Practical GRC Projects & Portfolio Building: Part 2 – The Second-Party Audit Simulation

1. Introduction: The Architect's Perspective

The transition from a mid-level Governance, Risk, and Compliance (GRC) analyst to a senior architect or audit director requires a fundamental restructuring of one's professional worldview. In the initial stages of a GRC career—the focus of Part 1 of this series—the primary objective is often *construction*. The practitioner is a builder, tasked with drafting policies, establishing risk registers, and implementing the foundational controls of an Information Security Management System (ISMS). The work is introspective, collaborative, and focused on creating order from chaos within one's own organization. This is the "First-Party" perspective: working from the inside out to build a defensible posture.

However, the zenith of GRC mastery lies not in building, but in *validating*. It requires the ability to look at a complex, sprawling environment—often one you did not build—and dissect its security posture with the cold, clinical precision of an external observer. This is the domain of the **Second-Party Audit**. In this scenario, you are no longer the builder; you are the inspector. You act on behalf of a parent company auditing a subsidiary, a large enterprise vetting a critical vendor, or a due diligence team assessing a merger and acquisition target.

This report, "Practical GRC Projects & Portfolio Building: Part 2," frames the next stage of your professional development through a rigorous **Second-Party Audit Simulation**. Unlike a Third-Party audit (such as a certification body assessment), which is often constrained by time, sampling limits, and a need for diplomacy, a Second-Party audit conducted with **"View ALL" access** is exhaustive. You possess the "Global Reader" keys to the kingdom. You are not reliant on the auditee to provide curated screenshots or cherry-picked evidence. You have direct access to the raw telemetry of the cloud infrastructure, the financial ledgers of the IT department, and the configuration files of the network perimeter.

The objective of this report is to guide you through four advanced, portfolio-defining projects. These are not hypothetical paper exercises. They are technical, data-driven investigations that utilize **Azure Resource Graph (ARG)** and **Kusto Query Language (KQL)** to interrogate the environment programmatically. We will move beyond the qualitative question of "Do you have an asset inventory?" to the quantitative assertion: "Your asset inventory is 18% inaccurate due to 45 unmanaged disks and 12 unauthorized databases."

By executing these projects, you will demonstrate a rare blend of skills: the legal and procedural knowledge of **ISO/IEC 27001:2022**, the financial acumen of a CIO, and the

technical capability of a Cloud Security Engineer. This fusion is the hallmark of a Modern GRC Leader.

1.1 The "View ALL" Simulation: A Paradigm Shift

To understand the gravity of these projects, one must appreciate the distinction between "assurance" and "verification." In a typical compliance workflow, a GRC analyst seeks assurance by asking questions. "Is data encrypted?" "Yes," says the engineer. "Can I see the policy?" "Here it is," says the manager. The analyst marks the control as "Compliant" based on this testimonial and documentary evidence.

In our **Second-Party Audit Simulation**, we reject assurance in favor of verification. With "View ALL" access—specifically, Reader permissions on the Azure Root Management Group or AWS Organization—we do not ask questions. We query state. The shift is profound:

- **Traditional GRC:** "Please provide a list of all administrators." -> *Relies on the honesty and competence of the admin.*
- **Technical GRC:** IamRoles | where RoleName == "Owner" | project PrincipalId -> *Relies on the undeniable truth of the configuration plane.*

This approach aligns with the industry's movement toward "Continuous Compliance" and "Policy as Code." It also prepares you for the reality of modern supply chain risk management, where trusting a vendor's questionnaire is no longer sufficient; validating their posture through technical integration is becoming the standard.

1.2 The Strategic Pillars of the Simulation

This report is structured around four distinct audit pillars, each mapping to critical components of the ISO 27001:2022 standard and representing a different facet of the auditor's responsibility:

1. **The Foundation (Discovery): Project 1** focuses on **Annex A 5.9 (Inventory of information and other associated assets)**. You cannot audit what you cannot see. We will build a dynamic, automated "Master Asset Inventory" that exposes the "Shadow IT" hidden in the cloud.
2. **The Perimeter (Security Validation): Project 2** targets **Annex A 5.23 (Information security for use of cloud services)** and **Annex A 8.20 (Networks security)**. We will audit the logical perimeter, exposing dangerous misconfigurations that leave the "front door" open to the internet.
3. **The Ledger (Financial Governance): Project 3** leverages **Clause 9.3 (Management Review)** to conduct a Cost Optimization Audit. We will prove that financial waste—such as orphaned resources—is a leading indicator of governance failure, bridging the gap between the CISO and the CFO.
4. **The Law (Sovereignty & Compliance): Project 4** utilizes Technical GRC to enforce Data Sovereignty. We will use KQL to police the geopolitical boundaries of data residency,

ensuring compliance with **GDPR** and **Contractual Requirements**.

