

A SAMPLE OF THE WEEKLY REVIEW

What Dex found. What to do next.

Selected Azure findings from a client review dated 2 October 2026. Names and resource identifiers have been removed. These findings are shown before remediation. Later examples are labelled separately.

Your virtual IT & security worker reviews and recommends. Your team or IT provider makes the changes. Dex is always read only.

01 / WEBSITE PROTECTION

A firewall set to watch, not block.

Evidence: The application gateway in front of customer websites used a Web Application Firewall policy in Detection mode. Its managed rules were set to log matching requests without blocking them.

Why it matters: Installing a firewall is only part of protecting a website. Confirm why blocking is not enabled and what other protection exists.

Next steps for your IT team

1. Check why Detection mode is in use.
2. Review rule matches, false positives and required exceptions.
3. After validation, enable Prevention mode and verify the results.

Technical reference: [Microsoft: Web Application Firewall Detection mode](#).

02 / RECOVER YOUR WORK

Four servers with stopped backups.

Evidence: Four running virtual machines had stopped receiving Azure backups. Their last recorded Azure backups were in May or August 2026.

Why it matters: Restoring an old backup could lose months of work. First check whether another backup system covers the missing period.

1. Confirm recovery requirements and alternative backup coverage.
2. Restore the required schedule and check successful backup runs.
3. Test a restore so recovery is demonstrated.

This finding concerns Azure Backup. It does not establish that every other backup method was absent.

03 / LIMIT DOWNTIME

Important data. Three days of backup history.

Evidence: A MySQL database holding nearly 2 TB ran on one burstable CPU, retained three days of backups, had no standby and had no enabled Azure Monitor alert covering it.

Why it matters: A problem discovered after that backup window could be harder to recover from. Confirm the downtime the business can accept and review the related settings together.

1. Confirm the workload, recovery window and acceptable downtime.
2. Check CPU usage and credits, storage headroom and other monitoring.
3. Review sizing, backup retention and standby against those requirements.

Database size alone does not establish that the CPU tier is inadequate. The right settings depend on the business workload.

FOLLOW-UP / RENEWED IN TIME

A renewal deadline caught in time.

Dex flagged a certificate approaching expiry. The IT team renewed it in time, avoiding an expiry-related interruption. This renewal was confirmed after the review; no notice period or financial loss is claimed.

OTHER REVIEW EXAMPLES

Access and costs left behind.

Old migration apps: Microsoft 365 migration apps retained full read and write access to mailboxes after their migration work was finished. Confirm that the apps are retired, then remove unnecessary access.

Unused services: A separate review found unused Azure resources, including empty App Service hosting plans, costing about \$200/month. Check dependencies before removing what is no longer needed. This is observed spend, not verified savings.

Former employees: Paid Microsoft 365 licences remained assigned after people left. Confirm offboarding and data retention requirements, then reclaim unnecessary licences.

What carries into the next week

Keep open items visible, record when they first appeared, and note what has been marked resolved or accepted. The customer or IT provider carries out the work. This sample contains selected findings, not the full client register.

Discuss weekly reviews for your business at dexonduty.com. Microsoft 365 and Azure are supported today.