Comprehensive GRC Audit Framework for the Azure Cyber Range: Operationalizing Global Visibility

Executive Summary

The recent architectural update to the Cyber Range, specifically the enablement of "View ALL Resources" via the Cyber Range Utilities Page, represents a fundamental paradigm shift in the operational capability available to users. Previously, the Cyber Range operated as a collection of siloed tenancies where users were restricted to a myopic view of their own resource groups. This limitation, while beneficial for reducing cognitive load and enforcing isolation, inherently prevented the execution of holistic Governance, Risk, and Compliance (GRC) audits. The transition to a platform-level view—where a user can observe the aggregate infrastructure including all Resource Groups, Virtual Machines (VMs), and associated assets—transforms the user from a mere operator into a high-level Auditor or Cloud Governance Officer.

This report outlines an exhaustive, expert-level framework for leveraging this new visibility to perform high-fidelity GRC audits. It moves beyond simple resource enumeration to deeply analyze security postures, cost inefficiencies, and compliance drifts across the entire range. By utilizing Azure Resource Graph (ARG) Explorer and the Kusto Query Language (KQL), users can now interrogate the Azure fabric to uncover second- and third-order risks—ranging from shadow IT infrastructure and unmanaged attack surfaces to significant financial waste and identity entitlement sprawl. This document serves as the definitive manual for conducting these audits, interpreting the data, and proposing remediation strategies aligned with industry standards such as the Center for Internet Security (CIS) Benchmarks and the Microsoft Cloud Security Benchmark (MCSB).

The implications of this visibility are profound. It allows for the detection of "Zombie" infrastructure that drains budget without providing value [1], the identification of "soft" security underbellies where development conveniences have left management ports exposed to the internet [2], and the tracking of data sovereignty risks through misconfigured storage accounts.[4] This report details the methodologies to execute these audits immediately.

---

1. The Paradigm Shift: From Tenant to Platform Governance

1.1 The Governance Void in Siloed Environments

In the previous configuration of the Cyber Range, governance was essentially opaque to the user. A user could ensure their own Virtual Machine (VM) was secure, but they had no visibility into whether a neighbor's compromised VM posed a lateral movement risk, or if the aggregate consumption of resources was optimized. This is analogous to a departmental manager who sees only their own budget, versus a CFO who sees the entire corporate ledger.

The "View ALL" feature, activated via the Account Reset / Cyber Range Utilities Page, bridges this gap. It provides the "God Mode" perspective required for auditing. In Azure terms, this elevates the user's effective scope from ResourceGroup level to Subscription or even ManagementGroup level visibility. This is the foundational requirement for any GRC function: you cannot govern what you cannot see.[5]

1.2 The Risks of Expanded Visibility

While the prompt notes that the primary downside is potential confusion due to the volume of resources, from a GRC perspective, the risk is information overload leading to analysis paralysis. A Cyber Range is dynamic; resources are spun up and torn down rapidly. An auditor looking at "ALL resources" sees a chaotic mix of transient student labs, persistent infrastructure, and abandoned experiments.

Therefore, the first task of the new GRC audit capability is **Noise Reduction**. This is achieved not by ignoring data, but by structured querying using Azure Resource Graph (ARG). ARG is designed for high-performance resource exploration, allowing the auditor to filter thousands of objects in milliseconds to find the specific deviations from policy that matter.[7]

1.3 The Strategic Value of the Audit

The prompt suggests use cases such as "security audit," "cost analysis," and "curiosity." In a professional context, these translate to:

- **Security Posture Management (CSPM):** proactively identifying misconfigurations before they are exploited.
- **Financial Operations (FinOps):** optimizing unit economics and eliminating waste.
- **Operational Excellence:** ensuring naming conventions and tagging strategies are adhered to for manageability.

By executing the audits detailed below, a user simulates the role of a Cloud Security Posture Management (CSPM) tool, effectively performing the work of automated systems like Microsoft Defender for Cloud, but with the manual nuance and contextual understanding of a human expert.[5]

---

2. Asset Management and Inventory Control

2.1 The Foundation of Security: Knowing What Exists

Control 1 of the CIS Critical Security Controls is "Inventory and Control of Enterprise Assets." In the Cyber Range, asset sprawl is the default state. Users create resources for a specific lab and often fail to delete them. The global view allows for the construction of a "Single Source of Truth" (SSoT).