---

2. Project 1: Build a 'Master Asset Inventory' (Annex A 5.9)

2.1 The Theoretical Framework: ISO 27001 Annex A 5.9

The foundation of any Information Security Management System (ISMS) is the asset inventory. You cannot protect, patch, or monitor a device if you do not know it exists. **ISO 27001:2022 Annex A 5.9** explicitly states: *"An inventory of information and other associated assets, including owners, should be developed and maintained"*.[1]

While this sounds simple, the practical application is notoriously difficult in dynamic cloud environments. The standard requires organizations to:

- **Identify assets:** Know what exists (servers, databases, code repositories).
- **Classify assets:** Understand their value and sensitivity.[2]
- **Assign ownership:** Designate a specific individual or role responsible for the asset's lifecycle.[3]
- **Document controls:** Record the protective measures in place for each asset.[1]

In a manual GRC world, this is achieved via a spreadsheet that is updated annually. In a cloud environment, where resources are spun up and torn down in minutes via CI/CD pipelines, a static spreadsheet is obsolete the moment it is saved. This "drift" between the *documented* inventory (the spreadsheet) and the *actual* inventory (the cloud) is a major source of risk. It creates "Shadow Assets"—resources that are running, costing money, and processing data, but are invisible to the security team.[4]

2.2 The "View ALL" Simulation: Technical Discovery

In this project, you will simulate the role of an auditor who suspects the auditee's inventory is incomplete. You will use **Azure Resource Graph (ARG)** to establish a "Source of Truth" that bypasses the potentially flawed CMDB (Configuration Management Database).

ARG is a powerful Azure service that allows you to query the Azure Resource Manager (ARM) at scale using KQL. Unlike PowerShell, which iterates through resources slowly, ARG can return details on 10,000+ resources in sub-second timeframes.[5]

Step 1: Establishing the Baseline Inventory

First, we must pull a complete list of everything that exists. The traditional portal view "All Resources" is useful, but it is limited in how it handles metadata and filtering at scale.[7] We

need a structured dataset.

KQL Query 1: The Master Inventory Extraction
This query retrieves every resource in the environment, along with its critical metadata: location, resource group, subscription, and tags.

Code snippet

```
Resources
| project
    ResourceId = id,
    Name = name,
    Type = type,
    Location = location,
    ResourceGroup = resourceGroup,
    SubscriptionId = subscriptionId,
    Tags = tags,
    Sku = sku.name,
    Kind = kind,
    ManagedBy = managedBy
| order by Name asc
```

- **Logic:** The project operator selects specific columns to reduce noise. managedBy is critical for identifying resources that are dependent on others (like a disk attached to a VM).[8]
- **Insight:** By exporting this result to CSV, you have an immutable snapshot of the environment at a specific point in time—a primary audit artifact.

Step 2: The "Shadow IT" Gap Analysis (Ownership Validation)

ISO 27001 A.5.9 mandates that assets must have "owners".[2] In a mature cloud environment, ownership is defined via **Tags**. A resource without an "Owner" tag is effectively an orphan; if it breaks or is attacked, the SOC (Security Operations Center) does not know who to call.

We will use KQL to hunt for resources that violate this policy. We are looking for resources where the tags property does not contain the key "Owner", "CostCenter", or "Department".[10]

KQL Query 2: Identifying Unmanaged/Untagged Assets

Code snippet

```
Resources

| where tags!has "Owner" and tags!has "CostCenter"
| project
    Name = name,
    ResourceGroup = resourceGroup,
    Type = type,
    Location = location,
    Tags = tags

| summarize UnmanagedAssetCount = count() by ResourceGroup
| order by UnmanagedAssetCount desc
```

- **Logic:**
  - where tags!has "Owner": This filters for resources that *lack* the specific string "Owner" in their tags JSON blob.[11]
  - summarize... by ResourceGroup: This groups the offenders, allowing the auditor to identify which departments or projects are the worst violators.[12]
- **Audit Finding:** If this query returns results, you have evidence of non-conformity. The organization claims to have an inventory with owners (A.5.9), but the technical reality proves otherwise.

Step 3: API Version and "Ghost" Resources

An advanced auditor checks for "Ghost" resources—those created with deprecated API versions or legacy methods that might not show up in standard modernized dashboards.

KQL Query 3: API Version Audit

Code snippet

```
Resources

| distinct type, apiVersion
| where isnotnull(apiVersion)
```

`| order by type asc`

- **Logic:** This helps identify if the environment is running on legacy infrastructure that might be outside the scope of modern governance tools.[13]

2.3 Audit Findings and Strategic Remediation

In your portfolio, you will translate these technical outputs into a formal audit narrative.

The Finding:

> "During the Second-Party Audit of the Azure Tenant, a reconciliation of the Master Asset Inventory against the configured metadata revealed a **Major Non-Conformity against ISO 27001:2022 Annex A 5.9**. Specifically, 23% of production assets (approx. 450 resources) lack defined 'Owner' or 'CostCenter' tags. This prevents effective lifecycle management and incident response, as no accountable party is designated for these assets within the ISMS."

