SURREY COUNTY COUNCIL
AUDIT REPORT

Review of
Incident Response
2015/16

Prepared for: Paul Brocklehurst, Head of IMT

Prepared by: Nighat Sheikh Senior Auditor

Sue Lewry-Jones
Chief Internal Auditor
Surrey County Council
County Hall
Kingston upon Thames
Surrey
KT1 2EA

February 2016

Additional circulation list:

External Audit	Grant Thornton UK LLP
Group Manager, Business Solutions	Chris Millard
Service Finance Manager	Susan Smyth
S151 Officer	Sheila Little
Strategic Director	Julie Fisher
Risk and Governance Manager	Cath Edwards
Audit and Governance Committee	All
Cabinet Member for Business Services and Resident Experience	Denise Le Gal
Chairman of Corporate Overview Board Select Committee	Steve Cosser

Glossary:

IMT	Information Management and Technology
KPI	Key Performance Indicator
SIEM	Security Information Events Monitoring
PSN	Public Sector Network
SPLUNK	Software for searching, monitoring, and analyzing machine-generated big data, via a web-style interface
Gov CERT	UK National Computer Emergency Response Team
BCI	Business Continuity Institute
CHECK	IT Health Check Service, or CHECK, was developed to enhance the availability and quality of the IT health check services that are provided to government in line with HMG policy
PCI DSS	Payment Card Industry Data Security Standard
SAQ C	Self Assessment Questionnaire C
PDQ	Process Data Quickly (card payment, chip & pin machines)
CMS	Content Management System
ISP	Internet Service Provider
ID	Identification Device
Single Sign On	Session/user authentication process that permits a user to enter one name and password in order to access multiple applications
CESG	Communications Electronics Security Group
GCSX	Government Connect Secure Extranet

Audit opinions:

Effective Controls evaluated are adequate, appropriate, and effective to provide reasonable assurance that risks are being managed and objectives should be met.

Some Improvement Needed A few specific control weaknesses were noted; generally however, controls evaluated are adequate, appropriate, and effective to provide reasonable assurance that risks are being managed and objectives should be met.

Major Improvement Needed Numerous specific control weaknesses were noted. Controls evaluated are unlikely to provide reasonable assurance that risks are being managed and objectives should be met.

Unsatisfactory Controls evaluated are not adequate, appropriate, or effective to provide reasonable assurance that risks are being managed and objectives should be met.

1. INTRODUCTION

1.1 An Information Security event is indicated by a single or a series of unwanted or unexpected information security events, which have a significant probability of compromising business operations and threatening information security.

1.2 Following the planning process and discussions with the IMT Service, it was agreed that an audit would be included in the agreed Internal Audit Plan for 2015/2016. Internal Audit would undertake a review to ensure that controls were operating effectively for Incident Response.

1.3 Incident Management is defined as the capability to effectively manage unexpected disruptive events, with the object of minimizing impact and maintaining or restoring normal operations, within defined time limits.

1.4 A review of Incident Management Response was included as part of the Annual Audit Plan approved by Audit and Governance Committee in March 2015 and was undertaken following agreement of the Terms of Reference included at Annex A. This report sets out the findings and recommendations of the review. The completed Management Action Plan accompanies this report as Annex B.

2. WORK UNDERTAKEN

2.1 A review of management's assessment of compliance and what sources of assurance they have to determine the degree of compliance was undertaken.

2.2 A risk matrix report has been completed. Risks have been assessed and controls in place evaluated to ensure that procedures are operating effectively.

2.3 Compliance testing was carried out to ensure controls are operating satisfactorily. The objective of the tests was to review the adequacy of the following:

- How incidents are being logged and investigated;
- How staff are able to minimize the impact of an incident to the organisation;
- How the authority is providing a defence against any subsequent incidents;
- How we ensure continuity of services after an incident and reporting of incidents.

