ABERDEEN CITY COUNCIL

COMMITTEE	Audit, Risk and Scrutiny Committee
DATE	22 February 2018
REPORT TITLE	Internal Audit Report AC1810 – Major IT Business Systems
REPORT NUMBER	IA/AC1810
LEAD OFFICER	David Hughes
AUTHOR	David Hughes

1. PURPOSE OF REPORT

1.1 The purpose of this report is to present the planned Internal Audit report on Major IT Business Systems.

2. RECOMMENDATION

2.1 It is recommended that the Committee review, discuss and comment on the issues raised within this report and the attached appendix.

3. BACKGROUND / MAIN ISSUES

3.1 Internal Audit has completed the attached report which relates to an audit of Major IT Business Systems.

4. FINANCIAL IMPLICATIONS

4.1 There are no direct financial implications arising from the recommendations of this report.

5. LEGAL IMPLICATIONS

5.1 There are no direct legal implications arising from the recommendations of this report.

6. MANAGEMENT OF RISK

6.1 The Internal Audit process considers risks involved in the areas subject to review. Any risk implications identified through the Internal Audit process are as detailed in the attached appendix.

7. IMPACT SECTION

7.1 **Economy** – The proposals in this report have no direct impact on the local economy.

7.2 **People** – There will be no differential impact, as a result of the proposals in this report, on people with protected characteristics. An equality impact assessment is not required because the reason for this report is for Committee to review, discuss and comment on the outcome of an internal audit. The proposals in this report will have no impact on improving the staff experience.

7.3 **Place** – The proposals in this report have no direct impact on the environment or how people friendly the place is.

7.4 **Technology** – The proposals in this report do not further advance technology for the improvement of public services and / or the City as a whole.

8. APPENDICES

8.1 Internal Audit report AC1810 – Major IT Business Systems.

9. REPORT AUTHOR DETAILS

David Hughes, Chief Internal Auditor
David.Hughes@aberdeenshire.gov.uk
(01467) 537861

ABERDEEN
CITY COUNCIL

Internal Audit Report

IT & Transformation

Major IT Business Systems

Issued to:

Simon Haston, Head of IT & Transformation
Fraser Bell, Head of Legal and Democratic Services
Steven Whyte, Head of Finance
Caroline Anderson, Information Manager
External Audit

Date of Issue: December 2017 **Report No. AC1810**

EXECUTIVE SUMMARY

The Council relies on its major IT business systems to deliver front-line services, pay and manage employees, manage contracts, pay suppliers, raise charges to customers and carry out statutory functions. The objective of this audit was to ensure that the risk of major IT business systems failure is adequately managed.

Whilst the process of classifying and risk assessing systems is under way, there have been delays in this process, presenting risks to business continuity. Business critical system disaster recovery testing is taking place, however it has yet to be scheduled for some.

The Council's cyber security is managed through the use of a next generation firewall and intrusion prevention system, email filtering software, and anti-virus software, which are being kept current through automatic updates. Arrangements are in place with the Council's data centre provider for scheduled updates to business critical systems. IT staff are being made aware of new threats to cyber security through membership of relevant groups and use of live online security feeds. Business critical systems are backed-up in full on a regular basis, with back up files held appropriately.

Recommendations have been made to enhance written procedures; formalise deadlines for the risk assessment of systems; re-assess system risk assessments where overdue; reflect business critical systems in business continuity plans and risk registers; and finalise the schedule of business critical system disaster recovery testing.

1. INTRODUCTION

1.1 The Council relies on its major IT business systems to deliver front-line services, pay and manage employees, manage contracts, pay suppliers, raise charges to customers and carry out statutory functions. Failure of these systems would disrupt critical functions, potentially cause financial loss or suffering, and potentially lead to reputational damage for the Council. IT and Transformation is responsible for monitoring the ICT Infrastructure and systems to prevent or minimise system unavailability.