The Remediation Strategy (The Consultant's Value):
You must propose a fix. The remediation is not just "add tags manually"—that is reactive. The remediation is systemic:

1. **Policy Definition:** Define a standard naming and tagging convention (e.g., *Standard-001: Cloud Resource Tagging*).
2. **Automated Enforcement:** Implement an **Azure Policy** with a "Deny" or "Modify" effect. This ensures that no resource can be deployed in the future unless the "Owner" tag is present.[10]
3. **Remediation Task:** Use the KQL output to generate a "To-Do" list for the engineering teams to retroactively tag the 450 orphaned resources.

2.4 Resume Bullets for Project 1

- **Engineered a dynamic 'Master Asset Inventory' utilizing Azure Resource Graph and KQL**, bridging the visibility gap between static CMDBs and live cloud infrastructure to satisfy **ISO 27001 Annex A 5.9**.
- **Conducted a programmatic audit of asset ownership**, identifying and driving remediation for 450+ unclassified cloud resources, reducing "Shadow IT" risk by 23% across the estate.
- **Implemented 'Policy-as-Code' governance**, designing Azure Policies to enforce mandatory tagging (Owner, CostCenter) at the deployment stage, ensuring continuous compliance with asset management standards.

---

3. Project 2: Conduct a 'Cloud Security Posture' Audit

(Annex A 5.23 & 8.20)

3.1 The Theoretical Framework: ISO 27001 Annex A 5.23 & 8.20

This project focuses on the security of the infrastructure itself, dealing with the unique risks of the cloud supply chain and the logical network perimeter.

Annex A 5.23: Information Security for Use of Cloud Services
This is a new control introduced in the 2022 revision of ISO 27001. It explicitly requires organizations to "specify and manage information security for the use of cloud services".14 This acknowledges the Shared Responsibility Model. The organization cannot simply outsource risk to Microsoft or AWS. The control mandates that the organization defines security requirements for the acquisition, use, management, and exit of cloud services.15

- *Key Insight:* Using a cloud service without configuring its security features (e.g., leaving a Storage Bucket public) is a violation of A.5.23 because the organization failed to "manage" the security of the service.[16]

Annex A 8.20: Networks Security
This control requires that "Networks and network devices should be secured, managed and controlled" to protect information systems.17 In an on-premise world, this meant firewalls and switches. In the cloud, this means Virtual Networks (VNETs) and Network Security Groups (NSGs).19

- *Key Insight:* The most common failure in A.8.20 is the exposure of management interfaces (RDP port 3389 and SSH port 22) to the public internet. This allows attackers to brute-force administrative credentials.[20]

3.2 The "View ALL" Simulation: Auditing the Logical Perimeter

In this phase, the auditor validates whether the organization is upholding its end of the Shared Responsibility Model. We will focus on the "Front Door"—the network ingress points.

Step 1: Auditing Network Security Groups (NSGs)

An NSG acts as a virtual firewall for specific subnets or network interfaces. A "lazy" administrator often creates a rule allowing "Any" traffic from "Any" source to port 22 or 3389 to make it easier to log in from home. This is a critical vulnerability.

We will use KQL to "explode" the complex JSON structure of NSG rules and hunt for these exposures. Note the use of mv-expand—this command is crucial because a single NSG contains a *list* of rules, and we need to evaluate each rule individually.[22]

KQL Query 4: The "Open Management Ports" Hunter

Code snippet

```
Resources

| where type =~ "microsoft.network/networksecuritygroups"
| mv-expand securityRules = properties.securityRules
| where securityRules.properties.access == "Allow"
   and securityRules.properties.direction == "Inbound"
   and (
      securityRules.properties.destinationPortRange == "22" or
      securityRules.properties.destinationPortRange == "3389" or
      securityRules.properties.destinationPortRange == "*"
   )
   and (
      securityRules.properties.sourceAddressPrefix == "*" or
      securityRules.properties.sourceAddressPrefix == "Internet"
   )

| project
   NSG_Name = name,
   Rule_Name = securityRules.name,
   Port = securityRules.properties.destinationPortRange,
   Source = securityRules.properties.sourceAddressPrefix,
   ResourceGroup = resourceGroup,
   Location = location

| order by NSG_Name asc
```

- **Logic:**
  - mv-expand: Converts the array of rules into separate rows so we can filter them.
  - destinationPortRange: Targets SSH (22), RDP (3389), or All ports (*).
  - sourceAddressPrefix: Targets rules that allow traffic from *Anywhere* ("*") or the explicit "Internet" tag.
- **Audit Finding:** Any result here is a "Red Flag." It directly contradicts **Annex A 8.20** requirements to "segregate networks" and "restrict access".[17]

Step 2: Validating Cloud Service Configuration (Storage Accounts)

Under **Annex A 5.23**, we must secure the *use* of services. A common failure is allowing unencrypted HTTP traffic to Storage Accounts.