2.4 There were no previous recommendations to follow up.

3. OVERALL AUDIT OPINION AND RECOMMENDATIONS SUMMARY

3.1 The overall opinion following this audit is some improvement needed.

3.2 A specific control weakness was noted; generally however, controls evaluated are adequate, appropriate, and effective to provide reasonable assurance that risks are being managed and objectives should be met.

3.3 **Recommendations analysis:** There was one medium priority recommendation summarised below:

Rating	Definition	No.	Para.Ref.
High	Major control weakness requiring immediate implementation of recommendation	0	
Medium	Existing procedures have a negative impact on internal control or the efficient use of resources	1	5.3.8
Low	Recommendation represents good practice but its implementation is not fundamental to internal control	0	
	Total number of audit recommendations	1	

4. MANAGEMENT SUMMARY

4.1 Surrey County Council has a robust system in place for managing ICT Incidents.IMT have established various conformance criteria and policies and procedures are in place for staff to follow in the event of an IT incident.

4.2 Internal Audit carried out a review to ensure that the system for managing the Incident Management process was adequate, and that effective internal controls applied to these functions. It was felt that in light of the discussions with officers and the compliance testing carried out, the system currently operating is sound. The council has in place an incident management policy and an established incident management process. Review of a sample of major incidents confirmed compliance with the process and expected best practice.

4.3 There is a system in place for reporting security weaknesses and threats, and systems for intrusion prevention and detection that are compliant with Public Services Network security requirements.

4.4 There is however one area which Internal Audit has found to be non-compliant with best practice, this was due to Business Continuity testing exercises not being carried out. Further details can be found at section 5.3 in this report.

4.5 In view of the above finding, set out in more detail in section 5 of this report, the overall audit opinion was found to be **Some Improvement Needed**.

5. FINDINGS AND RECOMMENDATIONS

5.1 Incident Management Policy / Major Incident Process

Findings

5.1.1 The authority currently has an Incident Management Policy which was last revised in November 2015. The policy incorporates the scope and purpose of the Incident Management process, and also refers to other policies which should be applied.

5.1.2 The operational procedures contained within the policy give specific guidance to all staff of where and how to report an incident, including the response and reporting of logged incidents.

5.1.3 The logged incidents recorded are given a specific priority from 1 – 6 with target response times for resolution.

5.1.4 There is also a Major Incident Process document which was last reviewed in May 2015. This document details the steps to take in case of a major incident for members of staff; it begins with notifying the IMT Service Desk and prioritisation of a case, to recording and escalation process and finally, resolution with a report detailing the incident.

5.1.5 The document also has a process flow diagram which details graphically the major incident process.

5.1.6 Testing was carried out, and a sample taken, from the major incident logs spreadsheet. All major incidents have to be logged with a support call reference number, and date and time of incident or logging of call.

5.1.7 The IMT Service Desk team has access to the spreadsheet but only the Service Desk Interim Manager and two Team Leaders have access to update details within this document.

5.1.8 A judgemental sample of ten cases was taken and it was noted that:

- All ten cases had a helpdesk / call reference number assigned.
- All ten cases date and time reported and call resolved time recorded.
- All ten cases had an engineer assigned (including 2 cases being assigned to BT).
- Eight / ten cases met the standard SLA for helpdesk resolution.
- All ten cases had a Major Incident Report detailing summary of events; resolution and recommendations/lessons learnt section.

5.2 **Incident Response Review**

Findings

5.2.1 A risk assessment was carried out and it was noted that risks are being adequately managed and control objectives are being met for the following functions relating to the Incident Response Review:

- Incident Reporting Procedures.
- Incident Management Processes (Documented).
- Procedures / Guidelines updated.
- Failing of reporting mechanisms.
- Mechanisms to enable incident monitoring to be quantified and monitored.
- Disciplinary process in place (for violation of organisational security policies).
- Major Incidents are given preferential treatment.
- Incident contacts regularly updated.
- Problem resolution process.
- Forensic Investigation in place.
- Post Incident Reviews up to date and carried out.
- Closure Reports sent to Management.

