






Audit Desk – Actions Tracking for Audit Professionals

Audit Desk is an easy to use, purpose-built action tracking system designed for Audit & Assurance professionals.

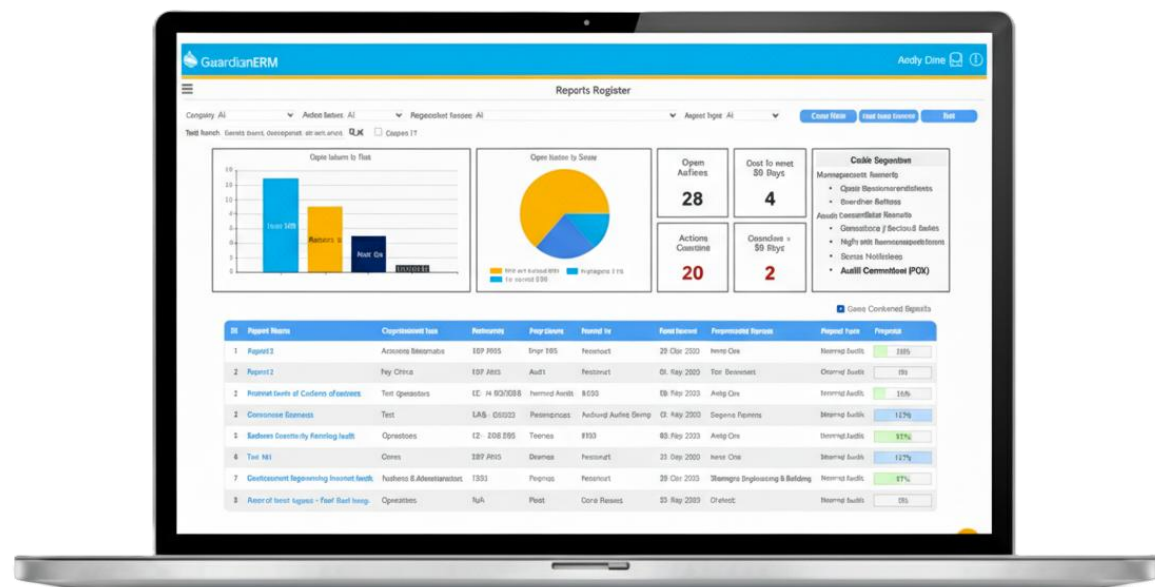
While many organisations still rely on spreadsheets and ad-hoc lists to manage audit recommendations & outstanding actions – Audit Desk bridges the gap that allows practitioners to move from static tracking methods to a simple and dynamic tech solution.

Some features within AuditDesk include:

 <b>Your Actions</b> All in One Location	Record all your actions in one system, link related findings and maintain traceability through unique IDs
 <b>Easy to Use</b> Planning & Tracking	Set due dates, monitor progress and upload evidence of remediation and maintain transparency
 <b>Assign &amp; Prioritise Tasks</b>	Allocate each action to an owner, set risk-based priorities and document management's response
 <b>Reporting &amp; Data Visualisations</b>	Generate executive ready dashboards and reports with exportable data for easy customisation
 <b>Secure Data Infrastructure</b>	Connect with existing systems securely using Single-Sign On, data encryption at rest & RBAC
 <b>Governance &amp; Validation</b>	Enforce independent verification, escalation of overdue items and maintain a complete audit trail



Audit Desk  
Actions Tracking for Audit Professionals

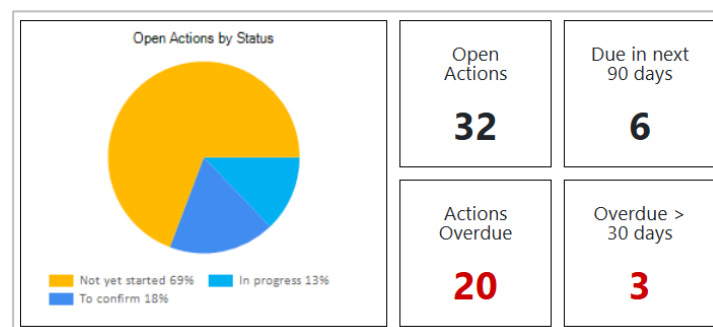


Driven by  GuardianERM

## How Does Audit Desk Work?

- Capture** Load findings and recommendations, upload relevant docs and record key details like report owner, source and key dates.
- Assign** Create actions, allocate action owners, set risk, deadlines and remediation notes.
- Track & Close** Monitor progress via dashboards, send reminders, gather evidence and verify completion of tasks.
- Executive Reporting** Generate executive ready reports and clear summaries for management and audit & risk committee audiences. Overdue items, Actions by risk and closure progress all in one click.