KQL Query 5: Secure Transfer Audit

```
Code snippet

Resources

| where type =~ "microsoft.storage/storageaccounts"
| where properties.supportsHttpsTrafficOnly == false
| project Name = name, ResourceGroup = resourceGroup, HttpsOnly =
properties.supportsHttpsTrafficOnly
```

- **Logic:** This identifies storage accounts that accept insecure HTTP connections, violating the principle of confidentiality.[23]

3.3 Audit Findings and Strategic Remediation

The Finding:

> "The Cloud Security Posture Audit identified critical vulnerabilities in the network perimeter, constituting a **Major Non-Conformity with Annex A 8.20 (Networks Security)**. Specifically, seven (7) Network Security Groups contain active inbound rules permitting unrestricted access (0.0.0.0/0) to administrative ports (SSH/RDP). This configuration exposes the environment to immediate brute-force and ransomware attacks. Additionally, the audit found gaps in **Annex A 5.23**, with multiple storage accounts lacking enforced HTTPS transport encryption."

The Remediation Strategy:

1. **Immediate Mitigation:** Disable the offending NSG rules immediately.
2. **Architecture Change:** Deploy **Azure Bastion** or **Just-In-Time (JIT)** VM Access. This allows administrators to access VMs securely via the Azure Portal (over HTTPS/443) without exposing the VM's ports to the public internet.[20]
3. **Process Integration:** Update the "Cloud Deployment Standard" to mandate the use of Bastion hosts for all management access.

3.4 Resume Bullets for Project 2

- **Led a 'Cloud Security Posture' audit simulating Second-Party verification**, identifying and remediating critical network exposures to ensure compliance with **ISO 27001 Annex A 8.20** and **A.5.23**.
- **Utilized advanced KQL (mv-expand) to audit Network Security Group (NSG)**

configurations, detecting illicit unrestricted ingress rules (SSH/RDP) across a multi-region Azure environment.
- **Designed and implemented a 'Secure Administrative Access' architecture**, replacing high-risk public IP exposures with **Azure Bastion** and **JIT Access**, significantly reducing the external attack surface.

---

4. Project 3: Financial Governance / Cost Optimization Audit (Clause 9.3)

4.1 The Theoretical Framework: ISO 27001 Clause 9.3

This project represents a sophisticated pivot in the GRC skillset: connecting security hygiene to financial performance. This is where you earn the trust of the C-Suite.

ISO 27001 Clause 9.3: Management Review
This clause requires top management to review the ISMS at planned intervals to ensure its "continuing suitability, adequacy and effectiveness".25
- **Suitability:** Is the ISMS fitting for the business?
- **Adequacy:** Are resources (people, budget, tools) sufficient?.[26]
- **Effectiveness:** Is it achieving its goals?

The "Waste is Risk" Hypothesis:
In a cloud environment, financial waste is almost always a symptom of poor governance.
- An **Orphaned Disk** (a managed disk not attached to any VM) is a cost leak. But it is *also* a security risk: What data is on it? Who is patching it? (No one, because it's not attached). Is it encrypted?.[5]
- An **Unassociated Public IP** is a cost leak. It is *also* a security risk: It represents an unused entry point that could be hijacked if a new resource inadvertently claims it.[27]

By identifying this waste, the auditor provides evidence that the organization is failing to **"Manage Assets" (A.5.9)** and is inefficient in its **"Use of Cloud Services" (A.5.23)**, thereby failing the **"Adequacy and Effectiveness"** test of **Clause 9.3**.[28]

4.2 The "View ALL" Simulation: Hunting for Governance Failures

Step 1: Identifying Orphaned Disks

When a Virtual Machine is deleted in Azure, the associated disk is *not* deleted by default (to prevent accidental data loss). If the administrator is lazy or the script is poor, the disk remains. It sits there, incurring monthly storage costs, often containing sensitive data.[5]

KQL Query 6: The Orphaned Disk Hunter

Code snippet

```
Resources

| where type =~ "microsoft.compute/disks"
| extend DiskState = tostring(properties.diskState)
| where managedBy == "" or DiskState == 'Unattached'
| project
    DiskName = name,
    SizeGB = properties.diskSizeGB,
    DiskState,
    Sku = sku.name,
    ResourceGroup = resourceGroup,
    Location = location,
    TimeCreated = properties.timeCreated

| order by SizeGB desc
```

- **Logic:**
  - managedBy == "": This field is empty if the disk is not currently "managed" (mounted) by a VM.[5]
  - DiskState == 'Unattached': An explicit status flag.[8]
- **Audit Finding:** "Detected 45 Orphaned Disks totaling 12TB of unmanaged storage."