5.2.2 There is a Major Incident Process document which was updated and reviewed in May 2015. The document details the various steps that staff need to be aware of in the event of any major incident; and explains how each case will be dealt with by the IMT Service Desk team as follows:

- Notify IMT Service Desk.
- Pass incident detail to Service Desk Senior Technician and or Team Leader/Manager.
- Pass case to IMT resolver team.

- Once resolved pass back to IMT Service Desk.
- Incident is discussed at the weekly operational review meeting.
- Problem management which investigates and inputs open actions into the problem process.

5.2.3 The IMT Service Desk all work towards standard KPI's (Key Performance Indicators) for dealing with requests and resolving issues. For major issues the IMT Service Desk has a specific document for analysis of incidents, from this document the IMT Service Desk operator can categorise or rate priority for an incident based on their own judgment and experience.

5.2.4 The authority use secure intrusion detection / prevention systems, which are compliant with PSN standards. Surrey County Council is currently using the following software applications:

- Nessus scanners for detection of any vulnerabilities.
- SPLUNK for Security Information Events Monitoring and also for conducting log analysis.
- SPLUNK Enterprise Security Module to produce alerts and dashboards.
- Symantec Endpoint Protection which produces logs that are then fed into the SIEM Security Information Events Monitoring system (SPLUNK).

5.2.5 There are various sources of incident awareness and risk intelligence monitoring tools used by the security team including:

- Gov CERT
- Security Focus
- Secunia

5.2.6 There is a system for reporting of security weaknesses or threats. The conformance criteria is clearly laid out within the IT Security Policy at page 69. These include the following definitions:

- Security incidents are defined.
- Incident procedures including advice to users from IMT in the event of an incident.
- Who is responsible for the reporting of security incidents and how these will be managed.
- Incident classification types.
- Differences between common security incidents e.g. daily events (human error, forgetting a password, forgetting to update a password within a specified timeframe), although repeated incidents may require further investigation. Significant and unusual events (which require further investigation), e.g. if a virus is detected by a user, this should immediately be reported to the IMT Service Desk.
- Statistics on such events.
- Reporting and review of events.
- Significant security events and unusual events (which require investigation).
- Reporting to Management.
- Incident closure to rectify action of staff involved (e.g. via education; disciplinary action).

5.2.7 There is a mechanism in place for monitoring of incidents; a report is produced by the Interim Service Desk Manager at the end of the month which details the type of incident including volumes of incidents, but does not include any malfunctions which may have occurred. Malfunctions such as how the incident may have been prevented from happening initially are included in the individual incident management reports.

5.2.8 Currently in regard to major incidents, costs per incident are not being evaluated. This is something that the Problem and Performance Manager is reviewing and will try to incorporate into his monthly performance reports.

5.2.9 There is a formal Disciplinary Process in place for all employees. Policies are available to view on the council intranet, include the following "Unauthorised action on behalf of the council or service including inappropriate use of IT systems and breaches of IT security" which may be treated as misconduct.

5.2.10 Priority incidents are managed and reported on a separate Major Incidents Spreadsheet, these are prioritised by specific category from the helpdesk call.

5.2.11 The Major Incident Report includes a section for permanent resolution. These documents are maintained by the IMT Service Desk/Manager.

5.2.12 All IT users must report any actual or suspected incident as soon as practical as per the Security Incidents and Data Breaches document available on the council intranet:

- "All staff (including contractors, temporaries, or homeworkers who use their own equipment for council business), must report to the IMT Service Desk and inform their line manager.
- Staff should not carry out any investigation or collection of evidence, unless asked to do so by the IMT Technical Services Team.
- Once a data breach has been reported, managers are required to complete the data breaches template and return to their Information Governance Team.
- A log of reported breaches is maintained corporately to monitor trends and provide necessary guidance to mitigate re-occurring breaches.
- Data breaches are investigated by managers in conjunction with their Information Governance Team.
- High level data breaches are managed through the Significant Event Process, where a service director will coordinate the process".

