CAIRNGORMS NATIONAL PARK AUTHORITY AUDIT & RISK COMMITTEE

FOR DISCUSSION

Title: **IT RISK**

Prepared by: **DANIE RALPH, FINANCE MANAGER**

Purpose

This paper is for the information of the Committee and presents an overview of IT risks noted in the Risk Register and what is currently being done, and planned to be done, to mitigate ICT risk to the Authority and provide a road map for future IT development.

The paper also represents a detailed analysis around specific strategic risks and as such follows up on previous internal audit recommendations that such detailed analyses of risk augments the Committee's approach to and leadership of risk management.

Recommendations

The Audit & Risk Committee is asked to:

a) Consider the information in the paper

Executive Summary

1. The Authority has recorded 4 specific IT service risks in the Risk Register, most recently presented to the Board at its meeting in December 2018 https://cairngorms.co.uk/resource/docs/boardpapers/07122018/181207CNPABdPaper9Annex3StrategicRiskRegisterV1.0.pdf :

    a) A17 - Technical: increasing ICT dependency for effective and efficient operations is not adequately backed up by **ICT systems support**;
    b) A18 - Technical: **cyber security** is inadequate to address risk of cyber-attack on systems;
    c) A9.2 - Resourcing: CNPA IT services are not sufficiently **robust/secure/or well enough** specified to support effective and efficient service delivery;
    d) A13 Resourcing: lead body role for multiple large scale externally funded projects is unable to be supported through available **cash flow and ICT systems**.

2. The essential component in each risk is bolded in para 1 and each will be considered as part of an emerging IT approach within the Authority's IT function, which in turn will be developed into a fuller IT strategy. For convenience this is referred to by the shorthand name of **SASI** which is a convenient catch all for our IT values and vision:

a) **S**table - the ICT platform is available during core working hours with planned outages kept to a minimum;
b) **A**ccessible – that staff are able to access data remotely to allow flexibility in working practices, such as working from home, and specific user needs are listened to;
c) **S**ecure - that the data maintained by the authority is not only adequately protected per Cyber Security PLUS certification but is safe; and that staff using the Authority's ICT systems are protected from unsafe, malicious or undesirable content;
d) **I**nnovative - as a general rule we follow Scottish governments approach to change, as outlined in The Improvement Guide, start small and if it doesn't work try something else. We see the process as iterative and on-going with innovation meaning, in our IT context, leading to improvement and supporting efficiency and effectiveness in working practices and service delivery.

Introduction

3. IT impacts on virtually everything the Authority does: in generating information, in decision making, financial reporting and monitoring, achieving operational effectiveness and efficiency, communications, resource management etc.. In the future, with developments in IT continually evolving and the Authority's ways of working changing and adapting to new technologies and practices, the dependency on IT will continue to increase and the reliability, integrity and availability of applications and data, rather than "the IT system" will become more important than ever, for users at all levels.

4. This paper will therefore provide members of the Audit and Risk committee an overview of IT risks, their interdependence, complexity, likely increasing cost and how what we are doing and intend to do to mitigate risk.

Stable and Accessible (risks A17, A9.2, A13)

5. As working methods are increasingly digital, it is important that access is available, and secure, not only during working hours but at all times so it is appropriate to look at these 2 components together

6. Like all organisations the Authority is dependent on reliable ICT to allow its staff to work effectively and efficiently. And like all organisations of a similar size there is an absolute limit to the service IT can provide as, with increased reliance on shared services and "cloud" solutions, any failure in access to the internet is outwith the control of the Authority so we are reliant on external providers to mitigate service disruption. That said the rest of this section considers what the Authority's IT function can do and is doing to provide stability, and effective and efficient operations. However, it has to be realised that as "cloud" solutions become more prevalent and popular, and the preferred direction of travel of Scottish Government, there is a reduction in control of access to applications and software available to the Authority and a growing risk on the dependence of external service providers. While this is not a risk yet highlighted in the Risk Register, if "cloud" solutions were to become the norm for the authority there is little more than can be done than note the risk of the

lack of internet provision, for whatever reason, as any mitigating solution is likely to be unaffordable.

7. The in-house IT function is currently one full time manager supported by an IT apprentice who started in August 2018. Additional technical support and advice is available from the Loch Lomond & Trossachs IT department, who also provide the data backup function as a hybrid "cloud" solution, and the "help desk" functions to cover IT staff holidays or absences.

8. External consultants are only used on the introduction of new or updated software/hardware where it is more cost effective to do so: for instance a new storage system will be in place before the end of February. The hardware will be delivered to HQ and configured remotely by the provider who has the expertise to carry this out quickly.

9. There is close cooperation with Loch Lomond and quarterly off-site meetings are now planned with their team, in addition to formal monthly telephone technical catch ups between the IT line staff. This is over and above frequent liaison day to day operations.