1.2 The objective of this audit was to ensure that the risk of major IT business systems failure is adequately managed.

1.3 The factual accuracy of this report and action to be taken with regard to the recommendations made have been agreed with Simon Haston, Head of IT & Transformation, Norman Hogg, Security Architect and Steven Robertson, Infrastructure Architect.

2. FINDINGS AND RECOMMENDATIONS

2.1 Ownership and Reporting

2.1.1 The IT and Transformation Business Continuity Plan, last prepared in May 2017, states that proactively monitoring the ICT infrastructure and systems, to prevent or minimise system failure, is a critical function of the Service. In doing so, the Service diagnoses and resolves ICT faults for live systems, computers, networks, telecommunications, and other associated ICT infrastructure services. The Service also monitors and maintains the Council's ICT Security Systems, ICT Asset Management system, and software licences.

2.1.2 Whilst IT & Transformation is responsible for the corporate IT infrastructure and core Council-wide systems, there are a number of IT systems which are maintained by Service systems teams. As part of a wider review of the Council's structure under the Target Operating Model, IT functions and systems teams are to be consolidated.

2.1.3 In September 2016, the Audit, Risk and Scrutiny Committee (AR&SC) approved changes to the Council's Information Governance oversight and reporting arrangements, which included the formation of the Information Governance Group (IGG). The purpose of the IGG is to support and drive the broader information governance agenda, provide the Corporate Management Team (CMT) with assurance that effective control mechanisms are in place, and manage and mitigate the Council's information risks. The Group previously provided a quarterly report to CMT on Information Governance Management and an annual report to AR&SC. From November 2017, these reports will go to the Governance Delivery Board on a monthly basis and thereafter reported through the Transformation Portfolio Framework. These reports include a section on cyber security risks, covering the number of incidents and attempts threatening the Council's information, software, infrastructure or computer network, that originate from inside and outside the organisation.

2.1.4 The 2017/18 quarter 1 performance report was reported to the IGG on 28 August 2017 and the annual report for July 2016 to June 2017 was discussed and noted by the AR&SC on 26 September 2017.

2.1.5 The IT Security Architect prepares a monthly ICT security report for IT&T senior management. This includes various statistics including: web risks prevented; email traffic; events prevented by the intrusion prevention system; telephone activity; IT risk register status; and an update on the operational risks of high importance. A sample of reports covering 3 months was selected to establish if they had been issued on a monthly basis. A report was not produced for one of the months selected (July 2017) however reports were produced for June and August 2017, indicating a frequent update on IT activity and risks is being circulated to the senior IT&T management team.

2.2 Business Impact and Risk Assessment

2.2.1 Directorate risk registers are reported to the Audit, Risk and Scrutiny Committee on a rolling basis. The CH&I Risk Register was last reported in June 2017, the E&CS Risk Register in September 2016, and the Corporate Governance Risk Register in April 2016. They all included the risk of major IT Business Systems failure and identified potential impact (see below), causes, control effectiveness, and mitigating actions. The Corporate Risk Register was reported to AR&SC in September 2017. This includes risk Corp007 'Risk of poor information management and security', covering impacts, causes and controls at a Council level. Controls include critical systems being risk assessed and protected appropriately. The Corporate Risk Register has been amended since it was reported to AR&SC in September 2017 and will be reported to CMT on 21 December 2017 with cyber security separated from Corp007 as a Corporate risk in its own right.

2.2.2 The risk registers identify the potential impacts of business system failure as: failure to deliver essential services; harm to vulnerable members of the public; harm to the local economy; inability to pay employees; inability to pay suppliers or raise revenue from customers; contracts not managed; workforce not managed; statutory requirements not met and reputational damage. Whilst Directorate risk registers identify the risk of major IT Business System failure, all major 'business critical' systems are not included in the Directorate risk registers.

Recommendation
Consideration should be given to identifying business critical systems in the Directorate risk registers.

Service Response / Action
Agreed.