The audit begins by querying the Resources table to generate a breakdown of assets by type and location. This high-level heatmap reveals the "center of gravity" of the infrastructure. For example, if 90% of resources are in East US but a cluster of highly expensive GPU VMs appears in West Europe, this anomaly warrants immediate investigation. It could indicate a user bypassing regional policy restrictions or a compromised account launching resources in a non-standard region to evade detection.[8]

2.2 Tagging Hygiene: The Metadata of Governance

Tagging is the primary mechanism for organizing cloud resources. It allows for the association of technical assets with business contexts (e.g., Owner, Project, CostCenter). In a Cyber Range, where the "business context" might be a specific class or student ID, the absence of tags renders the resource an "orphan."

2.2.1 Auditing for Tagging Drift

A robust audit identifies resources that lack mandatory tags. The "View ALL" feature allows the auditor to scan the entire subscription for compliance.

- **Missing Tags:** Resources with no tags are impossible to attribute to a user without digging into Activity Logs (which may be purged).
- **Inconsistent Taxonomy:** The use of environment: prod vs. Environment: Production. Case sensitivity matters in KQL and automation scripts.

The risk of poor tagging is operational blindness. If a VM is attacking a target, and it has no Owner tag, the incident response team (or the range administrator) loses critical minutes trying to identify who deployed it.

Table 1: Tagging Compliance Audit Matrix

Audit Focus	Risk Description	Governance Consequence
Untagged Resources	Assets with tags == null or	Inability to perform

	empty arrays.[11]	chargeback or identify ownership during incidents.
Schema Validation	Tags that exist but violate policy (e.g., Owner: TBD).[12]	Automation failure; cleanup scripts may skip these resources.
Case Sensitivity	CostCenter vs costcenter.[13]	Fragmentation of reporting data; difficulty in aggregating costs.

2.2.2 The KQL Mechanism for Tag Auditing

To execute this audit, one leverages the tags property bag within the ARG Resources table. The query logic involves filtering for resources where the specific tag key is missing. This highlights the power of the global view: a user can now identify *systemic* non-compliance across the range. For example, if an entire Resource Group is missing tags, it suggests a deployment script error or a lack of policy enforcement at the group level.[14]

---

3. Financial Governance (FinOps): Eliminating Waste and Zombie Infrastructure

3.1 The Economic Impact of "Zombie" Resources

Cost optimization is a core pillar of the Microsoft Well-Architected Framework. In a Cyber Range, where learning involves trial and error, the creation of "Zombie" infrastructure—resources that exist and incur costs but provide no value—is endemic. The "View ALL" capability allows for a comprehensive "Waste Audit" that was previously impossible when users could only see their active successes, not their forgotten failures.

3.2 Orphaned Managed Disks: The Silent Budget Killer

One of the most persistent sources of wasted spend in Azure is the unattached Managed Disk. When a Virtual Machine (VM) is deleted, its associated disks are **not** deleted by default. This is a safety feature to prevent data loss, but in a test environment, it leads to massive debt. If a user deletes a VM but forgets the disk, the disk persists in the storage account, incurring monthly storage costs (especially for Premium SSDs) despite being unconnected to any compute resource.[16]

3.2.1 Deep Dive: The Audit Mechanism

The audit involves querying the microsoft.compute/disks resource type and filtering for the

managedBy property.

- **Connected Disk:** The managedBy property contains the Resource ID of the VM it is attached to.
- **Orphaned Disk:** The managedBy property is null or empty.[17]

The financial implication is linear and cumulative.

$$\text{Total Waste} = \sum (\text{Disk Size} \times \text{Tier Cost})$$

In a range with hundreds of users, this can amount to thousands of dollars monthly. Furthermore, these disks represent a security risk (data leakage). If a disk containing sensitive audit logs or credentials is left orphaned, it could potentially be attached to a different VM by a malicious actor with sufficient permissions (Contributor), effectively bypassing the original VM's access controls.16

3.3 Stopped vs. Deallocated Virtual Machines

A nuanced aspect of Azure billing that often confuses new users (as noted in the prompt) is the distinction between a VM that is "Stopped" and one that is "Deallocated."

