

## Part I – Governance and Framework

---

### 1 . Executive Summary

The **Barborawy Azure Cloud Compliance Handbook** defines the governance and technical structures required to maintain continuous compliance with:

- **PCI DSS 4.0** – cardholder-data protection
- **EU GDPR (2016/679)** – data privacy and lawful processing
- **Swiss revDSG (2023)** – Swiss Federal Data Protection Act
- **ISO 27001:2022 / NIST SP 800-53 Rev 5** – information-security management frameworks

The handbook ensures all Azure-based workloads operated or managed by Barborawy meet or exceed regulatory requirements by using **Azure-native governance tooling**—Policy, Blueprints, Defender for Cloud, Sentinel, Purview, and Compliance Manager.

---

### 2 . Purpose and Scope

#### Purpose

This framework:

- Establishes a single authoritative source for Barborawy’s Azure compliance requirements.
- Defines how regulatory, contractual, and industry controls are implemented within Azure.
- Aligns corporate risk appetite with cloud-security baselines.
- Ensures consistent configuration, monitoring, and evidence collection across all subscriptions.

#### Scope

Applies to:

- All Azure subscriptions and management groups owned or managed by Barborawy.
- All workloads processing **Cardholder Data (CHD)** or **Personal Data (PD)** of EU or Swiss residents.
- All contractors, subsidiaries, or managed-service providers granted Azure access.

- All supporting infrastructure connected to the CDE or PD environment.
- 

### 3 . Regulatory Context

| <b>Regulation</b>            | <b>Primary Objective</b>                           | <b>Enforcement Body</b>                                      | <b>Key Azure Relevance</b>                         |
|------------------------------|--|--|--|
| <b>PCI DSS v4.0</b>          | Secure processing of card data                     | PCI Security Standards Council                               | Encryption, network segmentation, audit logging    |
| <b>EU GDPR</b>               | Lawful and transparent processing of personal data | European Data Protection Authorities                         | Data minimization, breach reporting, access rights |
| <b>Swiss revDSG (2023)</b>   | Privacy by Design & Cross-border data protection   | FDPIC – Federal Data Protection and Information Commissioner | Data sovereignty (CH/EU), breach notification      |
| <b>ISO 27001/NIST 800-53</b> | Security management and control standardization    | Voluntary / audit based                                      | Policy structure and risk management alignment     |

---

### 4 . Governance Objectives

1. **Unified Compliance Model** – integrate all regulations into one Azure policy baseline.
  2. **Automation First** – use Policy, Defender for Cloud, and Logic Apps to reduce manual auditing.
  3. **Evidence Readiness** – continuous export of compliance data to immutable storage.
  4. **Risk Transparency** – visible metrics on risk posture and regulatory gaps.
  5. **Continuous Improvement** – quarterly review and revision of controls.
- 

### 5 . Shared Responsibility Model (Azure)

| <b>Layer</b>            | <b>Microsoft Responsibility</b>       | <b>Barborawy Responsibility</b>              |
|-------------------------|---------------------------------------|--|
| Physical Infrastructure | Datacenter security, redundancy       | —  |
| Network                 | Hypervisor firewall, routing security | NSG, Azure Firewall, subnet isolation        |
| Platform Services       | PaaS patching, host OS security       | App hardening, connection policies           |
| Identity                | Entra ID availability & resilience    | RBAC, MFA, Conditional Access                |
| Data                    | Encryption features availability      | Key management, classification, retention    |
| Governance              | Compliance tooling                    | Policy assignment, reporting, audit response |

## 6 . Barborawy Governance Structure

| <b>Role</b>                                      | <b>Responsibility</b>                                 |
|--|---|
| <b>Board of Directors / CEO</b>                  | Approve policy framework; receive compliance reports  |
| <b>Chief Information Security Officer (CISO)</b> | Maintain strategy, ensure regulatory alignment        |
| <b>Cloud Governance Board</b>                    | Approve Azure policies, review metrics quarterly      |
| <b>Compliance Officer (DPO)</b>                  | Manage GDPR / revDSG matters and breach notifications |
| <b>Cloud Security Architect</b>                  | Design Azure compliant architectures                  |
| <b>Azure Administrators</b>                      | Implement Policy, RBAC, logging controls              |
| <b>Internal Audit</b>                            | Verify control effectiveness and evidence             |
| <b>Third-Party Providers</b>                     | Adhere to Barborawy's contractual compliance clauses  |

## 7 . RACI Matrix

| Activity               | CISO DPO Cloud Architect Admin Audit |   |   |   |   |  |
|------------------------|--------------------------------------|---|---|---|---|--|
|                        | A                                    | C | C | I | I |  |
| Define Policies        | A                                    | C | C | I | I |  |
| Approve Policies       | A                                    | R | C | I | I |  |
| Implement Azure Policy | I                                    | C | R | A | I |  |
| Manage Key Vaults      | I                                    | C | A | R | I |  |
| Identity Access Review | I                                    | A | C | R | C |  |
| Report Compliance      | A                                    | R | C | I | C |  |
| Incident Management    | A                                    | R | C | R | I |  |

---

## 8 . Compliance Principles

- Lawfulness & Transparency** – processing of data shall be lawful and traceable.
  - Least Privilege** – access granted strictly per role.
  - Data Minimization** – store only necessary data for defined purposes.
  - Encryption & Integrity** – all data at rest and in transit encrypted via approved keys.
  - Privacy by Design** – secure configuration embedded into deployment templates.
  - Auditability** – all security events and changes recorded and retained  $\geq 12$  months.
  - Accountability** – management accepts ownership of compliance outcomes.
- 