5.2.13 From the Security Incidents and Data Breaches document as mentioned in 5.2.12, second bullet point, staff are given limited guidance for the collection of digital evidence, there are no specific procedures to follow for cases leading to a court case, and the need for evidence, and chain of custody for collection of evidence, is paramount. The Technical Delivery Manager believes that the guidance which is published is sufficient for the council's need, and if anything further identified is believed to be a criminal act, specialists or the Police would be notified to investigate.

5.2.14 Details of Post incident reviews are included within Major Incident Reports, and these include details of IT services impacted; any devices/services affected; teams involved; cause/reason for incident; whether the incident could have been prevented and if so how; a summary of events; resolution; any issues arising from the event; recommendations/lessons learnt and finally whether it was a known error. It also details who to assign for permanent resolution.

5.2.15 Incident closure is also detailed within the Major Incident Report. Within the section recommendations/lessons learnt, an incident response post mortem analysis is conducted. This report is also widely distributed dependant on the significance of the incident.

5.2.16 An IMT Incident Risk Register was updated in December 2015. A review of the Risk Management process is currently being carried out by Internal Audit.

5.3 **Business Continuity / Disaster Recovery Testing**

Findings

5.3.1 There is an IMT Business Continuity Plan which was updated in May 2015; the objectives of the plan are as follows:

- To identify IMT mission critical activities and the resources required to ensure these activities could carry on under any circumstance.
- To analyse and respond to the risks to IMT.
- To provide a framework for recovery of the services.
- To identify alternative working arrangements to allow continuation of service.
- To identify key roles and responsibilities to be involved in the recovery process.

5.3.2 From the assumptions within the document, it is clear that the Business Continuity Plan will need to be tested annually and evaluated to ensure it adequately meets the needs of the service.

5.3.3 From discussions held with various officers within IMT it was noted that the Business Continuity Plan had not been tested, and from documentation sent through to audit, the last exercise which had been carried out was the Migration of Data Centres in November 2012.

5.3.4 A meeting was held with the Head of Emergency Management to discuss the process of testing Business Continuity. This included detailing the methods and techniques used for Business Continuity exercises within the council, based on BCI good practice methods.

5.3.5 The authority has carried out table top exercises for all services, and records have been kept, with dates of when the last exercise was carried out. It was noted that IMT had not carried out an exercise in the last three years.

5.3.6 It is important that IMT cover the following areas in their Business Continuity Plan:

- Ability to effect safe and swift shutdown of systems without data loss
- Callout contract with IT provider that covers breakdown, network problems and other failures
- Renegotiating service contract, if it doesn’t include Business Continuity options
- Security of systems, PCs and laptops
- Security of stored data
- Cascade call procedure – particularly if land lines are down

Risks

5.3.7 Risks can range from minor risks, which may not have any significant impact on the council; to moderate risks which could have a minor impact, with minor internal disruption to a service; to significant risks which potentially could cause a moderate impact, with internal disruption on one or more business units; to a major risk which could lead to a significant impact, with potential for either fatality or serious injury to several people.

Recommendation

5.3.8 Formal testing of the IMT Building Continuity Plan should be carried out within the next financial year. This will ensure that the IMT team can respond to a major incident and that immediate support is available for all critical infrastructure environments, and all priority support applications.

5.4 PSN–Compliance / IMT Security

Findings

5.4.1 An audit was completed on PSN compliance in December 2014 with an Effective opinion.

5.4.2 The authority has once again been accredited until July 2016. Certification demonstrates that the infrastructure is sufficiently secure to connect to PSN for another year.

5.4.3 A penetration test/health check was carried out in June 2015. This led to an action plan for the authority to remediate. This was completed by an independent security assessor who is also CHECK registered.

5.4.4 The remediation plan for the current year was assessed by audit; it was found that there were a couple of outstanding issues still to be resolved for the onsite remediation plan. The remediation plan for external outstanding issues was also assessed; all issues had been resolved within a few weeks of the report being issued.