- **Stopped (OS Shutdown):** The user ran shutdown -h now inside the Linux shell. The OS is down, but the Azure hardware is still reserved. **Billing continues.**
- **Stopped (Deallocated):** The user stopped the VM via the Azure Portal or CLI. The hardware is released. **Billing stops** (though storage costs for disks persist).[1]

3.3.1 Identifying Non-Deallocated Zombies

With the global view, an auditor can query for VMs where the power state is PowerState/stopped rather than PowerState/deallocated. These are resources that are burning budget for zero utility. The audit should also look for VMs that have been deallocated for an excessive period (e.g., > 45 days). A VM deallocated for months is likely abandoned and is a prime candidate for deletion (along with its disks and NICs).[20]

3.4 Public IP Sprawl and Dissociation

Public IP addresses in Azure are billable resources, regardless of association. Similar to disks, Public IPs can become dissociated from network interfaces (NICs). An audit should identify microsoft.network/publicipaddresses resources where the ipConfiguration reference is null. These "dangling" IPs not only waste money but also pose a threat if they are on allow-lists for other services (e.g., a SQL Server firewall allowing a specific IP). If that IP is released and re-assigned to a different tenant, a third party could inadvertently gain access to systems trusting that IP.[22]

---

4. Network Security Governance: Reducing the Attack Surface

4.1 The Danger of Permissive Network Security Groups (NSGs)

In a learning environment, users often default to the path of least resistance: allowing all traffic to ensure connectivity. This manifests as NSG rules with Source: Any (0.0.0.0/0), Destination: Any, and Action: Allow on management ports like SSH (22) and RDP (3389). This configuration leaves VMs vulnerable to brute-force attacks, credential stuffing, and botnet recruitment. The "Internet" is a hostile environment; a VM with port 3389 open will receive login attempts within seconds of deployment.[2]

4.2 Auditing Inbound Exposure via ARG

The "View All" capability is particularly potent here. An auditor can scan *every* NSG in the subscription to identify rules that expose critical ports to the entire internet.

The technical complexity of this audit lies in the data structure. NSG rules are nested properties. The KQL query must use mv-expand to flatten the securityRules array, allowing the auditor to evaluate each rule individually against the criteria:

1. access == 'Allow'
2. direction == 'Inbound'
3. sourceAddressPrefix == '*' or Internet
4. destinationPortRange contains 22, 3389, or covers them via a range (e.g., 0-65535).[3]

Insight: Finding a high volume of such rules suggests a training gap. Users likely do not understand how to use Just-In-Time (JIT) VM Access or Azure Bastion. The recommendation would be to implement Azure Bastion, which tunnels RDP/SSH over SSL (443), eliminating the need for open management ports on the public internet.[2]

4.3 The "Joined" Risk: Public IPs on Exposed VMs

A theoretical risk becomes a concrete vulnerability when an exposed NSG rule is applied to a NIC that actually possesses a Public IP. A comprehensive audit uses a join operation in KQL to correlate three distinct datasets:

1. **Virtual Machines:** To get the VM ID and name.
2. **Network Interfaces:** To link VMs to IP Configurations.
3. **Public IPs:** To confirm the presence of a routable internet address.
4. **NSGs:** To confirm the permissive rule.

By intersecting these data points, the auditor generates a "Critical Risk List" of VMs that are directly reachable from the internet on management ports. This is a high-priority remediation target. The "View All" feature is essential here because these components (VM, NIC, IP, NSG)

might exist in different resource groups (though rare in simple setups, it is common in hub-and-spoke architectures).[25]

---

5. Identity and Access Management (IAM): The New Security Perimeter

5.1 Role-Based Access Control (RBAC) Hygiene

Identity is the modern security perimeter. In Azure, RBAC controls who can do what. A common misconfiguration in collaborative environments is the over-provisioning of the Owner or Contributor roles. The Owner role, in particular, allows a user to manipulate role assignments, effectively enabling them to grant access to others or even lock out legitimate administrators. This is known as "Role Roulette" – granting broad permissions without understanding the granular implications.[27]

5.1.1 Auditing Privileged Role Assignments

With the ability to view all resources, the auditor can inspect role assignments across subscriptions. The goal is to identify:

- **Excessive Owners:** Subscriptions with more than 2-3 owners.
- **External Guest Users:** Accounts invited from outside the organization (B2B guests) that hold Owner or Contributor rights. This is a severe risk; if the guest's home identity is compromised, the attacker pivots into the Cyber Range.[30]

The audit query targets the authorizationresources table (specifically microsoft.authorization/roleassignments). By filtering for the Role Definition IDs corresponding to Owner (8e3af657-a8ff-443c-a75c-2fe8c4bcb635) and Contributor (b24988ac-6180-42a0-ab88-20f7382dd24c), and correlating with principalType == 'User', the auditor can map out the privilege landscape. This visibility prevents "Permission Creep," where users accumulate rights over time that they no longer need.[31]

5.2 Service Principal Governance

Service Principals (SPs) are non-human identities used by applications and automation scripts. Unlike users, SPs do not have MFA challenges in the same way interactive logins do. If an SP with Contributor rights has its credentials (client secret) exposed in code, it offers a silent backdoor into the environment.

The audit involves listing all SPs with elevated permissions and checking for their creation dates and owners. "Orphaned" Service Principals—those created by users who have since left the organization—are a prime target for cleanup. The "View All" feature allows the auditor to see SPs created by other users that might have been forgotten but still hold keys to the

kingdom.[32]

---

6. Data Sovereignty and Storage Governance

6.1 The Scourge of Public Blobs

One of the most frequent causes of massive data breaches in the cloud is the misconfigured Storage Account allowing anonymous public read access to containers (blobs). Developers often enable this for convenience during testing (e.g., to host images for a website) and forget to disable it. This turns the storage account into a public file server.[4]

6.1.1 Detecting Anonymous Access

The audit focuses on the allowBlobPublicAccess property of the microsoft.storage/storageaccounts resource.

- **Risk:** If this is set to true (or null in older API versions), the storage account *permits* the configuration of public containers. Even if no containers are currently public, the *potential* exists.
- **Governance Goal:** Enforce this to false at the account level. This overrides any container-level settings, providing a hard guarantee that no data can be accidentally exposed.

This audit requires scanning every storage account in the range. Without "View All," a user could only secure their own data; now, they can identify systemic data leakage risks across the platform.[33]

Table 2: Storage Security Configuration Audit

Property	Desired State	Risk of Deviation
allowBlobPublicAccess	False / Disabled	**Data Exfiltration:** Anonymous users can enumerate and download blob data.[4]
minimumTlsVersion	TLS1_2	**Man-in-the-Middle:** Legacy protocols (TLS 1.0/1.1) have known crypto vulnerabilities.[34]

networkRuleSet.defaultAction	Deny	**Unrestricted Access:** The storage endpoint accepts traffic from any IP on the internet.[35]

6.2 Storage Firewall Configuration

Beyond public blobs, the storage account's network ruleset controls which networks can connect. A governance audit checks the networkRuleSet.defaultAction.

- **Allow:** The storage account is exposed to the public internet (though authentication is still required).
- **Deny:** The storage account is firewalled and only accepts traffic from specific Virtual Networks (Service Endpoints) or whitelisted IPs.

In a high-security Cyber Range, Deny should be the standard. The audit identifies all accounts set to Allow and flags them for remediation, pushing users towards using Private Endpoints for secure connectivity.[36]

---

7. Database Governance: SQL and Data Integrity

7.1 SQL Auditing and Threat Detection

For Azure SQL Servers, governance requires visibility into database events. Auditing tracks database events and writes them to an audit log in an Azure storage account, Log Analytics workspace, or Event Hubs. This is crucial for forensic analysis after an incident.

The audit query targets microsoft.sql/servers and checks the auditingSettings. If the state is Disabled, the database is effectively a black box regarding user activity. An auditor cannot see if a user is executing DROP TABLE commands or running unauthorized SELECT queries on sensitive tables. Furthermore, "Advanced Threat Protection" (Defender for SQL) should be enabled to detect anomalous activities like SQL injection attempts or unusual login locations.[38]

7.2 Public Network Access for SQL

Similar to storage, Azure SQL supports a "Public Network Access" toggle. If enabled, the database listens on a public endpoint. While a firewall may still block specific IPs, the exposure of the endpoint itself increases the risk of Denial of Service (DoS) or brute-force attacks. The audit should identify all SQL servers where publicNetworkAccess is Enabled and flag them for review, recommending the use of Private Links instead.[40]

---

8. Compliance Framework Alignment (CIS & NIST)

8.1 Automating CIS Benchmark Verification

The Center for Internet Security (CIS) Azure Benchmark provides a prescriptive set of best practices. The "View All" capability allows the user to manually verify compliance against these benchmarks using the data collected in the previous sections. The auditor can essentially run a "Mock Audit" against the platform.