## 9 . Policy Lifecycle

| Phase            | Description   | Responsible            |
|------------------|---|------------------------|
| <b>Define</b>    | Identify new requirements (PCI/GDPR/revDSG)         | Cloud Governance Board |
| <b>Approve</b>   | Formal sign-off and publication                     | CISO + Board           |
| <b>Implement</b> | Deploy Azure Policy, Blueprints, automation         | Admins                 |
| <b>Monitor</b>   | Review compliance via Defender for Cloud dashboards | Compliance Officer     |

| Phase  | Description                              | Responsible           |
|--------|--|-----------------------|
| Review | Annual update or upon major Azure change | Internal Audit & CISO |

---

## 10 . Risk Management Framework

- Identify Azure services and data flows in scope.
- Evaluate risk per asset (High / Medium / Low).
- Mitigate with Azure controls (NAT gateway, encryption, RBAC).
- Monitor residual risk through Defender for Cloud.
- Record and report quarterly to the Governance Board.

---

## 11 . Data Protection and Privacy Governance

| Principle             | PCI / GDPR / revDSG Reference | Azure Implementation                  |
|-----------------------|-------------------------------|---------------------------------------|
| Data Classification   | GDPR Art 30 revDSG Art 7      | Mandatory Tags: DataCategory, Owner   |
| Encryption at Rest    | PCI Req 3.5                   | Storage Encryption + CMK (Key Vault)  |
| Encryption in Transit | PCI Req 4.1 GDPR Art 32       | TLS 1.2+, HTTPS-only policies         |
| Retention & Deletion  | GDPR Art 17 revDSG Art 6      | Lifecycle Rules + Soft Delete         |
| Data Access Requests  | GDPR Art 15 revDSG Art 25     | Purview + Logic App DSAR Workflow     |
| Cross-Border Transfer | GDPR Art 44 revDSG Art 16     | Allowed Locations Policy (EU/CH only) |

---

## 12 . Incident Response and Notification

- **Detection:** Sentinel alerts & Defender for Cloud incidents.
- **Containment:** Automated Logic App to disable affected identities or VMs.
- **Eradication:** Patch or revoke keys.
- **Recovery:** Validate system integrity post-incident.

- **Notification:**
    - PCI → Notify Acquirer and PCI Council within 72 hours.
    - GDPR → Supervisory Authority ≤ 72 hours.
    - revDSG → FDPIC “as soon as possible.”
- 

## 13 . Training and Awareness

- Annual PCI/GDPR/revDSG training for Azure admins and developers.
  - Quarterly update sessions on Azure security tooling.
  - Evidence of completion maintained 3 years.
- 

## 14 . Governance Tools Overview

| Tool                           | Purpose                                  |
|--------------------------------|--|
| Azure Policy / Initiatives     | Automated control enforcement            |
| Azure Defender for Cloud       | Threat protection + regulatory score     |
| Microsoft Sentinel             | SIEM + SOAR incident management          |
| Azure Purview                  | Data catalog, mapping and classification |
| Compliance Manager             | Task management and audit tracking       |
| Blueprints / Bicep / Terraform | Infrastructure-as-Code governance        |

---

## 15 . Review and Maintenance

- Annual review by CISO and Audit.
- Immediate update after regulatory change (PCI, GDPR, revDSG).
- Archive previous versions ≥ 5 years.

## Part II – Regulatory Integration

---

### 1 . Purpose of the Integration Matrix

Barborawy operates under three mandatory frameworks:

| Framework                  | Primary Objective   | Data Type Affected                   | Azure Relevance                                  |
|----------------------------|---|--------------------------------------|--|
| <b>PCI DSS 4.0</b>         | Protect cardholder data (CHD) and payment systems                     | Payment data (CHD)                   | Encryption, network segmentation, access control |
| <b>GDPR (EU 2016/679)</b>  | Ensure lawful, transparent, and secure processing of personal data    | EU residents, personal data          | Privacy by Design, DSARs, breach notification    |
| <b>Swiss revDSG (2023)</b> | Guarantee privacy and cross-border data protection for Swiss citizens | Swiss personal Data sovereignty data | (CH/EU), FDPIC reporting                         |

This section consolidates overlapping and distinct obligations into unified **Azure controls** that Barborawy must configure, monitor, and evidence.

---

### 2 . Cross-Regulatory Mapping

| Control Category     | PCI DSS v4 Req. | GDPR Articles     | revDSG Articles | Azure Implementation                        |
|----------------------|-----------------|-------------------|-----------------|---|
| Network Security     | 1–2             | 32                | 8               | NSGs, Azure Firewall, Private Endpoints     |
| Data Protection      | 3–4             | 5 (Integrity), 32 | 8, 9            | Key Vault CMK, Storage Encryption, TLS 1.2+ |
|                      |                 | 25                |                 |   |
| Access Control       | 7–9             | (Limitation), 32  | 8               | Entra ID, RBAC, PIM, MFA                    |
|                      |                 |                   |                 |   |
| Logging & Monitoring | 10              | 30 (Records), 33  | 24              | Log Analytics, Sentinel, Defender for Cloud |
| Vulnerability Mgmt   | 6               | 32                | 8               | Defender for Cloud Assessments              |

| <b>Control Category</b> | <b>PCI DSS v4 Req.</b> | <b>GDPR Articles</b> | <b>revDSG Articles</b> | <b>Azure Implementation</b>                   |
|-------------------------|------------------------|----------------------|------------------------|---|
| Breach Response         | 12                     | 33–34                | 24                     | Sentinel Playbooks + Logic Apps notifications |
| Data Subject Rights     | —                      | 12–23                | 25                     | Purview + DSAR Automation Logic App           |
| Data Transfers          | —                      | 44–49                | 16                     | Allowed Locations Policy (EU/CH only)         |
| Privacy by Design       | —                      | 25                   | 8                      | Azure Blueprints & ARM templates hardening    |
| Documentation           | 12                     | 30                   | 27                     | Compliance Manager evidence store             |