Implementation Date	Responsible Officer	Grading
January 2018	Performance and Risk Manager	Significant within audited area

2.2.3 In November 2014, IT & Transformation (IT&T), began undertaking risk assessments of IT systems across the Council. Stage 1 is ongoing and involves categorising systems as either "critical", "considered", or "nominal", based on the time following a system failure that there would be a severe business impact. This process is now overseen by the IGG. These risk assessments were forwarded to system owners within Services for final categorisation to be agreed. Critical systems are further classified by ICT as "business critical" or "department critical" depending on how widespread the impact of failure would be. There are currently 301 systems across the Council; risk assessments have been completed and issued to Services for 250 of them, 222 responses have been received.

2.2.4 The final stage is to review the governance of the 20 business critical systems, but this has not yet commenced. It will involve discussions with technical staff and system owners and reviewing completed Internal Audits / requesting Internal Audits be carried out on the systems concerned. The IT Security Architect has advised that the final stage can be run concurrently with the completion of the initial classification stage.

2.2.5 Target completion dates have not been set for the various stages of the system criticality review. This increases the risk that threats to major IT business systems will not be identified and controlled where necessary in a timely manner.

2.2.6 System criticality is assessed based on the impact (severe, moderate, minimal) of the system being unavailable across a number of areas including: financial; reputational; contractual; customer; inter-connections; number of users affected; and ability of the Council to continue business operations without the system. Reasons are provided for the system criticality identified across each of these areas on initial assessment by System Owners, the IT Security Architect and the system Account Manager. Previously the IT Manager reviewed and approved the risk assessments. This is now the responsibility of the Senior Information Risk Officer.

2.2.7 The risk assessments relating to eight business critical and two department critical systems were reviewed. One was not dated as approved for use whilst the others were approved in or before April 2015. Three of the assessments did not identify the system owners and two were not assessed across all impact areas.

Recommendation
Target deadlines should be formalised for the various stages of the IT system risk assessment review.

Risk assessments should be reassessed, updated and approved where necessary.

Service Response / Action
Part 1: Agreed.

Part 2: Agreed. Risk assessments for business critical systems will be scheduled for every 3 years and any risk assessments last carried out over 3 years ago will be prioritised for reassessment.

Implementation Date	Responsible Officer	Grading
March 2018	IT Security Architect	Significant within audited area

2.2.8 As part of the above review, since July 2017 Business Continuity Plans are being checked by the Emergency Planning Strategist to ensure they include reference to business critical systems and the Performance and Risk Manager is ensuring that relevant Services have assessed the risk associated with the systems. The Emergency Planning Strategist has confirmed a request has been issued to Plan owners to update Plans by 31 December 2017. This will include the requirement to include all critical systems in Plans as appropriate. A recommendation is included for tracking purposes.

Recommendation
Business Continuity Plans should be updated to include business critical systems where appropriate.

Service Response / Action
Agreed.

Implementation Date	Responsible Officer	Grading
December 2017	Emergency Planning Strategist	Significant within audited area

2.2.9 The IT Customer Service Manager is also required to reference the relevant systems as critical within Service Now, the Council's IT Service Management Tool, to facilitate management of the critical systems identified. Progress to date is recorded on a separate spreadsheet of critical systems maintained by the IT Security Architect. This indicates that eighteen of the 20 business critical systems have been updated on Service Now as critical.

2.2.10 A monthly update on the progress with the risk assessment process is required to be provided to the Information Governance Group. The 2016/17 quarter 4 Information Governance Management performance report included a deadline of 31 July 2017 to complete the first stage of IT investigations, identifying all systems and system owners and obtaining their interpretation of system criticality based on set criteria. The IT Security Architect is managing this process and maintains a 'Combined list' spreadsheet of all systems to track progress. The system owner has been identified for 250 systems and has yet to be identified for 51 systems. The spreadsheet identifies the classification of the business system and the progress preparing and agreeing the risk assessment with the Service (form created; form first populated; form repopulated and form agreed). 79 systems have not been classified to date.

2.2.11 Whilst the 'Combined list' spreadsheet identifies the business critical systems, it does not indicate if the risk assessments for these systems have been considered when preparing the Directorate risk registers.

