IT Disaster Recovery Update

Audit Plan Ref: 20-21 FT19

June 2022

Disaster Recovery (DR) - Definitions

Disaster

A sudden, catastrophic event causing damage or loss to the IT infrastructure that compromises an organisation's ability to provide critical services. Eg a cyber attack, fire or natural disaster.

Disaster Recovery

The method by which the IT infrastructure is recovered after a *disaster* type event. Components will include technology – such as stand by sites and backups, and procedures such as recovery plans and regular tests.

Why is it important?

Disruption risks harm to residents, reputational damage, dissatisfied customers and financial loss. The longer the recovery time, the greater the adverse impact. A disaster recovery plan should enable rapid recovery from disruptions, regardless of the cause.

And what it isn't

A DR plan is complimented by a robust Business Continuity Plan (BCP). It is the BCP plan which describes how the business will continue to function whilst IT systems are unavailable.

TS Disaster Recovery - Background

ECCs previous IT DR Audit in 2016/17 – No assurance

- TS proposed that DR capability was to be delivered as part of the migration of locally hosted IT services to the Microsoft Azure Cloud.
- The cloud architecture was designed with DR in mind from the ground up. It spans two geographically dispersed regions each capable of running the service. Data is replicated between the two.
- DR policy written and approved
- The Cloud Migration Programme is still in progress – over 60% of on premises services have now been migrated, DR requirements revisited for each.
- TS have recently recruited a DR & Resilience Manager with responsibility for disaster recovery to lead the operation and testing of this new capability.

Disaster Recovery Audit – December 2021

An audit opinion of *Limited Assurance*

- There has been an improvement in the control environment since our prior audit.

- The previous IT Disaster Recovery audit in 2016/17 received an overall opinion of *No Assurance* with 5 Critical recommendations.

- Several control weaknesses remain and whilst this audit has not raised any new Critical recommendations, a total of 3 Major and 3 Moderate recommendations have been made.