### 3 . PCI DSS 4.0 Key Azure Mappings

| <b>PCI Requirement</b>                  | <b>Goal</b>                         | <b>Azure Control</b>                       |
|---|-------------------------------------|--|
| <b>1 – Firewalls &amp; Segmentation</b> | Isolate CDE from untrusted networks | Azure Firewall Premium, NSGs               |
| <b>2 – Secure Configurations</b>        | Remove defaults & harden systems    | Azure Policy Baseline + Defender Benchmark |
| <b>3 – Protect Stored CHD</b>           | Encryption at rest                  | Storage Encryption w/ CMK                  |
| <b>4 – Encrypt Transmission</b>         | Secure transit of CHD               | TLS 1.2+, HTTPS Only Policy                |
| <b>5 – Malware Protection</b>           | Protect systems from malware        | Defender for Endpoint integration          |
| <b>6 – Vulnerability Mgmt</b>           | Patch and scan regularly            | Update Mgmt Center, Defender scans         |
| <b>7 – Access Control</b>               | Restrict CHD access to need-to-know | RBAC + Conditional Access                  |
| <b>8 – User Auth</b>                    | Strong MFA and logging              | Entra ID MFA + Sign-In Logs                |
| <b>9 – Physical Security</b>            | Data center control                 | Handled by Microsoft                       |

| <b>PCI Requirement</b>                 | <b>Goal</b>              | <b>Azure Control</b>                 |
|--|--------------------------|--------------------------------------|
| <b>10 – Logging &amp; Audit Trails</b> | Trace user actions       | Log Analytics + Sentinel             |
| <b>11 – Testing &amp; Scans</b>        | Continuous testing       | Defender Assessments                 |
| <b>12 – Policy Governance</b>          | Maintain security policy | Governance Framework (this document) |

---

#### 4 . GDPR Azure Mappings

| <b>GDPR Article</b> | <b>Requirement</b>                                     | <b>Azure Enforcement Example</b>         |
|---------------------|--|--|
| Art 5               | Principles of processing (data minimization, accuracy) | Mandatory Tags + Data Classification     |
| Art 6               | Lawfulness of processing                               | Document legal basis in Purview Metadata |
| Art 25              | Privacy by Design / Default                            | Blueprint templates w/ secure defaults   |
| Art 30              | Records of processing activities                       | Purview Data Map & Data Catalog          |
| Art 32              | Security of processing                                 | Defender for Cloud + Key Vault           |
| Art 33              | Breach notification 72 h                               | Sentinel Playbook → email to DPO         |
| Art 44–49           | International data transfer rules                      | Allowed Locations Policy (EU/CH)         |
| Art 15–17           | Data Subject Rights (Access, Erasure)                  | DSAR Logic App automation                |

---

#### 5 . Swiss revDSG Azure Mappings

| <b>revDSG Article</b> | <b>Requirement</b> | <b>Azure Implementation</b>         |
|-----------------------|--------------------|-------------------------------------|
| Art 8                 | Privacy by Design  | Azure Blueprints + secure templates |

| <b>revDSG Article</b> | <b>Requirement</b>                  | <b>Azure Implementation</b>                            |
|-----------------------|-------------------------------------|--|
| Art 9                 | Data Processing Security            | Key Vault + Encryption Policy                          |
| Art 16                | Cross-border disclosure             | Allowed Locations Policy (EU/CH)                       |
| Art 24                | Breach Notification to FDPIC        | Sentinel Playbook + Teams Alert                        |
| Art 25                | Data Access and Correction Requests | Purview + Logic App workflow                           |
| Art 27                | Processor Obligations               | Vendor Assessment Reports stored in Compliance Manager |

---

## 6 . ISO 27001 / NIST Alignment

| <b>Control Domain</b>  | <b>ISO 27001 Clause</b> | <b>NIST SP 800-53 Control</b> | <b>Azure Service Mapping</b>   |
|------------------------|-------------------------|-------------------------------|--------------------------------|
| Access Control         | A.9                     | AC-1–AC-6                     | Entra ID, RBAC, PIM            |
| Cryptography           | A.10                    | SC-12                         | Key Vault, Disk Encryption     |
| Logging & Monitoring   | A.12                    | AU-2                          | Log Analytics, Sentinel        |
| Operations Security    | A.12                    | CM-6                          | Defender Recommendations       |
| Supplier Relationships | A.15                    | SR-1                          | Vendor Policy Initiative       |
| Incident Mgmt          | A.16                    | IR-4                          | Sentinel Playbooks             |
| Compliance             | A.18                    | CA-2                          | Compliance Manager Assessments |

---

## 7 . Unified Obligations Matrix

| <b>Requirement Type</b> | <b>Typical Azure Policy/Control</b> | <b>Evidence Source</b>   |
|-------------------------|-------------------------------------|--------------------------|
| Encryption in Transit   | Storage → EnforceHttpsOnly          | Policy Compliance Report |

| Requirement Type           | Typical Azure Policy/Control  | Evidence Source                 |
|----------------------------|-------------------------------|---------------------------------|
| Data at Rest Encryption    | RequireCustomerManagedKeys    | Key Vault Access Logs           |
| Access Restrictions        | AllowedRoleAssignments        | Entra ID Review Export          |
| Data Localization          | AllowedLocations              | Defender Regulatory View        |
| Log Retention $\geq$ 12 mo | DeployDiagnosticSettings      | Log Analytics Retention Config  |
| Breach Reporting           | Sentinel Logic App            | Incident Register + Email Audit |
| DSAR Response              | Purview Workflow              | DSAR Ticket Log                 |
| Vendor Compliance          | Compliance Manager Assessment | Vendor Evidence Folder          |