Step 2: Identifying Unassociated Public IPs

Similar to disks, Public IPs can be left behind. These are distinct resources in Azure.

KQL Query 7: The Loose IP Hunter

Code snippet

```
Resources

| where type =~ "microsoft.network/publicipaddresses"
| where isempty(properties.ipConfiguration)
| project
```

```
  IP_Name = name,
  IP_Address = properties.ipAddress,
  Location = location,
  ResourceGroup = resourceGroup,
  Sku = sku.name
```

- **Logic:** properties.ipConfiguration links the IP to a Network Interface Card (NIC). If this property is empty, the IP leads nowhere.[29]

4.3 Audit Findings and Strategic Remediation

This audit culminates in a **Management Review Input Report**. This is different from a technical bug ticket. It speaks the language of business.

The Finding (Executive Summary Style):

> "The Q4 Financial Governance Audit, conducted as part of the Clause 9.3 Management Review, identified significant inefficiencies in Asset Lifecycle Management. The audit revealed **$15,000/year in annualized waste** attributed to 'Orphaned' resources (45 unattached disks and 12 unused Public IPs).
>
> **Governance Implication:** This waste indicates a breakdown in the Decommissioning Process (Annex A 8.10 - Information Deletion). These assets are currently unmonitored, unpatched, and represent 'Shadow Data' repositories that persist outside of the active security perimeter."

The Remediation Strategy:

1. **Process Update:** Revise the "Server Decommissioning Checklist" to explicitly require the deletion of associated disks and IPs.
2. **Automated Cleanup:** Implement an Azure Logic App or Automation Account script that runs weekly to identify and (after a retention period) delete orphaned resources.
3. **Governance Metric:** Establish "Cloud Waste ($)" as a Key Performance Indicator (KPI) for the Infrastructure Team in the next Management Review cycle.

4.4 Resume Bullets for Project 3

- **Executed a 'Financial Governance & Cost Optimization' audit aligned with ISO 27001 Clause 9.3**, utilizing KQL to identify and remediate 'Orphaned' cloud resources, resulting in a 15% reduction in unnecessary cloud spend.
- **Bridged the gap between Security and Finance** by framing 'Cloud Waste' as a governance failure and security risk (Shadow Data), successfully advocating for tighter Asset Lifecycle controls.
- **Delivered data-driven Management Review inputs**, quantifying the financial impact of non-compliance and demonstrating the ROI of robust Information Security governance.

---

5. Project 4: Technical GRC: Use KQL for Data Sovereignty Checks

5.1 The Theoretical Framework: Data Sovereignty

Data Sovereignty is the concept that data is subject to the laws of the nation in which it is physically stored. This is a critical component of **Compliance with legal and contractual requirements (Annex A 5.31)** and **Understanding the needs of interested parties (Clause 4.2)**.

- **GDPR (Europe):** Restricts the transfer of personal data outside the EU/EEA unless specific safeguards are in place.
- **Federal/Government:** Often mandates data stays within specific government cloud regions.
- **Client Contracts:** A client may stipulate "My data must stay in Australia."

If a developer inadvertently deploys a database in "East US" instead of "West Europe," the organization may be in breach of contract or law. Manual auditing of thousands of resources for geolocation is impossible. Technical GRC automation is the only solution.

5.2 The "View ALL" Simulation: Geolocation & Encryption Auditing

Step 1: Auditing Resource Location

We will use KQL to summarize the physical location of all resources and identify outliers.

KQL Query 8: The Sovereignty Enforcer

Code snippet

```
Resources
| summarize ResourceCount = count() by location
| order by ResourceCount desc
```

- **Logic:** This provides a high-level heatmap. If you expect 100% of resources to be in westeurope and you see 5 resources in southeastasia, you have an anomaly.[6]

KQL Query 9: The Violation Hunter
This query is specific. It defines an "Allowed List" and returns anything that defies it.

Code snippet

```
let AllowedRegions = dynamic(["westeurope", "northeurope"]);
Resources

| where location!in (AllowedRegions)
| where type!has "trafficmanager" // Exclude global services that have no specific region
| project
    ResourceName = name,
    Type = type,
    Location = location,
    ResourceGroup = resourceGroup,
    Tags = tags

| order by Location asc
```

- **Logic:**
  - dynamic(["..."]): Creates an array of permitted values.
  - !in: The "Not In" operator filters for violations.
  - !has "trafficmanager": Filters out "Global" resources (like Azure Traffic Manager or Azure DNS) which technically have "global" as a location and would otherwise trigger false positives.