10. Over the last 2 years "unplanned" downtime of the system is negligible. "Planned" downtime is usually to facilitate implementation of urgent patches, email server restarts or the installation of new or replacement hardware within the server room. Usually major hardware upgrades are scheduled for holidays or weekends to minimise disruption. Staff working at home can access emails at any time, and can have access to the Server with VM software. Accessibility issues using the VM have been significantly reduced with residual issues often caused by connectivity issues at the user end rather than the Authority's systems, so are outwith our control environment.

11. The IT department not only runs the infrastructure but is also involved with mobile device sourcing and management, telephony and copier/printing management. All the Authority's telephony needs are now met by the MS Lync system which means that costs have reduced as a dedicated line between HQ and Ballater is no longer needed. This saves £20,000 per year, and BT call charges have been replaced by usage charges by the Lync provider.

Secure (risks A18, A9.2)

12. The Authority takes the security of its network, ICT assets and data seriously and has a number of protocols and policies in place to prevent and mitigate risk. Security is much wider than purely cyber security, which is of growing concern generally, and covers not only the physical security of individual items of hardware but of the whole ICT infrastructure and estate. The "estate" comprises the "server", laptops, tablets and desktop devices, printers and multifunction devices and increasingly any other web enabled devices.

13. SG have recently invested £2.7m in what is known as the "Internet of Things" (IoT). The IoT is the interconnection of computing devices embedded in everyday objects enabling them to send and receive data. The IoTScotland will provide a wireless

network for applications and services to collect data from devices and send that data without the need for 3G/4G or Wi-Fi, supporting businesses "to develop new and innovative applications changing the way they work". In our case this could mean remotely accessing data on people counters or camera traps.

14. As the range of devices capable of being connected increases so does the risk of security breach, and why a great deal of effort is placed not just on the physical security of assets but on cyber security and the prevention of unauthorised access to the system.

15. The protocols and policies in use range from the tagging of high value assets, restricting access to the server room at all times, restricting access to the system to only identified staff users, to running specific countermeasures in the background of server and system operations (firewalls, email scanning etc) to forwarding on email warnings on specific threats – phishing or other fraud. Third party suppliers, for example banks, also carry regular updates and warnings about threats which must be observed by staff.

16. Authorised access to the "system" is therefore on 2 levels (1) access to the infrastructure /servers is restricted to IT staff only, or on occasions with specific permissions to Loch Lomond staff or third parties when new kit or software is added, and (2) at staff member level, where access to the system, on any hardware device, is by a recognised user name and password, which is changed regularly. Therefore only designated and recognised individuals can access the system and data.

17. Unauthorised access to the "system" is more challenging and GCHQ reckon that any organisation can only protect itself to about 80% of the threats, which of course grow in frequency and sophistication. To an extent we will always be behind the curve in addressing cyber security but can mitigate the threat not just by appropriate processes and certification but by vigilance (phishing, CEO and invoice frauds) to adopting best practice and recognising that all staff that they have a part to play.

18. The Authority has recently gained the Cyber Essentials Security PLUS certification, which is a test of the Authority's IT systems by an external Certifying Body.

19. A primary objective of the UK Government's National Cyber Security Strategy is to make the UK a safer place online and to achieve this the Cyber Essentials scheme was introduced in 2014. It is a cost-effective assurance mechanism developed by CREST (**C**ybe**R** **ES**sen**T**ials!) for the National Cyber Security Centre (NCSC), the information security arm of GCHQ and focuses on 5 essential mitigation strategies:

    a) boundary firewalls and internet gateways
    b) secure configuration
    c) access control
    d) malware protection
    e) patch management

Cyber Essentials Security Plus certification looks specifically at the following:

a) can malicious files enter the organisation from the internet either through web traffic of email messages?
b) how effective the anti-virus and malware solutions are if malicious content enters the Authority, and
c) should the Authority's protection measure fail how likely is it that it will be compromised due to failings in patching the Authority's workstations. (Technology subject to cyber attacks includes desktop PCs, laptops, tablets, smartphones and internet connected services including email, web and application servers.)

20. As mentioned above concentrating on the 5 main controls will stop 80% of cyber-attacks. That still means that 1 in 5 attacks will/could succeed.

21. The assurance to be gained from the certification is that the Authority's data is adequately protected and demonstrates the cyber security is being taken seriously.

22. The Cyber Essentials certification is now embedded in IT protocols and the next round of certification is scheduled for December 2019.

Innovation (risk A17, A18, A9.2, A13)

23. Innovation can mean many things and is often misunderstood. The word does not sit well with the Authority's ICT needs as innovating can be challenging in a small NDPB with limited financial resources. For instance, we cannot by changing work practices save a great deal of money, and the applications we use in operations are modest – iDox for planning and MS Office for all other needs, so we may not be able to achieve obvious or significant productivity gains. We may, however, be able to do things better, not necessarily quicker or cheaper and we will always be reacting to change because ICT and software development is dynamic.