## 8 . Evidence Collection Requirements

| Regulation | Minimum Retention    | Required Evidence                        | Azure Storage Location          |
|------------|----------------------|--|---------------------------------|
| PCI DSS    | 12 months of logs    | Access logs, Vulnerability reports       | Immutable Blob Storage          |
| GDPR       | 3 years (min)        | DSAR requests, Breach logs, Audit trails | Compliance SharePoint / Purview |
| revDSG     | 5 years recommended  | Consent records, FDPIC reports           | Azure Storage Account WORM      |
| ISO 27001  | Per policy lifecycle | Audit evidence package                   | Compliance Manager Workspace    |

## 9 . Integrated Audit Workflow

1. **Weekly:** Compliance Officer exports Defender for Cloud score.
2. **Monthly:** Azure Admin generates Policy Compliance Report.
3. **Quarterly:** Internal Audit reviews controls per matrix.
4. **Annually:** Independent PCI/GDPR audit.

- 
- 5. **Triggered:** Breach → 72 h notification process (GDPR/DSG).
- 

## 10 . Key Takeaways

- Barborawy's compliance posture spans **three jurisdictions** but can be **automated and unified** in Azure.
  - The **Regulatory Integration Matrix** acts as a **single source of truth** linking legal requirements to specific Azure controls.
  - Evidence generation and retention are built directly into Barborawy's Azure ecosystem.
- 

## End of Part II – Regulatory Integration

---

Would you like me to continue with **Part III – Azure Governance Policies**, which details every governance policy area (Identity, Network, Data, Logging, Backup, Vendor, etc.) and their enforcement in Azure Policy?

**Du:**

235

**ChatGPT:**

Just to clarify — when you say “**235**”, do you mean:

- You want me to **continue with Part III** of the handbook (Azure Governance Policies)?
- Or you are referring to a **specific section, page count, or numbered policy (e.g., Policy #235)**?

If your intent is to **move forward with Part III**, I'll start generating it next — this part contains the full catalogue of Azure governance domains:

1. Identity & Access Control
2. Network Security
3. Data Protection & Encryption
4. Logging & Monitoring
5. Vulnerability & Patch Management
6. Backup & Business Continuity

7. Third-Party & Vendor Governance
8. Tagging & Resource Consistency
9. Incident Response
10. Policy Automation

## **Part III – Azure Governance Policies**

**Scope:** All Barborawy Azure management groups, subscriptions, and resource groups in PCI/GDPR/revDSG scope.

**Assignment:** Default at **Management Group** level; exceptions via documented waivers with CISO/DPO approval.

---

### **1. Identity & Access Control (PCI 7–9, GDPR Art. 25/32, revDSG Art. 8)**

#### **1.1 Objectives**

- Enforce strong authentication, least privilege, just-in-time (JIT) elevation, and full auditability.

#### **1.2 Policy Requirements**

| <b>Control</b>           | <b>Requirement</b>  | <b>Effect</b>                    | <b>Evidence</b>                      |
|--------------------------|---|----------------------------------|--------------------------------------|
| MFA for privileged roles | All Entra directory roles and subscription Owners/Contributors require MFA via Conditional Access | <b>Audit</b> (via CA policy)     | Entra Sign-in logs                   |
| PIM for privileged roles | All high-privilege roles must be <b>eligible</b> (not permanent) with JIT and approval            | <b>Audit / DeployIfNotExists</b> | PIM audit logs                       |
| Least privilege          | No user/group assigned <b>Owner</b> at subscription; only Dedicated Admin Groups allowed          | <b>Deny</b>                      | Role assignments export              |
| Break-glass              | Max 2 emergency accounts w/ exclusions tracked; monitored weekly                                  | <b>Audit</b>                     | Sentinel alert history               |
| Legacy auth              | POP/IMAP/SMTP AUTH disabled tenant-wide   | <b>Audit</b>                     | Entra sign-in logs (legacy events=0) |

#### **1.3 Sample Azure Policy – Limit Subscription Owners**

```
{
  "properties": {
    "displayName": "Limit number of Owner role assignments at subscription",
    "policyType": "Custom",
    "mode": "All",
    "parameters": {
      "maxOwners": { "type": "Integer", "defaultValue": 2 }
    },
    "policyRule": {
      "if": { "field": "type", "equals": "Microsoft.Authorization/roleAssignments" },
      "then": {
        "effect": "AuditIfNotExists",
        "details": {
          "type": "Microsoft.Authorization/roleAssignments",
          "name": "Owner",
          "existenceCondition": {
            "count": {
              "field": "Microsoft.Authorization/roleAssignments/roleDefinitionId",
              "where": { "like": "*//roleDefinitions/*" }
            },
            "lessOrEquals": "[parameters('maxOwners')]"
          }
        }
      }
    }
  }
}
```

## 1.4 Assignment & Verification

- **Assign** initiative “Barborawy-IAM-Baseline” at the **Tenant Root Management Group**.
  - **Verify** quarterly via Access Reviews (export CSV as evidence).
- 

## 2. Network Security & Segmentation (PCI 1–2, GDPR 32, revDSG 8)

### 2.1 Objectives

- Isolate CDE; no public ingress; inspect egress; enable DDoS and full network logging.