Step 2: Validating Encryption Sovereignty (PMK vs. CMK)

Data sovereignty often extends to *who holds the keys*. For highly sensitive data, regulations may require **Customer Managed Keys (CMK)** rather than default **Platform Managed Keys (PMK)**. CMK ensures that even the cloud provider cannot access the data.[30]

KQL Query 10: Encryption Key Type Audit

Code snippet

```
Resources

| where type =~ "microsoft.compute/disks"
| extend EncryptionType = tostring(properties.encryption.type)
```

```
| project
    DiskName = name,
    EncryptionType,
    Location = location,
    ResourceGroup = resourceGroup

| summarize count() by EncryptionType
```

- **Logic:**
    - properties.encryption.type: Returns values like EncryptionAtRestWithPlatformKey (PMK) or EncryptionAtRestWithCustomerKey (CMK).[32]
- **Audit Finding:** If the policy mandates CMK for the "Finance" resource group, and this query returns "PlatformKey," you have a finding.

5.3 Audit Findings and Strategic Remediation

The Finding:

> "The Data Sovereignty Audit identified a **Critical Non-Conformity regarding Legal Requirements (Clause 4.2)**. Five (5) SQL Database instances containing Customer PII were identified in the 'Southeast Asia' region, violating the 'EU-Only' data residency clause in the Master Service Agreement (MSA) with key European clients. Additionally, the audit found that the 'High Assurance' HR database is encrypted with standard Platform Managed Keys (PMK), failing to meet the Customer Managed Key (CMK) requirement defined in the internal Encryption Policy."

The Remediation Strategy:

1. **Immediate Migration:** Initiate a "Resource Move" or "Backup/Restore" operation to migrate the SQL instances to the West Europe region.
2. **Azure Policy (Deny):** Implement a "Allowed Locations" policy at the Subscription level. This will block any future attempt to deploy resources outside of the approved list (e.g., block 'Southeast Asia').[33]
3. **Key Rotation:** Re-deploy the HR database disk encryption sets to utilize Key Vault-backed Customer Managed Keys.

5.4 Resume Bullets for Project 4

- **Engineered automated Data Sovereignty validation protocols** utilizing KQL and Azure Resource Graph, ensuring 100% adherence to **GDPR** and regional data residency requirements across a multi-national cloud footprint.
- **Developed technical audit scripts to verify encryption standards (PMK vs. CMK)**, providing assurance for high-security data enclaves and meeting strict regulatory compliance targets.

- **Transformed 'Legal Requirements' (Clause 4.2) into code-based governance checks**, utilizing Azure Policy to enforce geolocation boundaries and reduce the risk of cross-border compliance breaches.

---

6. Audit Artifacts & Deliverables

To complete your portfolio, you must generate the artifacts that a real auditor would produce. Below are templates and structures for the **Non-Conformity Report (NCR)** and the **Executive Summary**.

6.1 The Non-Conformity Report (NCR) Template

An NCR is the formal record of a failure. It must be structured, factual, and reference the specific requirement.[33]

Field	Content
NCR ID	NCR-2025-04-A
Date	2025-01-04
Auditor	, Lead GRC Architect
Area	Cloud Infrastructure / Network Security
ISO 27001 Control	**Annex A 8.20 (Networks Security)**
Requirement	"Networks and network devices should be secured, managed and controlled to protect information in systems and applications." [17]
Non-Conformity Description	Technical audit via KQL identified 7 Network Security Groups (NSGs) with Inbound Allow rules for ports 22 (SSH) and 3389 (RDP) from Source 0.0.0.0/0 (Any). This allows unrestricted public access to management interfaces.

Evidence	Evidence_File_A820_NSG_Export.csv (Sanitized) - See attached KQL Query output.
Severity	**Major** (Direct external exposure of administrative interfaces)
Root Cause	Lack of "Secure by Design" templates; Administrators prioritizing convenience over security during remote work setup.
Proposed Correction	Disable rules immediately. Implement Azure Bastion.
Target Date	2025-01-05 (24 Hours)
Status	Open

6.2 The Executive Summary Report

The Executive Summary is for the C-Suite. It must be concise (1-2 pages), focused on risk and money, and free of jargon.[36]

Title: Second-Party Audit of Cloud Infrastructure Governance
Date: January 4, 2025
To: Chief Information Security Officer (CISO), Chief Financial Officer (CFO)
1. Executive Overview
This report details the findings of the Second-Party Audit Simulation conducted on the Azure Production Environment. The audit utilized "View ALL" access to programmatically verify alignment with ISO 27001:2022. The assessment focused on Asset Management, Network Security, Financial Governance, and Data Sovereignty.
2. Key Findings

- **Asset Management (A.5.9):** The automated discovery identified a **23% gap** between the documented asset inventory and the actual cloud environment. 450 resources lack defined ownership, creating significant "Shadow IT" risk.
- **Security Posture (A.8.20): Critical Network Exposures** were detected. Seven (7) administrative interfaces are exposed to the public internet, representing an immediate ransomware vector.
- **Financial Governance (Clause 9.3):** The audit identified **$15,000 in annualized waste** due to orphaned storage and IPs, highlighting a failure in decommissioning processes.
- **Compliance (Clause 4.2):** Data Sovereignty violations were detected, with client data

residing in unapproved regions (Southeast Asia), posing a potential contractual breach.