Recommendation
Consideration should be given to using the list of risk assessments maintained by IT and updating this to capture when Directorate risk registers have been updated with business critical systems.

Service Response / Action
Agreed.

Implementation Date	Responsible Officer	Grading
January 2018	Performance and Risk Manager	Important within audited area

2.2.12 Guidance is not available on the process undertaken when preparing, reviewing and agreeing risk assessments. It was also noted that the definition of "critical"; "considered" and "nominal" is not included on the risk assessment form. The lack of written procedures and definitions of system classifications increases the risk that a system will be wrongly classified, resulting in risk and business continuity not being adequately considered for all business critical systems.

Recommendation
Written procedures should be prepared on how to carry out risk assessments.

Service Response / Action
Agreed

Implementation Date	Responsible Officer	Grading
April 2018	IT Security Architect	Significant within audited area

2.3 Business Continuity Planning

2.3.1 The Council's Business Continuity Policy requires Business Continuity Plans to be reviewed and tested annually. The IT&T Business Continuity Plan (BCP) was last updated in August 2017 to include details of recent incidents (website and power disruption) and was last tested in January 2017. It was noted that the Plan was incomplete, with appendix C: documentary requirements, being blank. This increases the risk that the necessary written procedures will be unavailable in the event of an incident that disrupts delivery of critical ICT functions.

Recommendation
The IT and Transformation Business Continuity Plan appendix C should be completed.

Service Response / Action
Agreed.

Implementation Date	Responsible Officer	Grading
January 2018	Incident & Problem Co-ordinator	Important within audited area

2.3.2 Within the IT&T BCP, the Service has detailed 17 suppliers that are heavily relied on to deliver support, which includes the data centre hosting provider, telephony and internet

service providers, and cyber security software suppliers. The Business Continuity Policy requires external suppliers to complete the Key Supplier Business Continuity Planning Assessment Questionnaire or confirm with Commercial and Procurement Services that they have checked the Business Continuity arrangements of the supplier and / or are content that alternative suppliers are available. A recommendation covering this issue was made and agreed in Internal Audit report AC1804 (Business Continuity Planning).

2.3.3 None of the suppliers had been requested to submit a Key Supplier Business Continuity Planning Assessment Questionnaire. The IT Security Architect has advised that this is mitigated by the fact that alternative suppliers are available for 14 of the suppliers and 1 key supplier is no longer required. A tender response from one key supplier confirmed business continuity arrangements. The lack of supplier business continuity arrangements for telephone system and support supplier is higher risk, since there are few readily available alternatives. In the event that the supplier were to cease trading, the IT Security Architect has advised that the subsidiary company would continue delivery of service. A draft business case has been prepared for a converged communication strategy which would reduce dependency on this system.

2.3.4 The IT Security Architect provided a copy of the tender questionnaire for providers of new IT systems. Included within the Information Security section were the requirements for suppliers to provide a Business Continuity Policy and evidence of disaster recovery built into the system.

2.4 Prevention

2.4.1 Data breaches and cyber-attacks can be prevented by keeping firewall, antivirus, application and operating software current. The majority of the Council's security products are managed under a single contract by a security partner. Patches are issued by product providers to keep software current.

2.4.2 The Council uses a next generation firewall. This is designed to provide threat prevention, visibility of network traffic based on applications, users, content and devices. Security rules are set to prevent access to known malicious websites or in line with Council policy e.g. in relation to use of social media sites.

2.4.3 The Council's email filtering software enables rules to be set on quarantining emails (such as in response to reports of a ransomware threat) and also removes known viruses from email attachments.

2.4.4 The IT Security Architect advised that the firewall automatically checks and applies updates for threat prevention once per day however high security updates are applied as soon as they are available. New anti-virus definitions are applied to the Council's anti-virus software automatically every 15 minutes. The Trend Manager console tracks deployment of anti-virus software. The Council's email filtering software is updated automatically to block new threats also. Email filtering updates occur every 30 or 60 minutes, depending on the nature of the antivirus or antispam filter being updated. Evidence of recent patches successfully applied in October was obtained.

