 and do not reflect the current service life-cycle for user requests, resolving failures, problem management and routine tasks. There is a risk that without a repeatable foundation for control that key activities for service delivery will be missed and cause impact on service delivery times and service quality. **(Medium)**

Service Operation

- Staffing capacity / utilisation for first-line service desk staff was not available for review and is not used to determine productivity to identify the resources required to meet demand. There is a risk that actual resource sufficiency cannot be demonstrated to identify any potential shortfalls in staffing to meet work demands or to recognise the impact and be able to plan for staff absence. **(Medium)**

- There is currently no formal profile of staff skills to identify what is required to deliver the service, the actual skill capability of the team for the roles assigned and the shortfalls of skill that will require further on-the-job experience, support or training. There is a risk that staff capability may fall short of requirement and training needs may not be routinely assessed and addressed ahead of role assignment resulting in an impact to the quality of service operations. **(Medium)**

- There is little evidence of knowledge management to capture acquired technical and business knowledge relevant to service delivery. The use of the ticketing system knowledge management had not been used since the last dated entry of October 2018 and no other tool was being used to capture knowledge to help with problem diagnosis and incident fixes. There is a risk that productivity is reduced as delays are incurred seeking the knowledge which may be inconsistent and that 'wheel reinvention' may occur adding cost and impacting user perception of service performance of IT, as the service desk may be a user's only interface to the IT department. **(Medium)**

- Service delivery reporting appears inconsistent with several months missed in the year with senior management indicating they have received no view of the status or performance of service desk operations. Within the service delivery team there is little evidence of data analysis to derive service performance, such as the ratio of tickets that are processed by first-line relative to third-line over time. SLA breaches in November 2019 consumed 31% of all open tickets. The causes of this could not be identified and whether any of these SLA failures were due to third-party delays. Without grouping of the tickets in analysis, it was not possible to determine if the SLA failures are attributed to few or many problems. Without data analysis to identify the most significant contributory factors there is a risk that the root causes will not be identified and prevented and allow the issues to continue to impact upon service performance. **(Medium)**

- Problem management activity aimed at preventing recurring incidents and minimising the impact of incidents that cannot be prevented is not yet a mature and established process with only recent examples of analysis being performed on incidents to establish a basic understanding of the workload and problems. Though activity is intended to expand in this area to move the team away from reactive and towards more proactive and preventative activity. **(Medium)**

Continual Service Improvement

- Insightful data analysis to identify incident trends of recurring incidents and potential problems is in its infancy with little evidence of analysis driving continual improvement. We noted recent work has begun to develop dashboards though the ability to 'drill-down' into the summaries was not yet available to the team. Standard reports have not yet been agreed as 'testing' and 'experiments' to determine what data can be extracted and used from the ticketing tool is ongoing. The current dashboards (at the time of the audit), showed high-level summaries limiting any drill-down to identify opportunities for improvement. There is no trend analysis of ticket types and limited trend graphs generally, though this is in work to identify data that will be meaningful and helpful to support improvement opportunities. **(Medium)**

1.4 Additional information to support our conclusion

The following table highlights the number and categories of management actions made. The detailed findings section lists the specific actions agreed with management to implement.

Risk	Control design not effective*		Non compliance with controls*		Agreed actions		
					Low	Medium	High
Principal risk: ability to maintain I.T provision	8	(11)	1	(11)	0	7	2
Total					**0**	**7**	**2**

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

An additional observation we have not raised as an issue is the status of the current role definitions presented for audit. It was not clear if what was presented for audit were current or recent draft role descriptions. They did not indicate if they had been reviewed by the Service Delivery Manager for ongoing suitability. For example, the Service Support Manager role definition quoted that a ‘desirable qualification’ for the role was to achieve ITIL v2. This version of the IT infrastructure Library (ITIL) had been superseded in 2007 (ITIL V3) and in 2019 (ITIL V4).