- **CIS 2.1:** Ensure that standard pricing tier is selected (Defender for Cloud).
- **CIS 3.1:** Ensure that 'Secure transfer required' is set to 'Enabled' for Storage Accounts.
- **CIS 6.1:** Ensure that RDP access is restricted from the internet.

By mapping the ARG queries to these specific CIS controls, the auditor can generate a "Compliance Scorecard" for the Cyber Range. This moves the exercise from a technical treasure hunt to a formal compliance audit, providing a quantifiable metric of the environment's health (e.g., "We are 65% compliant with CIS Level 1").[42]

---

9. Second-Order Insights and Strategic Recommendations

9.1 The "Broken Window" Theory of Cloud Governance

The data gathered from these audits often reveals a correlation between different types of negligence. A resource group containing a VM with open RDP ports (Network risk) often contains orphaned disks (Cost risk) and lacks proper tagging (Asset risk). This clustering of failures suggests that specific users or departments are systematically ignoring governance standards.

Strategic Recommendation: Rather than fixing individual resources, the GRC response should be to identify these "high-risk clusters" and target the owners for re-training. This addresses the root cause (human behavior) rather than the symptom (misconfiguration).

9.2 From Detective to Preventative: The Policy Loop

While the "View All" feature enables *detective* governance (finding bad things after they happen), the ultimate goal is *preventative* governance. The insights gained here should drive the creation of **Azure Policy** definitions.

- *Observation:* Many storage accounts have public access.
- *Action:* Assign a Policy with the Deny effect to prevent the creation of storage accounts with allowBlobPublicAccess = true.

This feedback loop—Audit -> Analyze -> Policy Creation—is the maturity cycle of Cloud GRC. The audit provided by the new visibility is the fuel for this engine.[9]

9.3 Cost-Security Synergy

There is a direct synergy between FinOps and Security. Deleting a zombie VM to save money *also* eliminates a potential foothold for attackers. A VM that doesn't exist cannot be hacked. This dual-benefit narrative is powerful when presenting audit findings to leadership. "We can reduce the attack surface by 20% while simultaneously cutting the monthly bill by 15%." This framing ensures that governance initiatives get funded and prioritized.

Conclusion

The enablement of full resource visibility in the Cyber Range is not merely a "quality of life" improvement; it is an operational game-changer. It unlocks the ability to perform enterprise-grade Governance, Risk, and Compliance audits that were previously impossible. By systematically interrogating the environment using the strategies and queries outlined in this report—covering Identity, Network, Data, and Cost—a user can transform the range from a chaotic collection of resources into a governed, secure, and optimized cloud platform.

The "View All" feature provides the raw data; the GRC framework provides the wisdom to interpret it. Whether for security experience, cost optimization, or simple curiosity, the ability to see the whole picture is the first step towards mastering the cloud. The next step is taking action on what is found.

Appendix A: Essential KQL Audit Queries for the Cyber Range

A.1 Unattached Managed Disks (Cost/Security)

This query identifies disks that are paying for storage but not attached to any VM.

Code snippet

```
Resources
| where type =~ 'microsoft.compute/disks'
| where properties.diskState == 'Unattached'
| project name, subscriptionId, resourceGroup, location, diskSizeGB = properties.diskSizeGB, sku = properties.sku.name
```

```
| sort by diskSizeGB desc
```

A.2 Publicly Exposed NSG Rules (Network Security)

This query flattens NSG rules to find Inbound Allow rules from the Internet on high-risk ports.

```
Code snippet

Resources

| where type =~ 'microsoft.network/networksecuritygroups'
| mv-expand rules=properties.securityRules
| where rules.properties.access == 'Allow'
| where rules.properties.direction == 'Inbound'
| where rules.properties.sourceAddressPrefix == '*' or rules.properties.sourceAddressPrefix
== 'Internet'
| where rules.properties.destinationPortRange == '22' or
rules.properties.destinationPortRange == '3389'
| project NSGName=name, RuleName=rules.name,
Port=rules.properties.destinationPortRange, Source=rules.properties.sourceAddressPrefix
```