2.4.5 The Incident and Problem Co-ordinator arranges with the Council's Data Centre provider for patches to be applied to business critical systems on an agreed schedule. Agreement with system owners is sought where appropriate.

2.4.6 The IT Security Architect monitors the status of Microsoft patching on a weekly basis. Microsoft patches are released on a Tuesday and are applied by the Council on Thursday in the same week. The System Centre Configuration Manager application is used to roll

out and monitor patches. Evidence of the 12 October 2017 patch being successfully applied was obtained.

2.4.7 The ransomware attack that affected the NHS in May 2017 did not affect the Council. This ransomware can be avoided by applying a patch. On checking the Council's PC estate on 15 May 2017, following the announcement of the incident in the NHS, the IT Security Architect established that 97% of Council PCs were found to have been updated for this patch.

2.4.8 The IT Security Architect and Infrastructure Architect are members of the Local Authorities Information Security Group, the Cyber Security Information Sharing Partnership and subscribes to a number of live feeds, providing updates every 15 minutes, that will detail any new cyber threats requiring action. The IT Security Architect is also updated of new security threats by the firewall provider. Application and Threat Content Release Notes and System Alerts.

2.4.9 The IT Infrastructure Architect advised that the Council employs a security scanning appliance, that has been set to scan the external and internal network environment on a monthly basis, and alert IT staff to potential vulnerabilities, as part of the contract with the ITHC partner.

2.4.10 Business critical systems are backed up in full on a weekly basis and incrementally on a daily basis by the Council's Data Centre provider, with 30 days of back up files held locally in Aberdeen and a 90 day offsite retention held in the disaster recovery datacentre in Dundee.

2.4.11 Five business critical systems were selected and the back-up schedule requested form from the Infrastructure Architect. Back-ups were scheduled daily for each of these business critical systems. ICT receive daily emails detailing the status of the back-ups for all systems other than Benefits, which go directly to the Benefits team.

2.5 PSN Compliance

2.5.1 The Public Services Network (PSN) compliance is a means of demonstrating the Council's IT security arrangements, policies and controls are sufficiently rigorous to enable interaction with the Network and those connected to it. The PSN offers a secure means for the Council to access shared services with other PSN compliant organisations such as the DWP, for the purposes of accessing benefits data.

2.5.2 In order to obtain the necessary PSN compliance certificate from the Cabinet Office, the Council must demonstrate it can comply with PSN requirements, by undertaking an annual IT Health Check (ITHC). This involves carrying out external penetration testing on the Council's perimeter network infrastructure, to check for security misconfiguration and other weaknesses that could lead to system compromise. Internal vulnerability assessment is also carried out to ensure security is not affected by internal system interactions.

2.5.3 The Council's ITHC partner is a National Cyber Security Centre approved CHECK company as required by the Cabinet Office. An external IT health check was carried out in August 2017. This involved an assessment of externally available infrastructure to check for security misconfiguration and other vulnerabilities; remote access solution testing; and a review of the Outlook webmail application. The Council was commended for their attitude towards IT security, found to have many best practice controls in place to prevent malicious attack and there were few services directly exposed to the internet, with those that were providing no direct means of compromise. One high vulnerability

weakness was identified (and this is being addressed). The Council had not been advised of the outcome of the assessment by the Cabinet Office as at 27 November 2017.

2.5.4 The ITHC partner also carried out an internal IT health check, as required by the Cabinet Office, in July 2017. This involved: internal network penetration testing; build reviews of workstations / servers; a mobile device review; a wireless network assessment; a firewall ruleset review; and a remote access configuration review. The overall security of the Council internal network was found to be good, with adherence to a number of best practices evident. However a number of vulnerabilities were identified, including user password policies.

2.5.5 The recommendations made by the ITHC partner are tracked in the Remedial Action Plan maintained by the IT Security Architect, reported to the Cabinet Office. The IT Infrastructure Architect advised the recommendations are also managed within the onsite security reporting appliance that feeds into the ITHC partners reporting portal.