5.4.5 The outstanding issues were discussed with the Network and Security Technical Officer and although there were two actions which had not been resolved; the authority had decided to accept the risk for these two issues, one was due to the practicalities of implementing individual passwords, for the shared local administrator user login, on end user devices. The other was not being able to patch for a specific vulnerability, this was an inherent problem. The issue is being mitigated somewhat, by asking users to use complex passwords to prevent a brute force attack.

5.4.6 Surrey County Council was audited by PSN in November 2015. No issues were raised.

5.4.7 There has not been any major hacking or disruptive attacks on the council's network in the last year, although there has been a denial of service attack against one of the ISP's (JaNet). A full major incident report was completed, with issues arising from the incident reported to the appropriate officers.

5.4.8 A staff warning message has recently been sent out reminding staff not to open attachments, within messages from unknown recipients. This was following the council receiving an unusually large number of viruses/malware attached to emails which could cause major disruption to the systems, potentially leading to a shutdown of all systems, as per a recent incident at Lincolnshire County Council.

5.5 PCI DSS

Findings

5.5.1 The authority has completed an attestation of compliance to PCI DSS, this allows the authority to accept credit and debit card payments via a variety of methods including:

- Acquirers and payment gateways.
- Third party systems.
- Payment by telephone.
- Online payments.
- PDQ machines (face to face and some mediated payments).
- Schools mange their own PCI DSS.

5.5.2 All staff taking payments for the authority are asked to sign off a document, reminding them of responsibilities including the following:

- All users must have a unique user ID and password. This information must not be shared.
- If card details are written down they must be held securely, and destroyed once payment is taken.
- Card details must never be collected or stored electronically.

5.5.3 A discussion was held with the Team Lead (Data Management), to ensure that the process for PCI DSS was compliant with the requirement. From this discussion it was noted the compliance document SAQ C was completed. This is due to no debit or credit card details being stored electronically on the network. The SAQ document was sent off in November 2015. This exercise is completed annually. PCI DSS have not carried out an audit, and the self assessment along with regular quarterly scans is accepted for compliancy.

5.5.4 It was noted by Internal Audit that payments were taken by Helpdesk Finance Officers and each officer had individual login and passwords. There was an issue for Contact Centre staff taking payments for copy certificates, as the officers were using generic login and passwords to take payments, so it would be difficult to recognise which officer had taken the payment. This was in breach of PCI DSS compliance.

5.5.5 A discussion was held with IT Projects and Systems Lead; she confirmed generic logins were being used by Contact Centre staff, the reason being a variety of staff were taking payments for copy certificates only, and it was difficult to set up individual users.

5.5.6 Internal Audit advised this was not compliant with PCI DSS and could possibly breach the requirement. Forty five officers had the ability to take payments over the telephone and Internal Audit suggested the service liaise with IMT and request whether single sign on facility could be implemented; (session/user authentication process that permits a user to enter one name and password in order to access multiple applications). This would ensure all users had individual ID and password and would be matched to their network login.

5.5.7 The IT Projects and Systems Lead set up an action plan to ensure that the service was in compliance with the requirement. Initially a message was placed on Surrey County Council website to say "Due to technical issues the Contact Centre is currently unable to take payments for birth, death or marriage copy certificates over the phone. You can order and pay for copy certificate online. If you do not have internet access at home, please visit one of our libraries where you can use the internet facilities to access Surrey County Council website".

5.5.8 IMT was contacted and it was agreed that twelve officers would be given individual logins to enable service delivery again. IMT CMS & Collaboration Lead (IMT Development) confirmed that this issue was resolved. IMT were unable to give a timescale for giving all users individual logins, as with the new Outlook project due to be implemented, all users would have this facility.