Similarly, the SDM role presented appeared to be a draft document with incomplete fields, no grading or mandatory or desirable experience or qualification. There is a risk that staff may not be aware of their correct role definition and the extent of their responsibilities and the skills required or to achieve. However, as we were unable to determine their publication status, we have recorded this as an observation.

2 DETAILED FINDINGS

Categorisation of internal audit findings	
Priority	**Definition**
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible regulatory scrutiny/reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, regulatory scrutiny, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management
1	Account Access HR notify IT to revoke accounts for staff leavers is in place. An IT account creation, amendment and deletion high-level process map is in place.	Yes	no	The service desk administers the creation, amendment and deletion of staff leaving employment. A new in-house script to identify "ICT AD User dashboard" report had been developed to highlight all Active Directory (AD) accounts with no activity within the last 60 days. The total number of AD accounts we noted was 1,529. We also noted that 352 accounts were showing as having no activity in the last 60 days which may suggest a staff leaver, long-term absence or staff move. We sampled four of these 'active' accounts at random and cross-referenced them to Active Directory and found that all four accounts were still 'active' The following shows the collar reference (staff number), leaving date and result: • Collar No: 000150, leaving date: 01/04/2018, Account status: 'Active' • Collar No: 009266, leaving date: 03/10/2018, Account status: 'Active' • Collar No: 009061, leaving date: 12/09/2019, Account status: 'Active'	High	Management will review and ratify all inactive accounts exceeding 60 days with HR to validate if staff continue in employment or have left and require account disablement. Where anomalies are identified, management will review the end to end leavers process to

<table>
<tr><th>Ref</th><th>Control</th><th>Adequate control design (yes/no)</th><th>Controls complied with (yes/no)</th><th>Audit findings and implications</th><th>Priority</th><th>Action for management</th></tr>
<tr><td></td><td></td><td></td><td></td><td>
Collar No: 009059, leaving date: 12/11/2017, Account status: ‘Active’
We were unable to identify an HR deletion request record for the above in the IT storage folder for HR deletion forms to verify whether the staff were actual staff leavers.

We were not able to identify if the control weakness was due to HR not informing the IT team (as no records had been filed). There is a risk that some or all these accounts are associated with staff who have left employment with a risk that for those staff who have moved forced that they continue to have access to data (that could be sensitive) that they may no longer be approved to access.

This is mitigated somewhat by the accounts only being exposed to the internal network (behind a firewall where VPN connection is otherwise revoked by collection of a work’s device), though does not mitigate against access to staff who have moved internally.
<table>
<tr><th>Risk Exposure</th><th>Root cause</th></tr>
<tr><td>Risk that failure to adequately disable accounts for staff leavers allows staff access to data that is not approved for their role.</td><td>HR leaver notification process control is not being complied with.</td></tr>
</table>
</td><td></td><td>identify the reason for process breakdown.

Responsible Officer:

Services Delivery Manager

Implementation Date:

30 June 2020</td></tr>
<tr><td>2</td><td>Missing control

<u>Major Incident Service Delivery</u>

The major incident management service delivery process identifies the order of activity or the assignees to the identified roles.</td><td>No</td><td>-</td><td>The major incident service delivery process to be followed in the event of a major disruption to IT services is recorded as a high-level information flow in excel.

The process status is not clear. Some of the fields on the breakdown are incomplete, assignees to the roles are not identified and the sequence of steps is not prescribed to define how the incident is diagnosed as an ‘emergency’ and who declares it.

There is a risk that in the event of a major incident that staff may not be aware of their roles and responsibilities that may introduce delays that increase the impact of the incident.</td><td>High</td><td>Management will review and identify all required roles to support major incident service delivery and ensure named contacts are assigned to the identified roles.

Management will ensure the reviewed and completed document is</td></tr>
</table>

<table>
<tr><th>Ref</th><th>Control</th><th>Adequate control design (yes/no)</th><th>Controls complied with (yes/no)</th><th>Audit findings and implications</th><th>Priority</th><th>Action for management</th></tr>
<tr><td></td><td></td><td></td><td></td><td><table><tr><th>Risk Exposure</th><th>Root cause</th></tr><tr><td>Risk that the IT service major incident process may not be effective in addressing a major incident.</td><td>Lack of formality given to process governance.</td></tr></table></td><td></td><td>distributed to the key stakeholders.