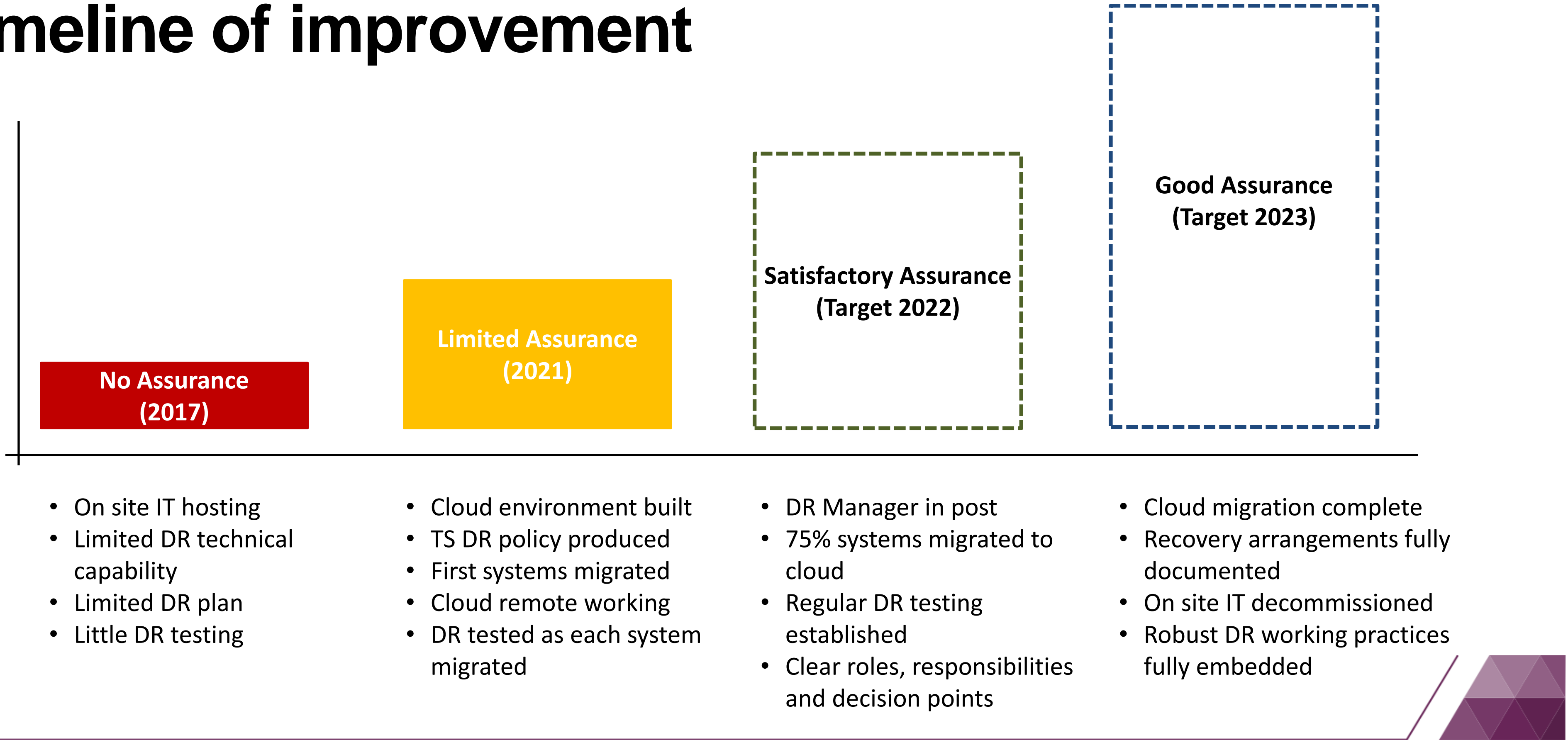| Recommendations from 2021 DR Audit	Status	Target
MAJOR – Uncompleted Business Impact Analysis (BIA) 1. Emergency Planning & Resilience to facilitate BIA completion. 2. Technology Services (TS) to assess BIA against current DR capability. 3. IT DR Plan to agree and document recovery order and interdependencies. *DR & Resilience Manager now recruited and he will lead the TS parts of this work.*	**Open**	- 30/09/22 30/09/22
MAJOR – Operating effectiveness of the disaster recovery requirements 1. DR requirements to be assessed when updates to BIAs occur. 2. TS to review Recovery Time Objective (RTO) & Recovery Point Objective (RPO) at Design Board.	Complete	
MAJOR – IT Disaster Recovery Testing IT DR plan to be tested at least annually. *DR & Resilience Manager now recruited and he will lead this work.*	**Open**	30/09/22
Moderate – Roles and responsibilities for invoking the IT Disaster Recovery Plan Disaster recovery invocation procedure and responsibilities should be documented.	**Open**	30/09/22
Moderate - Draft IT Disaster Recovery Plan Complete Cloud Migration, document recovery arrangements and publish IT DR Plan. *DR & Resilience Manager now recruited and he will lead this work.*	**Open**	31/05/23
Moderate – Cloud Strategy Sign Off Cloud Strategy to be signed off.	Complete	-

Progress since last audit

Investment in cloud technology has significantly improved our capabilities:

- Improvements in the home working solutions provided by TS have greatly reduced our reliance on ECC premises .
- The Cloud Migration of on-site services has reduced the impact of a loss of County Hall
- Adoption of Office 365 – which has very high levels of resilience built-in has reduced the need for TS to implement and maintain costly DR capabilities in this area
- Upgrade of wi-fi systems across the ECC estate have improved our ability to work mobile and flexibly from any ECC location.
- Recent increase in Cybersecurity threats has prompted additional system backup and restore checks to be undertaken giving a higher level of assurance they are working effectively.

Timeline of improvement

**Good Assurance
(Target 2023)**

**Satisfactory Assurance
(Target 2022)**

**Limited Assurance
(2021)**

**No Assurance
(2017)**

- On site IT hosting
- Limited DR technical capability
- Limited DR plan
- Little DR testing

- Cloud environment built
- TS DR policy produced
- First systems migrated
- Cloud remote working
- DR tested as each system migrated

- DR Manager in post
- 75% systems migrated to cloud
- Regular DR testing established
- Clear roles, responsibilities and decision points

- Cloud migration complete
- Recovery arrangements fully documented
- On site IT decommissioned
- Robust DR working practices fully embedded

Essex County Council

Questions?

DR & Resilience Journey

Technology Services

Essex County Council

ASSURANCE LEVEL

SATISFACTORY

LIMITED

NONE

TIME

Cloud Programme enabling DR capability

TS DR policy produced

First cloud DR test

Cloud based remote access implemented

DR & Resilience Manager recruited

Migration of on-prem apps to Cloud

New Wi-fi rollout completed

Routine DR testing

Ongoing migration of applications to SaaS