3. Strategic Recommendations

1. **Automate Governance:** Move from manual spreadsheets to **Azure Policy** enforcement for Tagging and Location restrictions.
2. **Close the Perimeter:** Mandate the use of **Azure Bastion** and remove all public management ports immediately.
3. **Optimize Spend:** Initiate a "Spring Cleaning" project to reclaim the identified $15,000 waste and reinvest it in security tooling.

4. Conclusion
While the organization has established policies, the technical implementation drifts significantly from these standards. The recommendation is to transition to a "Policy-as-Code" model to ensure that the infrastructure remains compliant by design.

---

7. Ethical Note: Redaction and Portfolio Presentation

When you build this portfolio, you are simulating a "View ALL" audit. If you perform this on a real environment (your employer's or a client's), you will see sensitive data (IP addresses, resource names, financial costs).

Strict Adherence to Confidentiality:
It is critical that you never publish raw data in your public portfolio (GitHub, LinkedIn, Blog). You must sanitize your artifacts.10
Redaction Checklist:

1. **Subscription IDs:** Replace a1b2-c3d4-e5f6... with 0000-0000-0000-0000.
2. **Resource Names:** Rename Server-Finance-Prod-01 to VM-App-01 or ``.
3. **IP Addresses:** Replace real public IPs with private range examples like 10.0.0.1 or generic 1.2.3.4.
4. **Company Names:** Use fictional entities like "Contoso," "Fabrikam," or "NexusCorp."

Portfolio Disclaimer:
Include this note in your repository or document:

> *"Note: This project is a simulation based on real-world audit methodologies. All data, configuration examples, and infrastructure artifacts presented here have been generated in a sandbox environment or fully sanitized to remove proprietary information, strictly adhering to ethical confidentiality standards."*

---

8. Conclusion

By completing these four projects, you have effectively simulated the responsibilities of a **GRC Architect** and **Lead Auditor**. You have moved beyond the passive "checking of boxes" to the active "interrogation of reality."

You have demonstrated that you can:

1. **Discover** the truth of an environment using **KQL** (Project 1).
2. **Validate** the security of the perimeter (Project 2).
3. **Optimize** the business value of the ISMS (Project 3).
4. **Enforce** complex legal requirements through code (Project 4).

This portfolio proves that you possess the nuanced, "Second-Party" perspective required to lead in the modern GRC landscape—a landscape where technical verification is the only acceptable form of assurance.

Works cited

1. ISO 27001:2022 - Control 5.9 - Inventory Of Information And Other Associated Assets, accessed January 4, 2026, https://iso-docs.com/blogs/iso-27001-2022-standard/iso-27001-2022-control-5-9-inventory-of-information-and-other-associated-assets
2. ISO 27001 Annex A 5.9 Inventory Of Information And Other Associated Assets Ultimate Guide - High Table, accessed January 4, 2026, https://hightable.io/iso-27001-annex-a-5-9-inventory-of-information-and-other-associated-assets/
3. ISO 27001:2022 Annex A Control 5.9 Explained - ISMS.online, accessed January 4, 2026, https://www.isms.online/iso-27001/annex-a-2022/5-9-inventory-of-information-other-associated-assets-2022/
4. ISO 27001:2022 Annex A Control 5.9: Inventory of Information and Other Associated Assets, accessed January 4, 2026, https://www.hicomply.com/hub/iso-27001-annex-a-5-9-inventory-of-information-other-associated-assets
5. Find Orphaned Azure Resources - Cloud, Systems Management and Automation -, accessed January 4, 2026, https://www.cloudsma.com/2021/02/find-orphaned-azure-resources/
6. Understanding the Azure Resource Graph query language - Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/governance/resource-graph/concepts/query-language
7. View and filter Azure resource information - Azure portal | Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/azure-portal/manage-filter-resource-views
8. Find and delete unattached Azure managed and unmanaged disks - Azure portal, accessed January 4, 2026,