Responsible Officer:

Services Delivery Manager

Implementation Date:

30 June 2020</td></tr>
<tr><td>3</td><td>Missing control

<u>Process Governance</u>

Process documentation is not controlled with formal evidence of review since 2013.</td><td>No</td><td>-</td><td>The process documentation sampled had not been formally reviewed for completeness or continuing suitability since 2013. This includes the following:

• Asset request process;
• Create, amend, delete account map; and
• Major incident management service delivery (process).

Whilst it was stated by the Service Delivery Manager that ‘tweaks’ had been made to the process documentation, there was no indication of what amendments had been made or when. The lack of review, dates and approval status may indicate a failure in process governance.

This can lead to staff being unaware of the process and miss important process steps or not operating the process in a consistent manner affecting the delivery and quality of service operation.

<table><tr><th>Risk Exposure</th><th>Root cause</th></tr><tr><td>Risk that the IT service major incident process may not be effective in addressing a major incident.</td><td>Lack of formality given to process governance.</td></tr></table></td><td>Medium</td><td>Management will review associate service delivery processes to confirm their ongoing suitability and data and approve for publication.

Management will ensure formal change and configuration control is applied to service delivery policy and process documentation.

Management will consider recording process workflow on a page to convey the flow of information between functions</td></tr>
</table>

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management
						and the roles responsible for each part of the workflow. **Responsible Officer:** Services Delivery Manager **Implementation Date:** 31 July 2020
4	**Missing control** <u>Service Desk Staffing Capacity</u> Staff utilisation data is routinely reported to show work loading, type of work and core and non-core hours worked.	No	-	There is no evidence of staff utilisation being used to derive staff productivity. We reviewed high-level 'performance charts' showing ticket resolutions. It was stated that there had been a loss of staff during October and November 2019. However, we noted from available web-based graphs that whilst the number of incoming incidents had increase from September 1,359 incidents to October's 1,715 incidents, we could not identify how many of these tickets had been resolved, as the available reports did not demonstrate this. It is understood from discussion with the Service Desk Supervisor that any sustained performance on ticket resolution would be due to staff incurring non-core hours. Though without time bookings and utilisation data, we were not able to corroborate this. There is no evidence of staff utilisation reports to determine the level of impact on the team through increased non-core hours. Thus, staff productivity cannot be objectively verified. There is a risk that management decision over changes to staff or service may not be able to quantify the impact on service delivery performance. **Risk Exposure** | **Root cause**	Medium	Management will ensure that staff effort on first-line support is consistently captured and staff utilisation trends are monitored and correlated to ticket closure trends to ensure there is sufficient staffing capacity to meet demand and ensure contingency plans are in place to deal with peak demand or staff absence. **Responsible Officer:** Services Delivery Manager

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management
				Management changes to staffing roles or levels may have an adverse impact on service performance. Time bookings do not fully cover all activities and non-core hours. Management are not appraised of the actual productivity and utilisation data to support effective resource planning.		**Implementation Date:** 31 July 2020
5	**Missing control** Staff Skills The capability required for the service delivery team roles, current capability and training needs is formally recorded and planned.	No	-	It was stated by the Service Delivery Manager that there is an intention to ensure cross-skilling to remove single points of failure. We would encourage such a move to ensure a wider skill capability and make the team more resilient to periods of staff absence. At the time of our review the role skills expectations had not been formally established for the roles in the team and the assessment of skill had not been formally recorded beyond a staff appraisal. Consequently, there was no identified training formally captured. There is a risk that team members are not aware of the capabilities, skills and experience required to fulfil their service delivery role and unable to provide continuity of support in times of staff absence, introducing service delays and as the service desk is often the only direct contact that users have with IT, any degradation in service desk performance could erode the user perception of IT.	Medium	Management will introduce a skills profile to identify the following: • The core and desirable business and technical skills for each role; • The actual skills of staff assigned to the roles (possibly using a combination of self-evaluation and ratification via appraisal); and • Gaps between expected and actual skill to allow training or on-the job experience opportunities to be planned as personal development.