### 2.2 Policy Requirements

| Control             | Requirement   | Effect                         | Evidence                        |
|---------------------|---|--------------------------------|---------------------------------|
| NSGs everywhere     | All subnets and NICs must attach NSG                        | <b>Deny</b>                    | Azure Policy compliance         |
| No public IP on CDE | Deny public IPs on NICs in CDE resource groups              | <b>Deny</b>                    | Resource Graph query            |
| Firewall Hub        | Hub-and-Spoke with <b>Azure Firewall Premium</b> and policy | <b>Audit/DeployIfNotExists</b> | Firewall policy state           |
| Private endpoints   | Storage/SQL/Key Vault/AppSvc in CDE must use Private Link   | <b>Deny</b>                    | Diagnostic: Private Link events |
| DDoS Standard       | All prod VNets in scope must enable DDoS Std                | <b>DeployIfNotExists</b>       | DDoS plan association           |
| Flow logs           | NSG flow logs + Traffic Analytics enabled                   | <b>DeployIfNotExists</b>       | LA workspace logs               |

### 2.3 Sample Azure Policy – Deny Public IPs on NICs

```
{
  "properties": {
    "displayName": "Deny public IP assignment to NICs in CDE",
    "mode": "All",
    "parameters": {
      "cdeTag": { "type": "String", "defaultValue": "true" }
    }
  }
}
```

```

    },
    "policyRule": {
        "if": {
            "allOf": [
                { "field": "type", "equals": "Microsoft.Network/networkInterfaces" },
                { "field": "tags.CDE", "equals": "[parameters('cdeTag')]" },
                { "field": "Microsoft.Network/networkInterfaces/ipconfigurations[*].publicIPAddress.id", "exists": "true" }
            ]
        },
        "then": { "effect": "deny" }
    }
}

```

---

### 3. Data Protection & Encryption (PCI 3–4, GDPR 25/32, revDSG 8/9/16)

#### 3.1 Objectives

- CMK-backed encryption, TLS 1.2+, key lifecycle governance, data localization.

#### 3.2 Policy Requirements

| Control  | Requirement  | Effect            | Evidence              |
|--|--|-------------------|-----------------------|
| CMK for critical Disk/DB/Storage with <b>Customer-data</b> | Disk/DB/Storage with <b>Customer-managed Keys</b> in Key Vault | <b>Audit/Deny</b> | KV key references     |
| HTTPS-only   | Storage and App Service require HTTPS/TLS1.2+                  | <b>Deny</b>       | Policy compliance     |
| KV posture   | Soft delete & purge protection <b>required</b>                 | <b>Deny</b>       | KV configuration logs |
| Key rotation   | ≤ 365 days rotation with alerting                              | <b>Audit</b>      | KV key metadata       |

| <b>Control</b>    | <b>Requirement</b>                      | <b>Effect</b> | <b>Evidence</b>               |
|-------------------|---|---------------|-------------------------------|
| Data localization | AllowedLocations: EU/CH only for CDE/PD | <b>Deny</b>   | Region list                   |
| Immutable backups | WORM enabled for backup containers      | <b>Audit</b>  | Storage immutability settings |

### 3.3 Sample Azure Policy – Enforce KV Soft Delete & Purge Protection

```
{
  "properties": {
    "displayName": "Require Key Vault soft delete and purge protection",
    "mode": "Indexed",
    "policyRule": {
      "if": { "field": "type", "equals": "Microsoft.KeyVault/vaults" },
      "then": {
        "effect": "deny",
        "details": [
          { "field": "Microsoft.KeyVault/vaults/enableSoftDelete", "equals": "true" },
          { "field": "Microsoft.KeyVault/vaults/enablePurgeProtection", "equals": "true" }
        ]
      }
    }
  }
}
```

## 4. Logging, Monitoring & Evidence (PCI 10, GDPR 30/33, revDSG 24)

### 4.1 Objectives

- Universal diagnostics, centralized SIEM, immutable evidence, retention ≥ 12 months (PCI), ≥ 3 years (GDPR/revDSG evidence).

### 4.2 Policy Requirements

| Control             | Requirement   | Effect   | Evidence                  |
|---------------------|---|--|---------------------------|
| Diagnostic settings | All supported resources send logs to <b>Log Analytics</b>               | Policy<br><b>DeployIfNotExists</b> remediate history |                           |
| Security center     | <b>Defender for Cloud</b> plan enabled (Servers/SQL/Storage/Containers) | Defender<br><b>DeployIfNotExists</b> coverage export |                           |
| Sentinel            | Each prod subscription joined to <b>Sentinel</b> workspace              | Audit  | Sentinel connection state |
| Retention           | LA retention ≥ 365d; evidence archives 3y                               | Audit  | Workspace config          |
| Change tracking     | AMA + Change Tracking on VMs  | <b>DeployIfNotExists</b>                             | AMA heartbeats            |

#### 4.3 Sample Azure Policy – Deploy Diagnostics to LA

```
{
  "properties": {
    "displayName": "Deploy diagnostic settings to Log Analytics",
    "policyType": "BuiltIn",
    "policyRule": { "...": "Use built-in 'Deploy diagnostic settings to Log Analytics workspace' with parameterized workspaceld" },
    "parameters": { "workspaceld": { "type": "String" } }
  }
}
```

(Use the built-in policy; wrap in an Initiative targeting common resource types.)

### 5. Vulnerability & Patch Management (PCI 6, ISO A.12)

#### 5.1 Objectives

- Continuous assessments, weekly scans, SLA-driven remediation.

#### 5.2 Policy Requirements

| <b>Control</b>       | <b>Requirement</b>                        | <b>Effect</b>            | <b>Evidence</b>            |
|----------------------|---|--------------------------|----------------------------|
| Defender for Servers | MDE/qualifying agent deployed on all VMs  | <b>DeployIfNotExists</b> | Defender inventory         |
| Unsupported OS       | Deny creation of non-supported images     | <b>Deny</b>              | Policy events              |
| Baseline drift       | CIS/Microsoft Baseline deviations audited | <b>Audit</b>             | Defender recommendations   |
| Update management    | Automatic OS updates enabled for prod     | <b>Audit</b>             | Update compliance workbook |
| Container scanning   | ACR image scanning enforced               | <b>DeployIfNotExists</b> | Defender for Containers    |

---

## 6. Backup, DR & Business Continuity (PCI 12.10, GDPR 32)

### 6.1 Objectives

- Encrypted, immutable, geo-redundant backups; tested restores; role-segregated restores.