24. One area that is changing is how we buy software, and how we pay for it. Overall in the Government sector the trend is for Capital costs to reduce with a concomitant increase in costs charged to Resource, putting further pressure on static or reducing, grant-in-aid allocations. The Government's strategy for digital platforms is to move increasingly toward the "cloud", which means that the "old" physical model of buying on DVDs and carrying software on local servers is disappearing. Buying a "perpetual license" with an up -front cost is being replaced by a new model for either an annual or monthly subscription fee, usually per user, and with higher prices for different levels of features. This not only changes the type of cost incurred (resource rather than capital) but can see costs increase if the mix of user licences is not carefully managed.

25. There is a potential new strategic risk to recognise in this regard either now or in the next few years, where the change in financing IT services and the switch from capital to revenue provision places an unmanageable pressure on the Authority's budget capacity.

26. Vendors also appear keen to move users to "cloud" solution which means the SaaS model. SaaS is "Software as a Service" where software is distributed and accessed over the internet. Software is bought on a subscription basis, updates are applied automatically without user intervention. This is potentially a risk as we do not have the capacity to "sandbox" (test updates before they are implemented) and / or implement critical updates only. Equally, there is also a risk mitigation in this service model as there is no longer a need for organisations to rely on locally implemented software upgrades being implemented.

27. There are also infrastructure changes implied from SaaS as no hardware is required (potentially a saving too) as the software is not hosted locally but in the cloud and is accessed via a web browser. And as systems are virtualised this is more attractive.

28. So, increasingly we are buying, or being offered, SaaS solutions. We are not being innovative as we are simply buying what is being made available. It is a complex area with some vendors still offering "on-premises" variations. We can manage the costs by identifying what we need, and only buying into that level; working closely with Loch Lomond NPA and achieve discounts by jointly procuring SaaS and by managing the timing of migration of current applications, running them as long as we can under current license and agreements, without affecting effectiveness, efficiency, and security.

29. In the medium term we can also look at whether open source software offers real benefits compared to current packages. Open source software is software which is designed to be publically accessible. It doesn't mean that the software is free, or any better than proprietary, but could be cheaper and comes with its own set of risks.

30. If we accept the IT infrastructure to be stable, accessible and secure, we can still make improvements and innovate, likely to be small and incremental, hopefully cost effective over all aspects of ICT and workings. A few examples of what we are currently doing are:

    a) Continuing to implement managed digital change – for example the current CRM and Document Management Systems which will support changes and develop effectiveness in working practices;
    b) the IT manager is attending the Smarter Working Scotland Conference looking at smarter working, paperless projects, digital reimagining and networking to see how other organisations are developing their ICT strategies, and where we can learn from them;
    c) the IT manager is attending the Improvement Scotland workshop to learn a new approach to introducing change;
    d) attending the SG Digital Champions programme;
    e) trying walk in IT clinics to bring the users of IT closer to the IT team;
    f) using the BDO Performance and Strategic Development advisory report to guide future developments;
    g) improvements, meaning the reduction in cost, carbon footprint and consumables have already been achieved by introducing new multi-function devices for printing, copying and scanning and reducing the number of printers in the office. Monthly reports are now prepared showing the number of pages printed, and the cost in terms of trees, carbon emissions and the equivalent light bulb usage.

Any opportunity to reduce operating costs with to compromising service will be looked at;

h) a specific IT risk register is being developed, concentrating on operational IT issues and also managing opportunities as well as risks;
i) looking at Scottish Wide Area Network (SWAN) again;
j) looking at collaboration with other National Parks or NDPBs;
k) education and developing closer working relationships between all staff and the IT team: while we can do a great deal to ensure the integrity and reliability of the infrastructure, cyber security etc., the biggest single threat to our IT systems comes from the human element, staff. It takes only one person to open a malware email and control systems can only provide support alongside effectively trained users.

31. To keep IT secure, using the current apps, and maintain a stable and accessible system, to further develop the IT function, it is going to cost more in cash resource terms. This not just due to inflationary pressures but because the direction of travel – the cloud – and that is will in part be dictated as part of Scottish Governments IT strategy and the Authority, as a small NDPB, will have to balance what is asked of us with what resources are made available, and work smarter.

Next Steps

32. We will continue to identify and monitor IT risks and management and mitigate them using appropriate controls. The controls do not operate in isolation and are dependent on many factors. They can be compromised due to weak links, subject to error and management override, and range from the simple to highly technical, and increasingly complex. We can manage them at the governance level and at the application and infrastructure level: both have to be considered and ranked into what are purely operational IT risks and those that impact the Authority's delivery of its Plans.

Danie Ralph
12 February 2019
danielralph@cairngorms.co.uk