Risk Exposure	Root cause
Team skill may be dependent on single points of failure of skill and knowledge affecting service desk performance and eroding user perception of IT.	No means to specify, assess and address skill and experience gaps for service delivery staff.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management
						Responsible Officer: Services Delivery Manager **Implementation Date:** 31 August 2020
6	**Missing control** <u>Knowledge Transfer</u> The service desk knowledge management module is used for capturing, distributing, and effectively using knowledge to help diagnose and restore services following an incident.	No	-	The service desk is not using any formal methods for knowledge sharing. The service desk tool contains a module for knowledge management. However, when we reviewed the content, only nine examples from 2018 existed indicating it was not being used to capture knowledge for new and changed systems and applications. We noted a process by which delivered applications would be delivered into the support ownership of service desk. A criterion of 64 questions were required to be answered before acceptance. The Service Desk Supervisor stated that these were then grouped into ITIL area. Though it was not evident how this knowledge was recorded beyond the individual forms. It was stated by the Service Desk Supervisor that the service desk tool was 'not the best tool'. However, as the team had changed and there had been no visible use or recording of operational issues, it was not possible to determine the tool's effectiveness. The use of knowledge management would help improve collaboration between teams, would minimise lost productivity and help reduce operational costs. The risks of not using a formal means of knowledge management includes: • Reduced outcomes and opportunities to collaborate on the knowledge lost; • Lost productivity incurred in delays in trying to find answers / solutions to incidents and problems; • An increase in duplication or 'wheel reinvention';	Medium	Management will encourage the use of the knowledge management tool. Management will review feedback from operators as to the knowledge management database usability and to identify and address any shortfalls to encourage an environment where knowledge is shared and captured. **Responsible Officer:** Services Delivery Manager **Implementation Date:**

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management
				• Reduced consistency of service delivery (as different solutions to the same issue may occur with variable results); and • Repeat demand for scarce 'experts' each time a similar incident occurs **Risk Exposure**: Ineffective and costly service delivery that fails to achieve defined business outcomes. **Root cause**: Knowledge management is not promoted or applied to create a collaborative and innovative environment.		31 August 2020
7	**Missing control** Service Reporting Service reports are consistently reported.	No	-	We noted that service reporting did not appear to be fully established. The Service Delivery Manager stated that initial reports had commenced in June 2019 to the Senior Leadership Team and that no reports had been produced in September or October 2019 due to staff sick leave. However, the Interim Head of IT confirmed that he had not received any reports this year. There appears to be a least an inconsistent delivery of reports, possible impacted by reduced resilience in the team. We reviewed the November 2019 report. It contained high-level ticket and request summaries and their source e.g. telephone, portal, in person. The reported data did not provide further insight behind the monthly summaries and there was no textual summary of the service performance to offer conclusions or if management attention or a decision was warranted. We noted that third-party adherence to contract SLAs that may otherwise impact on internal SLAs is not routinely monitored. Whilst it was stated by the Service Desk Supervisor that third-party delays have caused SLA failure this could not be corroborated through available reports. **Risk Exposure** / **Root cause**	Medium	Service delivery management and senior management will agree some key service performance measures for service delivery and a timeline for reporting. A basic RAG status and textual summary may help to summarise improvements, requests for support and management decision. Management will agree a means to identify third-party SLA measurement extract where recorded and timestamped with a