A.3 Storage Accounts Allowing Public Access (Data Protection)

This query checks for the allowBlobPublicAccess flag.

```
Code snippet

Resources

| where type =~ 'microsoft.storage/storageaccounts'
| extend allowBlobPublicAccess = properties.allowBlobPublicAccess
| where allowBlobPublicAccess == true or isnull(allowBlobPublicAccess)
| project name, resourceGroup, subscriptionId, allowBlobPublicAccess
```

A.4 Identifying "Zombie" VMs (Cost Optimization)

This query distinguishes between VMs that are just "Stopped" (Billable) and "Deallocated"

(Non-Billable).

Code snippet

Resources

```
| where type =~ 'Microsoft.Compute/virtualMachines'
| extend PowerState = tostring(properties.extended.instanceView.powerState.code)
| where PowerState == 'PowerState/stopped' or PowerState == 'PowerState/deallocated'
| project name, resourceGroup, PowerState, location
```

Works cited

1. Top 10 Azure Cost Optimization Checklist - Lucidity, accessed January 4, 2026, https://www.lucidity.cloud/blog/azure-cost-optimization-checklist
2. Working with VMs and NSGs in Azure Bastion | Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/bastion/bastion-nsg
3. Azure PowerShell: Scan all the Network Security Groups in all the subscriptions and list the internet exposed ports - Reddit, accessed January 4, 2026, https://www.reddit.com/r/AZURE/comments/irhjdk/azure_powershell_scan_all_the_network_security/
4. Remediate anonymous read access to blob data (Azure Resource Manager deployments), accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-prevent
5. Azure security logging and auditing | Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/security/fundamentals/log-audit
6. The Microsoft 365 governance implementation checklist IT directors, accessed January 4, 2026, https://www.syskit.com/blog/microsoft-365-governance-checklist/
7. Overview of Azure Resource Graph - Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/governance/resource-graph/overview
8. Explore your Azure resources with Resource Graph - Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/governance/resource-graph/concepts/explore-resources
9. Regulatory Compliance details for Microsoft cloud security benchmark - Azure Policy, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/governance/policy/samples/azure-security-benchmark
10. Starter Resource Graph query samples - Azure - Microsoft Learn, accessed

January 4, 2026, https://learn.microsoft.com/en-us/azure/governance/resource-graph/samples/starter
11. Find the resources which are untagged / not having any Tags in a Subscription, accessed January 4, 2026, https://learn.microsoft.com/en-us/answers/questions/1532377/find-the-resources-which-are-untagged-not-having-a
12. Azure Tagging Best Practices Guide - Turbo360, accessed January 4, 2026, https://turbo360.com/blog/azure-tagging-best-practices
13. Azure resource graph unable to collect tags from resources - Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/answers/questions/1488498/azure-resource-graph-unable-to-collect-tags-from-r
14. How to display missing tags for resources and resource groups in azure subscription, accessed January 4, 2026, https://stackoverflow.com/questions/76859787/how-to-display-missing-tags-for-resources-and-resource-groups-in-azure-subscript
15. Inventory of Azure Resource Tagging with Graph Explorer and KQL, accessed January 4, 2026, https://lexhegt.me/inventory-azure-resource-tagging-with-graph-explorer/
16. Cost Optimization options for unattached Azure Managed Disks | Microsoft Community Hub, accessed January 4, 2026, https://techcommunity.microsoft.com/blog/azurestorageblog/cost-optimization-options-for-unattached-azure-managed-disks/3751770
17. Find and delete unattached Azure managed and unmanaged disks - Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/virtual-machines/windows/find-unattached-disks
18. Kusto Query to get Report on Orphaned Azure VM Disks and when they became unattached. - Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/answers/questions/1315021/kusto-query-to-get-report-on-orphaned-azure-vm-dis
19. Azure Storage Cost Optimization: 19 Ways To Cut Waste - CloudZero, accessed January 4, 2026, https://www.cloudzero.com/blog/azure-storage-cost-optimization/
20. Project Flash - Use Azure Resource Graph to monitor Azure Virtual Machine availability, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/virtual-machines/flash-azure-resource-graph
21. how to get Azure VM last reboot using azure resource graph - Stack Overflow, accessed January 4, 2026, https://stackoverflow.com/questions/74938904/how-to-get-azure-vm-last-reboot-using-azure-resource-graph
22. Public IP addresses in Azure - Virtual Network - Microsoft Learn, accessed January 4, 2026,