2.6 PCI DSS Compliance

2.6.1 PCI DSS (Payment Card Industry Data Security Standards) is a worldwide standard that was set up by the payment card industry to agree on minimum levels of security when processing and holding cardholder data. Compliance with the twelve PCI DSS requirements reduces the risk of fraudulent transactions and helps to shift liability for fraud from the merchant to the card issuer. The requirements cover all aspects of card payment transactions including software applications, telephony and communications networks, data storage and business processes.

2.6.2 As a 'merchant' processing transactions, Aberdeen City Council requires an 'acquirer' (World Pay Streamline) to securely authenticate transactions and process payments to the Council's bank account. Acquirers may be fined by card issuing schemes such as Visa and MasterCard if their merchant customers are not compliant with PCI DSS requirements and there is a data breach or evidence of fraud. Acquirers will therefore refuse service to merchants who do not show evidence of compliance. This loss of service would mean that the Council would no longer be able to take payments by card. The Council may also be liable to a fine from the Information Commissioners Office in the event of a loss of personal information, and would risk reputational damage.

2.6.3 Of the twelve PCI DSS Requirements, eight relate to network and computer system security and monitoring.

2.6.4 The Technology Team run scans of the external facing systems on a quarterly basis, for submission to the acquirer, to demonstrate compliance with PCI standards. The results are held in the Council's hosted portal, a platform that is provided by the ITHC partner. The Council was PCI DSS compliant for the quarter ending 17 November 2017 and has until the 17 February 2018 to run and submit a vulnerability scan to the acquirer, to demonstrate compliance for the current quarter.

2.7 Disaster Recovery

2.7.1 Business critical systems are backed up in full on a weekly basis and incrementally on a daily basis by the Council's Data Centre provider, with 30 days of back up files held locally in Aberdeen and a 90 day offsite retention held in the disaster recovery datacentre in Dundee.

2.7.2 Five business critical systems were selected and the back-up schedule requested form from the Infrastructure Architect. Back-ups were scheduled daily for each of these business critical systems. ICT receive daily emails detailing the status of the back-ups for all systems other than Benefits, which go directly to the Benefits team.

2.7.3 The Incident and Problem Co-ordinator carries out disaster recovery testing in conjunction with the Council's data centre provider on agreed dates. A schedule of systems to be tested in the next 4 years has been set up with testing dates included where known. There are presently 11 business critical systems absent from the disaster recovery schedule.

2.7.4 Written procedures are not currently in place describing the disaster recovery testing process managed by ICT, including how systems are selected for testing, the frequency of testing and how resulting actions are monitored.

Recommendation
Arrangements should be made to schedule disaster recovery testing for all business critical systems.

Written procedures should be prepared describing the disaster recovery process, including the basis of system selection for testing, the frequency with which systems are tested and the monitoring of resulting actions.

Service Response / Action
Agreed.

Implementation Date	Responsible Officer	Grading
January 2018	Incident & Problem Co-ordinator	Significant within audited area

2.7.5 Three business critical systems had dates for disaster recovery testing in 2017 and only the case management system for Social Work had been scheduled for completion as at 30 September 2017. Testing took place on 6 April 2017 and the Council's Data Centre provider have prepared a first draft report dated 11 May 2017 showing the results of testing. The report provided to Internal Audit was redacted by the IT Security Architect due to it containing sensitive information and was not signed and dated as approved by the Council's Data Centre provider. The lack of approval increases the risk that the report is incomplete and disaster recovery failings have yet to be highlighted and resolved. The Child Protection Register was tested on 4 October 2017 by the Council's Data Centre provider. There were no remedial actions resulting from the test. The remaining business critical systems to be tested in 2017, the schedule of which has been agreed with the service, are Total Mobile (28/11/2017) and Tranman (12/12/2017). Approval for the remaining systems is still out for consultation with the service.

Recommendation
A final approved disaster recovery report should be obtained for CareFirst.

Service Response / Action
Agreed.

