Agenda Item 11   Executive Board Meeting   Memo No 24/15
9 September 2015

Status: OFFICIAL

DISASTER RECOVERY

Purpose

1.   To advise the EB of the current position regarding ICT disaster recovery and to seek agreement on the issue of testing and continued support for the development program in this area.

Background

2.   In 2011 IS embarked on the Risk Mitigation Strategy to address a range of serious concerns regarding the stability & availability of the ICT systems upon which the FC depends. Work to implement the strategy has continued over the subsequent period despite the resource constraints imposed by SR10.

3.   One of the major areas addressed by the Risk Mitigation Strategy is that of Disaster Recovery (DR) where significant improvement has been achieved. IS currently estimate that, in the event of fire or flood at Silvan House, it would take 5 days to recover the major systems but there may be up to an additional 5 days of data loss. Once all the outstanding work on the Risk Mitigation Strategy is complete IS will be able to recover all the Commissions ICT systems in 3 working days and demonstrate / test this on a regular basis.

4.   At present Internal Audit are only able to provide Limited Assurance on the disaster recovery position as no testing has yet taken place.

Current Position

5.   A progress update on the Risk Mitigation Strategy is attached in Annex A.

6.   A diagrammatic overview of the work required to ensure full DR is set out in Annex B.

7.   A summary of the issues regarding DR testing is attached in Annex C.

Testing

8. DR Testing on a regular basis is essential. However, to undertake a DR test now would be very disruptive to the business and result in delay to the outstanding work. Director IS does not recommend a full test of the DR facility at this time due to the complexity and business disruption associated with systems recovery whilst also providing a live service. See Annex C for details.

Continued Development of DR

9. Annexs A & B show the progress to date and the remaining work necessary to achieve a fully tested DR environment, the major remaining items are:
    - Completion of the windows 7 roll out by July 2016 (£1.2m)
    - Upgrade of Microsoft Exchange e-mail by July 2016 (£250k)
    - Upgrade of Serengeti document mgt. system by Jan 2016 (£14k)
    - Revised System Back-up procedures by April 2016
    - Upgrade of FC Intranet by Dec 2017 (£120k)
    - Replacement of Contivity data network for small sites by April 2018 (£100k)

10. It should be noted that whilst supporting the goal of improved disaster recovery this remaining work also forms part of the necessary infrastructure maintenance to ensure business as usual continuity.

Resource Implications

11. No additional resource above the current IS organisation will be required if the current strategy as outlined in Annex A continues over the coming 3-4 years.

12. However, if it is deemed appropriate to accelerate the DR testing then additional resource of approx. 300 person days and supporting funding will be required.

Risk Assessment

13. The business risk associated with a fire or flood in Silvan House has already been significantly reduced but there remains 3-4 years work to do before the DR programme is complete and a full DR test undertaken.

14. However, if the business insists that a full DR test must be undertaken now, then there is a very high risk of delay to the existing IS programme of work along with a high risk of significant business disruption across the organisation and particularly to Forest Research.

15. Whilst Silvan House Divisions and countries/FR have Business Continuity Plans in accordance with the process agreed, all of these rely on an IT Disaster Recovery plan which is not yet complete.

Communications Issues

16.   N/a

Recommendation(s)

17.   The EB is asked to:
- Discuss the issues set put in this paper.
- Agree to continue to support the Risk mitigation programme as outlined in Annex A.
- Tolerate the 'Limited Assurance' audit position until it is appropriate to undertake a full Disaster Recovery test.
- Agree to the continued programme of work until such time as the countries and FR have their own arrangements in place for ICT provision.

David Felstead
Information Services
September 2015

ICT Infrastructure Risk Mitigation
(August 2015 update)

Background

Prior to 2011 the Forestry Commissions computer systems had grown in an unstructured manner with a series of lowest cost one-off solutions to individual problems. Consequently, the business of the Forestry Commission had become dependant on an ICT infrastructure that was:

- Ageing and increasingly unreliable;
- Excessively complex;
- Difficult to manage & maintain;
- Highly dependent on individual staff members;
- Increasingly difficult to back-up;
- Incapable of providing any Disaster Recovery.