### 6.2 Policy Requirements

| <b>Control</b>    | <b>Requirement</b>                         | <b>Effect</b>            | <b>Evidence</b>        |
|-------------------|--|--------------------------|------------------------|
| Backup enabled    | Azure Backup on all prod VMs/DBs           | <b>DeployIfNotExists</b> | Recovery Vault reports |
| Backup encryption | CMK or platform encryption verified        | <b>Audit</b>             | Vault/Key references   |
| WORM              | Immutable storage for backup vault exports | <b>Audit</b>             | Storage immutability   |
| Restore tests     | Semi-annual test evidence                  | <b>Audit</b>             | Test runbook exports   |

---

## 7. Third-Party & Vendor Governance (PCI 12.8, GDPR 28/44, revDSG 27)

### 7.1 Objectives

- Only approved marketplace images; processors bound to SCCs/CH adequacy; private connectivity.

## 7.2 Policy Requirements

| Control           | Requirement                                  | Effect       | Evidence                     |
|-------------------|--|--------------|------------------------------|
| Allow-list images | Only approved Marketplace offers             | <b>Deny</b>  | Deployment failures (policy) |
| Private link      | Partner PaaS via Private Endpoint            | <b>Deny</b>  | Private Link state           |
| Data transfer     | Disallow regions outside EU/CH for PD/CDE    | <b>Deny</b>  | Region checks                |
| Vendor evidence   | Compliance docs stored in Compliance Manager | <b>Audit</b> | Assessment snapshots         |

---

## 8. Tagging, Cost & Resource Consistency (ISO A.8, GDPR 5)

### 8.1 Objectives

- Mandatory tags drive automation (data classification, CDE scoping, owner, environment).

### 8.2 Policy Requirements

| Tag          | Description     | Enforcement                          |
|--------------|-----------------|--------------------------------------|
| Owner        | UPN or group ID | <b>Deny</b> create/update if missing |
| DataCategory | `CHD`           | PD                                   |
| Environment  | `Prod`          | Dev                                  |
| CDE          | `true`          | false`                               |

### 8.3 Sample Azure Policy – Require & Restrict Tag Values

```
{  
  "properties": {  
    "displayName": "Require tag 'DataCategory' and restrict values",  
    "mode": "Indexed",  
    "parameters": {  
      "allowed": {  
        "type": "Array",  
        "value": ["CHD"]  
      }  
    }  
  }  
}
```

```

    "defaultValue": ["CHD","PD","Internal","Public"]

}

},

"policyRule": {

  "if": { "field": "tags['DataCategory']", "notIn": "[parameters('allowed')]" },

  "then": { "effect": "deny" }

}

}

```

---

## **9. Incident Response & Breach Notification (PCI 12.10, GDPR 33/34, revDSG 24)**

### **9.1 Objectives**

- Detect, contain, eradicate, and report within statutory timelines; automate notifications.

### **9.2 Policy Requirements**

| <b>Control</b>    | <b>Requirement</b>                               | <b>Effect</b>            | <b>Evidence</b>   |
|-------------------|--|--------------------------|-------------------|
| Security contacts | Security contact at subscription set             | <b>DeployIfNotExists</b> | Sub settings      |
| Sentinel alerts   | Core PCI/GDPR/revDSG alerts deployed             | <b>DeployIfNotExists</b> | Sentinel rules    |
| Breach playbook   | Logic App: notify DPO/FDPIC/Acquirer w/ template | <b>DeployIfNotExists</b> | Logic App runs    |
| Retention         | Incident artifacts retained ≥ 3 years            | <b>Audit</b>             | Storage lifecycle |

---

## **10. Compliance Automation & Reporting (PCI 12, ISO A.18)**

### **10.1 Objectives**

- Unified dashboards, threshold alerts, automated exports to immutable evidence stores.

### **10.2 Policy Requirements**

| Control          | Requirement   | Effect                   | Evidence              |
|------------------|---|--------------------------|-----------------------|
| Regulatory views | Enable PCI DSS 4.0, ISO 27001, NIST, GDPR in Defender for Cloud | <b>DeployIfNotExists</b> | Regulatory blade      |
| Score alerts     | Alert when compliance score < 90%                               | <b>DeployIfNotExists</b> | Logic App runs        |
| Weekly exports   | Export Policy & Defender posture to WORM                        | <b>DeployIfNotExists</b> | Storage logs          |
| Quarterly pack   | Generate audit pack (Resource Graph + Sentinel workbook PDFs)   | <b>Audit</b>             | Evidence folder index |

---

## 11. Initiatives & Assignment Model

- **Initiatives (examples):**
    - Barborawy-PCI-Core: Network, encryption, logging, vulnerability, IR controls.
    - Barborawy-GDPR-revDSG: Data localization, DSAR workflow, breach notification.
    - Barborawy-IAM-Baseline: MFA, PIM, role limits, access reviews.
    - Barborawy-Ops-Foundations: Diagnostics, tagging, SKU/region allow lists.
  - **Hierarchy:**
    - Assign initiatives at **Mgmt Group: /barborawy/root**.
    - Override parameters in child management groups (e.g., Prod, NonProd).
    - Use **policy exemptions** only with: business justification, compensating control, expiry date, and **CISO/DPO sign-off**.
- 