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management
				Management is not aware of current and trending service delivery performance or where management support may be required. — Lack of resilience in the service delivery team to cope with staff absence.		view of identifying any third-party performance issues. **Responsible Officer:** Services Delivery Manager **Implementation Date:** 31 August 2020
8	**Missing control** <u>Problem Management</u> There a defined process or applied controls for IT problem management.	No	-	Problem management was not being routinely applied and had not yet fully matured as part of Service Operations as a service should first-line support be unable to fix the root cause of an incident. We were provided some examples of where problem There were some examples where this was being trialled using spreadsheets in the absence of any tools to assist. This resulted in identifying the top 30 repeated incidents. Though no corrective or preventative action had yet been realised at the time of our review. There was little evidence of trend analysis of incidents that might otherwise identify if some incidents are the symptoms of the same underlying problem with a view of either preventing further incidents, major or otherwise. There is a risk that potential problems are not being identified to enable preventative action to address the problem before it becomes a major incident that could impact many organizational departments. **Risk Exposure** — **Root cause** Problem management activity is not routinely applied to identify, prevent or address problems that impact upon — Lack of skills, knowledge, staff availability forcing priority focus on	Medium	Management shall develop a problem management process to deal with problems that do occur or could occur (prevention). Service Delivery Management will review the problem management capability of the tool to determine if it is suitable and the possibility if there an inhouse solution to support ticket analysis. **Responsible Officer:**

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications		Priority	Action for management
				users.	dealing with incidents (symptoms of a potential problem).		Services Delivery Manager **Implementation Date:** 30 September 2020
9	**Missing control** <u>Continual Service Improvement</u> Service availability and capacity reports established in September 2019. Service desk ticket analysis is mature to drive continual improvement activities. Management reporting is fully established.	No	-	We noted that use of available service data and knowledge of the service desk tool to identify and make use of the data for analysis and reporting was immature. The available dashboard of the service was derived from in-house scripts to interrogate the tools' raw database. The Service Delivery Manager stated that additional internal work was required to provide basic dashboard reporting. This included the development of scripts that interrogated the service desk tool's SQL data to access its raw data to derive reporting that could not be obtained from the tool. The staff identified shortfalls of the service desk tool had not been reported to management as a risk on the risk register, or as an issue on the monthly highlight report and there is a risk that management may not be aware. The apparent limitation of the tool was limiting the opportunity for meaningful analysis to identify opportunities for improvement. In the tools measurement and reporting capability was being addressed in-house by using a Microsoft business analytics to interrogate the tools database and extract the raw data into more meaningful charts. Though this analysis was at an early stage. The following was observed: • The service desk tool produces basic ticket and request count of information. We were unable to objectively verify average ticket closure time or the causes of SLA failure. We noted, for example that out of 351 tickets that were open, 109 tickets (31.14%) had breached SLA. Though without available analysis reports we could not confirm the contributory factors behind these failures and how many might be due to third-party delays, as suggested by		Medium	Management will develop and agree a continual service improvement process. This process will identify the sources of data reports and how potential improvement actions are tracked and reported. Service delivery management will review the open tickets beyond 12 months with a view to closing them as no longer valid and reviewing tickets greater than six months old to confirm with the user if they are still required. **Responsible Officer:**

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management
				the Service Desk Supervisor. We noted the oldest open ticket was October 2018. Aged tickets may no longer be valid and therefore unnecessarily adding to the queue measurements and perceived workload. • Problem management is not mature to derive analysis of incidents for trends or to conduct effective root cause analysis of problems with a view or dealing with problems effectively, or ensuring they are prevented at the early stages to avoid potential major incidents. • Management reporting is inconsistent and does not draw any conclusions on service performance or improvement to enable effective management decisions to be taken. Whilst we encourage the in-house service team to continue the efforts to improve the availability of data analysis reports, this must provide meaningful data to allow focussed analysis on areas where improvement opportunities can be taken to identify cost drivers, causes of repeat incidents (possible an underlying problem) and factors contributing to SLA failure.		Services Delivery Manager **Implementation Date:** 30 September 2020

Risk Exposure	Root causes
The reputation of IT is damaged and user perception of valued contribution to the organisation decreases.	Data analysis is not sufficiently mature to allow identification of areas to target improvements and reduce repeat tickets.