This situation represented an unacceptable risk to the business operations of the Forestry Commission and had to be addressed.

The Strategy

In response Information Services (IS) developed a strategy for the development of the ICT infrastructure that involved the creation three distinct computing environments for: production systems; pre-production integration testing; systems development and test. With the pre-production environment located at a second site to provide a disaster recovery capability.

This strategy demanded significant investment in both equipment and staff over a period of years, so an implementation plan was developed with the major stages of that plan being:

Stage 0 – Planning & procurement
Stage 1 – Back-up assurance
Stage 2 – Installation & configuration of the new infrastructure
Stage 3 – Application migration to the new infrastructure
Stage 4 – Provision of disaster recovery facility

Progress to date (August 2015)

Infrastructure risk mitigation activities completed to date (June 2015) are:

- Power & air conditioning improvements for the Silvan House Computer Hall have been implemented.

- A new disaster recovery facility at NRS (Roslin) has been built and commissioned.

- Installation & configuration of new systems hardware & operating environments is complete.

- Un-interruptible power supplies (UPS) for the production systems have been implemented.

- A new systems back-up & restore solution has been implemented.

- IT hardware to support Disaster Recovery is installed & operational at the Roslin facility.

- Improved data network connections to support disaster recovery at NRS have been implemented.

- Implementation of hot failover for the telephone system.

- Migration of business applications to the new hardware is underway. systems already migrated include:

    · Assyst
    · GLOS
    · Drive
    · e-financials
    · Forester
    · Plant and seed supply
    · Wildlife management

- Work to migrate Serengeti and Exchange (e-mail) is currently in progress.

- Full recovery of e-financials has been successfully demonstrated.

This work has already resulted in significant improvements to the reliability and performance of ICT systems.   In addition there has been a substantial improvement to our ability to withstand a major incident at Silvan House.

Further work

Further work to complete the risk mitigation plan includes:

- Migration of the remaining business applications, specifically; Intranet, Sales Recording Package (SRP) and a number of small non-business critical systems.
- Re-configuration of network links into Silvan House to provide resilience in the event of a single line failure.
- Re-configuration of network links into NRS for the PSN and public internet to support small sites.
- Development and documentation of detailed disaster recovery procedures.
- Disaster Recovery testing against different disaster scenarios to test documentation and train staff.

Summary

At the start of this programme a significant event; fire, flood, etc. at Silvan House could have been a catastrophe for the Forestry Commission with the potential loss of key IT systems across the whole business for many months.

The risk mitigation work completed so far has resulted in a substantial improvement in the ability of the Commission to withstand a major incident at Silvan House. IS currently estimate that in the worst case of a fire or flood in the Silvan House Computer Hall the major business systems can be recovered and operational at NRS within 5 days of the fire although there may be some additional loss of data of up to 5 business days.

Whilst the current position is a significant improvement, there is still work to be done and when this is complete IS will be able to demonstrate restoration of all the major business systems with no loss of data within three days of a fire, flood etc. at Silvan House.