https://learn.microsoft.com/en-us/azure/virtual-machines/disks-find-unattached-portal
9. ISO 27001:2022 Annex A 5.9 - Inventory Of Information And Other Associated Assets Explained - YouTube, accessed January 4, 2026, https://www.youtube.com/watch?v=YeeYsEu5PGg
10. azure - Query resources in resource groups where tags are missing ..., accessed January 4, 2026, https://stackoverflow.com/questions/79184599/query-resources-in-resource-groups-where-tags-are-missing
11. Essential KQL Queries for Azure with and without Log Analytics | AzureIs.Fun, accessed January 4, 2026, https://azureis.fun/posts/Essential-KQL-Queries-for-Azure-with-and-without-Log-Analytics/
12. summarize operator - Kusto | Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/kusto/query/summarize-operator?view=microsoft-fabric
13. Advanced Resource Graph query samples - Azure - Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/governance/resource-graph/samples/advanced
14. ISO 27001:2022 Annex A Control 5.23 Explained - ISMS.online, accessed January 4, 2026, https://www.isms.online/iso-27001/annex-a-2022/5-23-information-security-use-of-cloud-services-2022/
15. ISO 27001 Annex A 5.23 Information Security For Use Of Cloud Services Ultimate Guide, accessed January 4, 2026, https://hightable.io/iso-27001-annex-a-5-23-information-security-for-use-of-cloud-services/
16. ISO 27001:2022 - Control 5.23 - Information Security For Use Of Cloud Services, accessed January 4, 2026, https://iso-docs.com/blogs/iso-27001-2022-standard/iso-27001-2022-control-5-23-information-security-for-use-of-cloud-services
17. ISO 27001:2022 Annex A 8.20 – Network Security - ISMS.online, accessed January 4, 2026, https://www.isms.online/iso-27001/annex-a-2022/8-20-network-security-2022/
18. ISO 27001 Annex A 8.20 Network Security Ultimate Guide - High Table, accessed January 4, 2026, https://hightable.io/iso27001-annex-a-8-20-network-security/
19. Practical Advice for Locking Down the Network with ISO 27001 Controls A.8.20–A.8.22, accessed January 4, 2026, https://www.dqsglobal.com/en/explore/blog/practical-advice-for-locking-down-the-network-with-iso-27001-controls-a.8.20%E2%80%93a.8.22
20. Working with VMs and NSGs in Azure Bastion | Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/bastion/bastion-nsg
21. ISO 27001:2022 Annex A 8.20 - Network Security Explained - YouTube, accessed January 4, 2026, https://www.youtube.com/watch?v=migP5c6o3pk

22. 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/
23. Resource Graph Explorer - KQL queries for Azure APP services - null values - Microsoft Q&A, accessed January 4, 2026, https://learn.microsoft.com/en-us/answers/questions/1274882/resource-graph-explorer-kql-queries-for-azure-app
24. Tutorial: Filter network traffic with a network security group (NSG) - Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic
25. How to Implement ISO 27001:2022 Clause – 9.3 Management Review - ISMS.online, accessed January 4, 2026, https://www.isms.online/iso-27001/requirements-2022/how-to-implement-iso-27001-2022-clause-9-3-management-review/
26. ISO 27001:2022 Clause 9.3 - Management Review Explained - High Table, accessed January 4, 2026, https://hightable.io/iso-27001-clause-9-3-management-reviews-essential-guide/
27. Find and Delete Orphaned Public IP addresses in Azure Portal - GeeksforGeeks, accessed January 4, 2026, https://www.geeksforgeeks.org/devops/microsoft-azure-find-and-delete-orphaned-public-ip-addresses-in-azure-portal/
28. ISO 27001 Management Reviews: Both Misunderstood & Underappreciated - Intertec Blog, accessed January 4, 2026, https://blog.intertecintl.com/your-iso-27001-management-review-is-both-misunderstood-and-underappreciated
29. Find unassociate public IP Azure - Stack Overflow, accessed January 4, 2026, https://stackoverflow.com/questions/71527364/find-unassociate-public-ip-azure
30. Overview of Key Management in Azure | Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/security/fundamentals/key-management
31. Overview of managed disk encryption options - Azure Virtual Machines | Microsoft Learn, accessed January 4, 2026, https://learn.microsoft.com/en-us/azure/virtual-machines/disk-encryption-overview
32. Azure Resource Graph Explorer - How to query Disk Encryption for ..., accessed January 4, 2026, https://learn.microsoft.com/en-us/answers/questions/1159725/azure-resource-graph-explorer-how-to-query-disk-en
33. How to write a nonconformity report to meet ISO standards - Bywater Training, accessed January 4, 2026, https://www.bywater.co.uk/resources/how-should-a-nonconformity-report-be-structured/
34. Nonconformance Report (NCR): Definition, Example, and Process - SimplerQMS,

accessed January 4, 2026, https://simplerqms.com/non-conformance-report/
35. ISO 27001 Audit Non-Conformity Report Template, accessed January 4, 2026, https://iso-docs.com/blogs/iso-27001-isms/iso-27001-2022-audit-non-conformity-template
36. Executive summary: How to write one (with a template) - Diligent, accessed January 4, 2026, https://www.diligent.com/resources/blog/executive-summary-report
37. How to Write a Proposal Executive Summary (Free Template) - Loopio, accessed January 4, 2026, https://loopio.com/blog/proposal-executive-summary/
38. Example Executive Summaries With Templates | Smartsheet, accessed January 4, 2026, https://www.smartsheet.com/content/executive-summary-examples