## 12. Testing, Remediation & Rollback

- **Pre-Prod test:** Assign initiatives to a sandbox subscription; validate no false positives.
  - **Remediation:** Prefer **DeployIfNotExists** with modify where supported, else scripted remediation via Azure Automation/Logic Apps.
  - **Rollback:** Keep previous initiative versions; use assignment `nonComplianceMessage` to communicate change windows.
-

### **13. Evidence & KPI Matrix (for this Part)**

| <b>KPI</b>                      | <b>Target Source</b>                  |
|---------------------------------|---------------------------------------|
| % resources with diagnostics    | $\geq 98\%$ Policy compliance         |
| % CDE resources w/ Private Link | 100% Resource Graph                   |
| # Subscription Owners           | $\leq 2$ Role assignment export       |
| Defender coverage in prod       | 100% Defender inventory               |
| Compliance score (PCI)          | $\geq 90\%$ Defender Regulatory blade |

---

### **14. Exception Handling**

- Exceptions must **not** weaken PCI CHD confidentiality/integrity or GDPR/revDSG privacy outcomes without:
  - Documented compensating control,
  - Risk acceptance by CISO,
  - Time-bound expiry ( $\leq 90$  days),
  - Ticket reference and audit trail.

## **Part IV – Technical Implementation**

**Goal:** Stand up and enforce Barborawy's PCI DSS 4.0 + GDPR + revDSG controls using Azure-native services with Infrastructure-as-Code (IaC), automated remediation, centralized evidence, and auditable workflows.

---

### **1) Tenant & Management Group Foundation**

#### **1.1 Structure**

- **/ (Tenant Root)**
  - **/barborawy** (Root MG)
    - **/barborawy-prod**
    - **/barborawy-nonprod**
    - **/barborawy-monitoring** (Sentinel/Log Analytics)
    - **/barborawy-shared** (Hub/Firewall/KeyVault)

#### **1.2 Initial CLI Setup**

```
# Log in  
az login  
  
# Create management groups  
az account management-group create --name barborawy  
az account management-group create --name barborawy-prod --parent barborawy  
az account management-group create --name barborawy-nonprod --parent barborawy  
az account management-group create --name barborawy-monitoring --parent  
barborawy  
az account management-group create --name barborawy-shared --parent barborawy
```

---

### **2) Log Analytics + Microsoft Sentinel (Centralized SIEM)**

#### **2.1 Workspace & Sentinel**

```
# Resource Group for monitoring  
az group create -n rg-monitoring -l westeurope
```

```
# Log Analytics  
az monitor log-analytics workspace create -g rg-monitoring -n law-bbw-prod --retention-time 365
```

```
# Sentinel enablement  
az security sentinel create --resource-group rg-monitoring --workspace-name law-bbw-prod
```

## 2.2 Connect Diagnostic Settings (Policy-Driven)

Assign the built-in initiative: “**Deploy Diagnostic settings to Log Analytics workspace**” scoped to **/barborawy** with parameter workspaceld set to the LAW created above.

---

## 3) Defender for Cloud – Regulatory Compliance & Plans

### 3.1 Enable Plans (Servers, SQL, Storage, Containers)

```
# Enable plan at subscription scope (repeat for all prod subscriptions)  
SUB=<subscription-id>  
  
az security pricing create -n VirtualMachines --subscription $SUB --tier Standard  
az security pricing create -n SqlServers --subscription $SUB --tier Standard  
az security pricing create -n StorageAccounts --subscription $SUB --tier Standard  
az security pricing create -n AppServices --subscription $SUB --tier Standard  
az security pricing create -n KubernetesService --subscription $SUB --tier Standard  
az security pricing create -n ContainerRegistry --subscription $SUB --tier Standard
```

### 3.2 Turn On Regulatory Standards

In Defender > **Regulatory compliance**: enable **PCI DSS 4.0, ISO 27001:2022, NIST SP 800-53 R5**.

(For GDPR/revDSG, use policy/initiative + Compliance Manager tasks.)

---

## 4) Azure Policy – Initiatives & Assignments

### 4.1 Create Barborawy Initiatives (Examples)

- **Barborawy-PCI-Core:** Deny public IPs on NICs in CDE, require Private Endpoints for Storage/SQL/KeyVault, enforce HTTPS-only, require diagnostics, NSG on all subnets/NICs, DDoS Standard.
- **Barborawy-GDPR-revDSG:** AllowedLocations (EU/CH), require DataCategory/Owner tags, storage immutability for evidence, DSAR automation presence (DeployIfNotExists placeholder).
- **Barborawy-IAM-Baseline:** Limit Owners ≤2, enforce PIM (AuditIfNotExists), legacy auth disabled (Audit), access reviews on schedule (informational control).

#### 4.2 Example Initiative (Bicep)

```

param mgId string
param lawId string
param allowedRegions array =
['switzerlandnorth','switzerlandwest','westeurope','northeurope']

resource initiative 'Microsoft.Authorization/policySetDefinitions@2021-06-01' = {
  name: 'Barborawy-PCI-Core'
  properties: {
    displayName: 'Barborawy PCI Core Controls'
    policyDefinitions: [
      // Require HTTPS on Storage
      {
        policyDefinitionId: '/providers/Microsoft.Authorization/policyDefinitions/0c5a8b40-...
...httpsonly' // built-in
        parameters: {}
      }
      // Deny public IP on NIC
      {
        policyDefinitionId: '/providers/Microsoft.Authorization/policyDefinitions/3bde5a0b-...
...denyPublicIpNic'
        parameters: {}
      }
    ]
  }
}