Implementation Date	Responsible Officer	Grading
January 2018	Incident & Problem Co-ordinator	Significant within audited area

2.7.6 The Council in conjunction with the data centre provider, is working towards implementation of yearly disaster recovery exercises to simulate the loss of the primary data centre in Aberdeen. This would be with a view to ensuring all critical systems are made available in the event of a major data centre disaster through use of the alternative data centre in Dundee. The final pre-test to conclude the ability to conduct this exercise on an annual basis was carried out on the 12 November 2017. Results are yet to be provided to the Council by the data centre provider.

2.7.7 A number of critical systems, such the Housing Rents system; the Benefits System and the Case Management System for Social Work, use Oracle based platforms. Aberdeen City council is refreshing its oracle platforms with new hardware. This will involve replacing physical servers which will be consolidated to virtual 'unix zones'. The disaster recovery test schedule captures the details of the current and replacement servers, including whether the current server has been cloned for monitoring purposes. It does not however include the planned and actual replacement dates.

Recommendation
The Service should consider updating the disaster recovery test schedule to include planned and actual server replacement dates for monitoring purposes.

Service Response / Action
Agreed

Implementation Date	Responsible Officer	Grading
January 2018	Incident & Problem Co-ordinator	Important within audited area

2.8 Incident Management

2.8.1 In the event of an incident, which requires activation of the Business Continuity Plan, a Post Incident Report should be prepared, as required by the Business Continuity Policy. This should be shared appropriately and will be used to update the existing Business Continuity Plan as required.

2.8.2 On the evening of Saturday 28 January 2017, the homepage of the Council's website was replaced with an external image. The monitoring systems in place notified IT staff within 8 minutes of the incident, an incident response team was established and normal web services were resumed to the public within 3 hours. Investigations into the incident found the root cause was a vulnerability within the file upload feature which was previously used by members of the public to upload photos of events across Aberdeen. This feature has since been disabled. No customer data is held within the website infrastructure, and according to the incident report, there is no evidence to suggest that the hackers managed to gain access to the internal network where customer data is held, therefore no customer data was compromised.

2.8.3 A report was presented to the Audit, Risk and Scrutiny Committee in February 2017 which informed elected members of the incident and included the full incident report with high level actions to be addressed. The incident highlighted that the call-out procedure required to be reviewed, as there was no formal escalation process for the on-call person to respond to a major incident such as this. The incident process has been reviewed to take account of potential cybercrimes and an escalation process to Police Scotland is now in place.

2.8.4 As required by the Business Continuity, the incident details reported included: an event timeline; effect on Council functions; an assessment of the response; lessons learned; recommendations and action plan.

2.8.5 On 22 July 2017 the Uninterrupted Power Supplies (UPS) failed in the Marischal College Comms room, causing disruption to the Marischal core switch infrastructure. A copy of the draft incident report was obtained. There was no access to any IT Services, including telephony from Marischal College. Data Centre Services automatically rerouted via the disaster recovery resilient link. No data was lost as a result of the incident. The Council's security perimeter systems are ~~is~~ hosted in other core locations that were not impacted by the power outage.

2.8.6 The IT&T Plan has been updated to document both these incidents in line with the Business Continuity Policy.

AUDITORS: D Hughes
A Johnston
C Pirie

Appendix 1 – Grading of Recommendations

GRADE	DEFINITION
Major at a Corporate Level	The absence of, or failure to comply with, an appropriate internal control which could result in, for example, a material financial loss, or loss of reputation, to the Council.
Major at a Service Level	The absence of, or failure to comply with, an appropriate internal control which could result in, for example, a material financial loss to the Service/area audited. Financial Regulations have been consistently breached.
Significant within audited area	Addressing this issue will enhance internal controls. An element of control is missing or only partial in nature. The existence of the weakness identified has an impact on a system's adequacy and effectiveness. Financial Regulations have been breached.
Important within audited area	Although the element of internal control is satisfactory, a control weakness was identified, the existence of the weakness, taken independently or with other findings does not impair the overall system of internal control.