APPENDIX A: SCOPE

The scope below is a copy of the original document issued.

Scope of the review

The scope was planned to provide assurance on the controls and mitigations in place relating to the following risk:

Objective of the review	Risks relevant to the scope of the review	Risk source
To provide assurance over IT service delivery with specific focus on the service desk, specifically incident and problem management, utilisation and continual service improvement.	**Principal risk**: ability to maintain I.T provision	Principal Risk Register

When planning the audit, the following areas for consideration and limitations were agreed:

Areas for consideration:

The following areas will be considered as part of the review:

Service Governance

- We will assess the governance structure in place including service desk policies and processes, roles and responsibilities and the management of service desk operations and service issue escalation;
- We will assess service level management in place with internal business functions and review service monitoring to identify the extent to which service levels are being assessed, reported and attained; and
- We will assess service capacity management to review the processes in place to identify service demand and the plans in place to ensure adequate capacity and effective use of staff allocation and utilisation in the service desk.

Service Operation

- We will assess incident management and the process for logging, recording and resolving issues or providing 'workarounds' to restore service operations as quickly as possible;
- We will assess problem management activities to detect, log, investigate, diagnose and deliver resolutions (workarounds or permanent) and the practice for formal incident closure;
- We will assess the service operations to review the extent to which the service desk delivers agreed levels of service to users; and
- We will assess 3rd line engineering support activities to assess the current utilisation metrics captured and reported to management to enable planning and assignment of priority work.

Continual Service Improvement

- In respect of service measurement, we will assess the service measurements, data analysis and reporting in place to monitor incidents tickets type, severity and work queues and identify any corrective actions taken as a result of data analysis;

- In respect of service reporting, we will assess the frequency, coverage, distribution and the level of service reporting performed and how it is used to drive preventative actions that avoid recurring incidents; and
- In respect of service improvement, we will assess the effectiveness of process and practices implemented to improve the IT service.

Third-party management

- We will assess the level of security control around the granting of remote access to third parties, the extent of access granted and level of monitoring during remote connection and post-connection activities.

Limitations to the scope of the audit assignment:

- The scope of our work will be limited only to those areas that have been examined and reported and is not to be considered as a comprehensive review of all aspects of IT service management.
- All testing will be undertaken on a sample basis and for the financial year 2019 only.
- The focus of our review is primarily the design and operation of key controls and monitoring of service desk operations and will not include all monitoring controls or detailed testing.
- We will not confirm compliance with GDPR and/or provide any legal or regulatory advice.
- Our work in relation to IT service management will be at a high level only and will not include all service operational controls or detailed testing.
- The information provided in the final report should not be considered to detail all errors or risks that may currently or in the future exist within data security and governance, and it will be necessary for management to consider the results and make their own judgement on the risks affecting North Yorkshire Police and the level of specialist computer audit coverage they require in order to provide assurance that these risks are minimised.
- In addition, our work does not provide an absolute assurance that material error; loss or fraud does not exist.

APPENDIX B: FURTHER INFORMATION

Persons interviewed during the audit:

- Interim Head of IT
- Digital Delivery Manager
- Service Delivery Manager
- Service Management Analyst
- Service Desk Leader
- Service Management Analyst

Documentation reviewed during the audit:

- Asset Administrator (role profile)
- First Line Engineer (role profile)
- ICT Service Management Analyst (role profile)
- ITIL (topics assigned to Service analysts)
- Priority of incidents
- Service Availability and Capacity Report, September and October 2019

FOR FURTHER INFORMATION CONTACT

Dan Harris, Head of Internal Audit

Tel: 07792 948767

Daniel.Harris@rsmuk.com

Angela Ward, Senior Manager

Tel: 07966 091471

Angela.Ward@rsmuk.com

Philip Church, Client Manager

Tel: 07528 970082

Philip.Church@rsmuk.com

rsmuk.com