5.6 Cloud / Office 365

Findings

5.6.1 The authority is currently going through major changes as part of the 'Modern Worker Programme' primarily changing from the Lotus Notes environment to Microsoft Exchange Online apart from email requiring GCSX transit.

5.6.2 The programme is being managed by the Principal Consultant (Projects) Project Delivery Team.

5.6.3 A security risk assessment has been carried out and the top risks noted for this project are as follows:

- Non compliance with CESG guidance on unmanaged devices may jeopardise Council's reputation or data loss defence.
- Data loss from a lost, stolen or compromised unmanaged device.
- Data loss from a lost, stolen or managed device.
- Data loss from compromise to Microsoft data centre
- Data loss from compromise to Surrey County Council data centre.
- Extended service disruption due to Microsoft data centre or network.
- Extended data disruption due to Surrey County Council data centre or network.
- Poor performance of solution components due to poor network performance.

5.6.4 The data has been assigned safe harbour jurisdiction, data will mainly be held in the Microsoft Cloud European Union zone, but GCSX exchange data will be held in the UK in Surrey County Council's own Primary and Secondary Data Centres, according to GCSX requirements.

5.6.5 There will be certain enhanced security access controls for users outside of the Surrey County Council network perimeter; Microsoft's Azure active directory two-factor solution (something you have and something you know) will be utilised to ensure security.

5.6.6 Business Continuity requirements have been included within the project requirements and the solution features a SLA of 99.9% availability.

5.6.7 The Modern Worker project is currently in beta pilot phase (testing) stage and key milestones are being monitored and tracked. The updated risk and position will be presented to Risk and Information Governance Board on 2 March 2016.

6. ACKNOWLEDGEMENT

6.1 The assistance and co-operation of all the staff involved was greatly appreciated.

ANNEX A

TERMS OF REFERENCE

Incident Response Audit
2015/16

BACKGROUND

Following the planning process and discussions with IMT Service, it was agreed that an audit would be included in the agreed Internal Audit Annual Plan for 2015/2016 to undertake a review to ensure that controls were operating effectively for Incident Response Review.

Incident Management is defined as the capability to effectively manage unexpected disruptive events with the object of minimizing impacts and maintaining or restoring normal operations within defined time limits.

The Authority must be prepared for incidents that may occur from a variety of sources, including those due to maliciously planned attacks, as well as non-malicious attacks from trusted insiders that could result in damage.

Management needs to be able to evaluate independently the incident response process on a regular basis to gain assurance on the effectiveness of controls within the process.

PURPOSE OF THE AUDIT

To ensure that risks are being adequately managed including:

- Are incidents investigated adequately?
- Are incidents logged?
- How do we minimize the impact to the organisation from an incident?
- How do we provide a defence against subsequent attacks?
- How do we restore continuity of services after an incident?
- How are we reporting incidents and who too?
- Inability to satisfy regulatory processing due to outages?
- The Insider Threat – e.g. breaches relating to personal data being stolen/lost

WORK TO BE UNDERTAKEN

The findings of this audit will be based on discussions with officers responsible for the Incident Response Review and a review of relevant documentation which may include: Penetration test reports, findings and follow up actions, Information Governance reports and any incident reports will be tested to establish the process is operating effectively and that procedures in place are followed correctly.

OUTCOMES

The findings of this review will form a report to Surrey County Council management. This report will provide an overall audit opinion on the effectiveness of systems in place, plus set out recommendations for improvement if required. Subject to the availability of resources, and the agreement of the auditee, the audit will also seek to obtain an overview of arrangements in place for:

- Data quality and security;
- Equality and diversity;
- Value for Money; and
- Business continuity.

The outcome of any work undertaken will be used to inform our future audit planning processes and also contribute to an overall opinion on the adequacy of arrangements across the Council in these areas.

REPORTING ARRANGEMENTS

Auditor:	Nighat Sheikh, Senior Auditor
Supervisor:	Simon White Audit Performance Manager
Reporting to:	Paul Brocklehurst, Head of Information Management and Technology.
Audit Ref:	