David Felstead
Information Services
September 2015

**ICT Risk Mitigation
Project Dependency Map**

```
┌─────────────────────────────────────────┐
│  Windows 7 / Office 2010 Roll-out        │
│                                          │
│         (est. 600+ person days)          │
└─────────────────────────────────────────┘

┌──────────────────────┐        ┌─────────────────────────────────┐
│ Upgrade Blackberry   │        │  Upgrade Exchange to 2010       │
│ Enterprise Server to │───────▶│                                 │
│ V5                   │        │     (est. 300+ person days)     │
│ (20 person days)     │        └─────────────────────────────────┘
└──────────────────────┘

┌──────────────────────┐
│ Develop Back-up      │
│ procedures for VTL   │
│                      │
│ (est. 40 person days)│
└──────────────────────┘

┌──────────────────────┐
│ Upgrade Serengeti to │
│ V6                   │
│                      │
│ (est. 40 person days)│
└──────────────────────┘

┌──────────────────────┐
│ Migrate or replace   │
│ oracle portal as e-  │
│ connect platform     │
│ (unknown person days)│
└──────────────────────┘

┌──────────────────────┐
│ Duplicate Netilla VPN│
│ at NRS               │
│                      │
│ (est. 20 person days)│
└──────────────────────┘

┌──────────────────────┐        ┌──────────────────────┐
│ Replace Contivity    │        │ DR process           │
│ 10:10 at small sites │───────▶│ development &        │
│                      │        │ documentation        │
│ (est 100 person days)│        │ (est, 300+ person days)│
└──────────────────────┘        └──────────────────────┘
                                          │
                                          ▼
                                ╭──────────────────────╮
                                │ Full Disaster        │
                                │ Recovery Testing in  │
                                │ Place                │
                                ╰──────────────────────╯
```

Annex C

Disaster Recovery Testing – summary of current position

Whilst much of the work to achieve a fully operational disaster recovery facility at Roslin is complete, there is still work to be done before this can be fully tested in parallel with the day-to-day operations of the Forestry Commission. In fact it's significantly more difficult and time consuming to undertake the test than to perform a real-life recovery.

The main testing challenge is to recover the existing systems onto a duplicated environment and test the interaction between these systems without creating network address duplication and traffic collision between the live systems and the recovered copies of these systems at the DR site. There are three possible resolutions to this problem:
   i)   Take the live systems off-line for the duration of the DR recovery & test.
   ii)   Isolate the DR site from the live network and test locally at Roslin
   iii) Implement a technical solution to allow the co-existence of live systems and their DR duplicates on the same network.

Of these: (i) is most represents a true recovery scenario, but would result in continuous unavailability of all FC systems for a period of at least one week- this is clearly unacceptable. (iii) is the preferred option in the longer term but requires significant further work and will take at least three years to fully design and implement given the current resources and priorities.

This leaves option (ii) as the only practical short term option for testing the disaster recovery facility and would consist of the following activities:
   1.   Commandeer the meeting rooms, library and any available offices at NRS.
   2.   Set-up temporary desks and run cabling into the NRS Library.
   3.   Reassign IS technical staff to the recovery test and ask them to work from NRS for the duration of the test.
   4.   Disconnect the pre-production/DR equipment at NRS from the main FC network.
   5.   Undertake full systems restore from back-up of all the major systems onto the isolated network. (3 teams of 3 people working shifts over 4 days)
   6.   Ask selected business staff to work from NRS to test the systems & data recovery.

Whilst possible, this testing would result considerable business disruption, such as:
   -   Significant reduction in day-to-day IT Service Provision to all the FC for approx. 10 days
   -   Disruption and delay to IS project delivery
   -   Un-availability of meeting rooms & other shared areas (eg library) at NRS.
   -   Reduced network capacity & performance for staff at NRS

Conclusion & recommendation

As IS Director I am confident that the work undertaken over the past 3 years has significantly reduced the business risk associated with fire/flood etc. at Silvan House and that in the event of a disaster the FC's critical business systems can be recovered over a period of 5 days. However, I do not recommended a full test of the DR facility at this time due to the complexity and business disruption associated with systems recovery whilst also providing a live service.

I do recommend that IS continue to pursue the current programme to:
   a)   Upgrade MS Exchange; Document management & Intranet systems.
   b)   Re-configure the Data Network to support small sites & remote working at the DR site.
   c)   Implement the technical measures to enable parallel running of the live service and the DR site.
   d)   Undertake full DR testing once the above has been completed (approx. 3 years).

David Felstead
May 2015