

Identity Recovery Readiness Guide

How prepared is your organisation to
restore trust after an identity compromise?

Most organisations invest heavily in preventing identity attacks. **Far fewer are prepared for what happens next.**

When privileged identities, service accounts, Active Directory, or cloud identity systems are compromised, the challenge shifts from detection to recovery.

This guide outlines key areas every organisation should evaluate to improve identity recovery readiness and operational resilience.

RESILIENCE BEYOND PREVENTION

Why Identity Recovery Matters

- ✓ Many organisations have incident response plans.
- ✓ Many have backup strategies.
- ✓ Many have security monitoring.

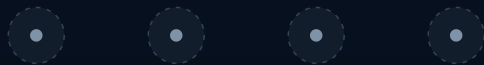
Yet relatively few have a documented and tested plan for **restoring trust in identity systems** following compromise.

WITHOUT IDENTITY TRUST

- ◆ Authentication becomes uncertain
- ◆ Privileged access cannot be validated
- ◆ Business operations may be disrupted
- ◆ Recovery timelines increase significantly

The ability to recover identity systems quickly is becoming a critical component of cyber resilience.

UNCERTAIN IDENTITY TRUST RESTORED & VALIDATED TRUST



● Trust unverified ● Recovered & re-validated

Privileged & Directory Recovery

AREAS **01-02** OF 06

01



RECOVERY READINESS AREA 01

Privileged Identity Recovery

QUESTIONS TO CONSIDER

- Can privileged accounts be rapidly identified?
- Do recovery procedures exist for administrative identities?
- Are privileged accounts regularly reviewed?
- Can emergency administrative access be established if required?

RISK OF WEAKNESS Delayed recovery and operational disruption.

02



RECOVERY READINESS AREA 02

Active Directory Recovery

QUESTIONS TO CONSIDER

- Are recovery procedures documented?
- Have recovery exercises been conducted?
- Are backups regularly validated?
- Can domain trust be re-established quickly?

RISK OF WEAKNESS Extended business interruption.

Cloud & Service Identity Recovery

AREAS 03-04 OF 06

03



RECOVERY READINESS AREA 03

Cloud Identity Recovery

QUESTIONS TO CONSIDER

- Can Entra ID administrative access be restored?
- Are emergency access accounts maintained?
- Are critical identity configurations documented?
- Are recovery responsibilities clearly assigned?

RISK OF WEAKNESS Loss of access to cloud services and applications.

04



RECOVERY READINESS AREA 04

Service Account Recovery

QUESTIONS TO CONSIDER

- Are critical service accounts documented?
- Are dependencies understood?
- Can credentials be rotated quickly?
- Are recovery procedures tested?

RISK OF WEAKNESS Application and operational outages.

Visibility & Proven Recovery

AREAS 05-06 OF 06

05



RECOVERY READINESS AREA 05

Identity Visibility

QUESTIONS TO CONSIDER

- Do you know which identities are most critical?
- Can privileged relationships be quickly identified?
- Are attack paths understood?
- Can recovery priorities be established rapidly?

RISK OF WEAKNESS Slower decision-making during recovery.

06



RECOVERY READINESS AREA 06

Recovery Testing

QUESTIONS TO CONSIDER

- Has identity recovery been tested in the last 12 months?
- Are recovery exercises documented?
- Are lessons learned captured?
- Are recovery metrics measured?

RISK OF WEAKNESS Unproven recovery capability.

SELF-ASSESSMENT

Identity Recovery Readiness Checklist

How many of the following can you confidently answer "Yes" to?



We have documented identity recovery procedures



We regularly test Active Directory recovery



Emergency access accounts are maintained



Critical service accounts are documented



Recovery responsibilities are clearly assigned



Identity recovery exercises have been conducted



Privileged identities are continuously reviewed



Recovery priorities are clearly understood

Recovery readiness is not measured during normal operations. **It is measured during disruption.**

If helpful, we'd be happy to have an initial discussion about your current approach to identity resilience and recovery readiness.

Request an Initial Conversation



OR

CONTACT

sales@cyberdna.com.au

WEB

cyberdna.com.au