ID	Report Name	Organisation Unit	Reference	Dept/Area	Issued By	Date Issued	Responsible Person
1	Report 1	Accounts Receivable	REP #001	Dept 101	Inconsult	21-Oct-2025	Michael Strong
2	Report 2	Pay Office	REP #002	Audit	Inconsult	01-Sep-2025	AndyR
3	Internal Audit of Conflicts of Interest	Test Operations	CC - IA 03/2018	Internal Audit	BDO2	01-Mar-2018	Andy Chu
5	Business Continuity Planning Audit	Operations	CC - BDO IA21	Finance	BDO	01-Feb-2021	Andy Chu



ID	Action	Risk	Status	Resp.Person	Comment
<b>Report: Report 1</b>					
1.3	New action for MS	High	Not yet started	Michael Strong	
1.4	Test	High	Not yet started	Andy Chu	Test
<b>Report: Report 2</b>					
2.3	Action 2.1	Critical	In progress	Stuart McMillan Assurant	
<b>Report: Internal Audit Report - Fuel Card Usage</b>					
8.1	Develop a procedure on fuel card usage for all fuel cards	High	Not yet started	Manager Buildings & Depot and Fleet & Workshop Supervisor	
8.5	Develop a regular review process to ensure that all fuel cards are accounted for	High	Not yet started	Fleet & Workshop Supervisor	
8.7	Investigate the anomalies identified by Internal Audit and take necessary action.	High	Not yet started	Fleet & Workshop Supervisor	

# Audit Desk: Security & Data Recovery

We take data security & privacy very seriously and ensure that GuardianERM is always secure – this means our clients can always **Confidently Manage Their Risks**

## Secure by Design, Ready for Assurance – Audit Desk is powered by GuardianERM

Audit Desk is built on GuardianERM's secure, enterprise-grade platform, ensuring your audit actions and recommendations are protected by strong security controls, reliable infrastructure and compliance-ready safeguards. Here are some of the security measures across the application, servers and supporting infrastructure:

### Application Security

- Strong password security settings by default with customisation available for users to align with internal security policy
- All passwords are encrypted, salted one-way hashed for maximum security
- Platform sessions implement tokens to ensure access is always secure
- GuardianERM automatically closes sessions when there is no session activity for a defined period

### Server & Infrastructure Security

- GuardianERM's production server is hosted on Microsoft Azure's Sydney data centres, meeting global and regional standards (ISO 27001/27018, SOC 1-3, IRAP, ASD Certification, EU/US frameworks)
- Hardened security environment with VPN protection, MFA, JIT access, strict firewall/port rules, IP-controlled access, security logging and automated monitoring

### Single Sign-On (SSO)

- SSO is an authentication method that allows users to securely sign on through an active Azure Directory
- Faster IT implementation and integration with an organisations existing infrastructure
- Centralisation of credentials means easier login, simple assessment of logs across various systems and enables IT teams to identify suspicious behaviour far quicker than segregated systems

### Pen Testing & Vulnerability Scanning

- Regular penetration testing across multiple attack vectors on both Azure infrastructure and GuardianERM servers
- Proactive internal monitoring, performed by our security team, ensures that we are consistently identifying and addressing emerging vulnerabilities
- Recent external penetration testing confirmed no high-risk vulnerabilities with the GuardianERM platform

### E2E Encryption

- GuardianERM ensures that your data is protected in-transit from browser to our servers
- We use the strongest internet encryption technologies to ensure that your data is always protected (HTTPS, SSE & latest TLS security)
- Data is stored on our secure, Australian based, servers and encrypted-at-rest for further security

### Backups & Disaster Recovery

- The server is locally protected by Azure Live Migration which detects hardware/network failures and moves the entire service to a new physical failover server without data loss
- All data is backed up daily and stored externally. A data rollback can be performed to reinstate any of the previous 30 days
- Physically secure data centres with biometric access, 24/7 security, man-trap entry, UPS redundancy and backup generators

For more information, see the [Security and Disaster Recovery](#) page on the GuardianERM website.