https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses
23. Azure Resource Graph sample queries for Azure networking - Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/networking/fundamentals/resource-graph-samples
24. How to set up an Azure alert for inbound port rule changes - Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/answers/questions/1402871/how-to-set-up-an-azure-alert-for-inbound-port-rule
25. Azure Resource Graph query to find all VMs with public IPs - Stack Overflow, accessed January 4, 2026, https://stackoverflow.com/questions/56758465/azure-resource-graph-query-to-find-all-vms-with-public-ips
26. How To Monitor For Risky Public Azure Virtual Machines - ARGOS Cloud Security, accessed January 4, 2026, https://argos-security.io/2021/09/15/how-to-monitor-for-risky-public-azure-virtual-machines/
27. Azure Identity Management and access control security best practices - Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices
28. THE 10 MOST COMMON AZURE MISCONFIGURATIONS AND HOW TO FIX THEM - dandh.ca., accessed January 4, 2026, https://www.dandh.ca/media/pdf/pages/cloud/vendor/CloudCheckr/CloudCheckr-The-10-Most-Common-Azure-Misconfigurations-and-How-to-Fix-Them.pdf
29. Azure API vulnerability and built-in roles misconfiguration enable corporate network compromise - Reddit, accessed January 4, 2026, https://www.reddit.com/r/AZURE/comments/1lpwxv2/azure_api_vulnerability_and_builtin_roles/
30. Assign Azure roles to external users using the Azure portal - Azure RBAC | Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-external-users
31. Azure Resource Graph Query for Subscription Owner Role Assignments, accessed January 4, 2026, https://blog.tyang.org/2024/10/30/azure-resource-graph-query-sub-owner-role-assignments
32. Find service principals with privileged roles - Seif Bassem, accessed January 4, 2026, https://www.seifbassem.com/blogs/posts/arg-service-principals-role-assignments/
33. Azure Policy 'Allow Blob anonymous access' - Reddit, accessed January 4, 2026, https://www.reddit.com/r/AZURE/comments/1akdb32/azure_policy_allow_blob_anonymous_access/

34. Secure your Azure Monitor deployment - Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/azure-monitor/fundamentals/best-practices-security
35. Restrict Default Network Access for Storage Accounts - Trend Micro, accessed January 4, 2026, https://www.trendmicro.com/cloudoneconformity/knowledge-base/azure/StorageAccounts/restrict-default-network-access.html
36. Set the default public network access rule of an Azure Storage account - Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security-set-default-access
37. Checking Public Network Access Status for Azure Storage Accounts - Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/answers/questions/1531464/checking-public-network-access-status-for-azure-st
38. How to Enable Auditing and Threat Detection for Azure SQL Database in a HIPAA-Compliant Healthcare Application - Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/answers/questions/5559153/how-to-enable-auditing-and-threat-detection-for-az
39. Enable Auditing for SQL Servers | Trend Micro, accessed January 4, 2026, https://www.trendmicro.com/cloudoneconformity/knowledge-base/azure/Sql/auditing.html
40. How to know the public exposure of your Azure resources? - Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/answers/questions/1886297/how-to-know-the-public-exposure-of-your-azure-reso
41. Findings all Azure SQL Servers with "Deny public network access" disabled, accessed January 4, 2026, https://techcommunity.microsoft.com/discussions/azure/findings-all-azure-sql-servers-with-deny-public-network-access-disabled/3159852
42. CIS Microsoft Azure Benchmarks - CIS Center for Internet Security, accessed January 4, 2026, https://www.cisecurity.org/benchmark/azure
43. Regulatory Compliance details for CIS Microsoft Azure Foundations Benchmark 2.0.0, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/governance/policy/samples/cis-azure-2-0-0
44. Azure Policy definitions audit effect - Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effect-audit