```

```

// Deploy diagnostics to LAW
{
    policyDefinitionId: '/providers/Microsoft.Authorization/policyDefinitions/deploy-
diagnostics'
    parameters: {
        workspaceId: { value: lawId }
    }
}
// Allowed locations
{
    policyDefinitionId: '/providers/Microsoft.Authorization/policyDefinitions/allowed-
locations'
    parameters: {
        listOfAllowedLocations: { value: allowedRegions }
    }
}
]
}
}

resource assign 'Microsoft.Authorization/policyAssignments@2022-06-01' existing = {
    name: 'Barborawy-PCI-Core-Assign'
    scope: tenantResourceId('Microsoft.Management/managementGroups', mgId)
}

```

```

resource assign 'Microsoft.Authorization/policyAssignments@2022-06-01' existing = {
    name: 'Barborawy-PCI-Core-Assign'
    scope: tenantResourceId('Microsoft.Management/managementGroups', mgId)
}

```

#### **4.3 Assignment via CLI**

```

MG=/providers/Microsoft.Management/managementGroups/barborawy-prod
POLICYSET=/providers/Microsoft.Authorization/policySetDefinitions/Barborawy-PCI-
Core
az policy assignment create -n pac-pci-core -d "PCI Core" --policy-set-definition
$POLICYSET --scope $MG \

```

```
--params '{ "workspaceId": { "value": "/subscriptions/<sub>/resourceGroups/rg-monitoring/providers/Microsoft.OperationalInsights/workspaces/law-bbw-prod" } }' \
--location westeurope
```

---

## 5) Hub-Spoke Networking (Firewall, DDoS, Private Link)

### 5.1 Hub (Firewall + DDoS + Bastion)

```
param location string = 'westeurope'
param rg string = 'rg-shared'
param vnetName string = 'vnet-hub'
param firewallName string = 'afw-bbw'
param ddosPlanName string = 'ddos-bbw'
```

```
resource rgRes 'Microsoft.Resources/resourceGroups@2022-09-01' = {
  name: rg
  location: location }
```

```
resource ddos 'Microsoft.Network/ddosProtectionPlans@2022-07-01' = {
  name: ddosPlanName
  location: location
}
```

```
resource vnet 'Microsoft.Network/virtualNetworks@2023-04-01' = {
  name: vnetName
  location: location
  properties: {
    addressSpace: { addressPrefixes: ['10.0.0.0/16'] }
    subnets: [
      { name: 'AzureFirewallSubnet' properties: { addressPrefix: '10.0.0.0/24' } }
      { name: 'AzureBastionSubnet' properties: { addressPrefix: '10.0.1.0/27' } }
      { name: 'shared-services' properties: { addressPrefix: '10.0.2.0/24' } }
    ]
  }
}
```

```
]
  enableDdosProtection: true
  ddosProtectionPlan: { id: ddos.id }
}
}
```

## 5.2 Spokes (CDE / Non-CDE) + Private DNS Zones

- Each spoke VNet peered to hub; deny Internet egress except via **Azure Firewall**.
  - Private endpoints for: **Storage, SQL, Key Vault, App Service**, plus **Private DNS Zones** linked to spokes.
- 

## 6) Key Vault (CMK), Encryption & Secrets Hygiene

### 6.1 Secure Key Vault (CLI)

RG=rg-shared

KV=kv-bbw-cmk

LOC=westeurope

```
az keyvault create -g $RG -n $KV -l $LOC --enable-purge-protection true --enable-soft-delete true --retention-days 90 \
--public-network-access Disabled
```

```
# RBAC (preferred); grant Key Vault Crypto User to workloads via managed identity
```

### 6.2 CMK for Storage/SQL (Examples)

# Storage account with CMK

```
az storage account create -g rg-cde -n stcdebbw01 -l westeurope --https-only true \
--allow-blob-public-access false --min-tls-version TLS1_2 --sku Standard_GRS \
--encryption-key-type-for-blob account
```

```
# Then set CMK with Key Vault key (requires Key Vault and key to exist)
```

### 6.3 Rotation & Monitoring

- Use **Key Rotation policy** in Key Vault (lifecycle rules).

- Alert on near-expiry keys with **Action Groups** -> Teams/Email.
- 

## 7) Identity (Entra ID), PIM, Conditional Access

### 7.1 Conditional Access (High-Level)

- **Policy 1:** Require MFA for all admin roles.
- **Policy 2:** Block legacy auth.
- **Policy 3:** Require compliant device for CDE admin portals.

### 7.2 PIM

- Make all privileged roles **eligible** (not active).
  - Require **MFA + Approval** for activation; **max 8 hours; justification required**.
  - Export **PIM activation logs** weekly to evidence storage (Automation Runbook/Logic App).
- 

## 8) Logging, Retention, and Immutable Evidence

### 8.1 Diagnostic Categories (Minimum)

- **Administrative, Security, Audit, Policy, Bastion, Firewall, KeyVaultAuditEvent, StorageRead/Write/Delete.**

### 8.2 Immutable Evidence Store (WORM)

```
az storage account create -g rg-monitoring -n stbbwEvidence --kind StorageV2 \
--min-tls-version TLS1_2 --https-only true --sku Standard_GRS
```

```
# Enable immutability policy on a container (time-based retention)
```

```
az storage container create --account-name stbbwEvidence -n evidence --auth-mode
login
```

```
# Then set immutability policy via Portal or ARM (legal hold/time-based lock).
```

---

## 9) Microsoft Purview – Data Map & DSAR Workflow

### 9.1 Purview Setup

- Create **Purview account** in monitoring or shared subscription.

- Register sources: Storage, SQL, Synapse, Power BI.
- Configure **scans** (weekly) + **classification rules** (CHD patterns, PII).
- Build **Business Glossary**: CHD, PD, retention labels.

## 9.2 DSAR Automation (Logic App Overview)

**Trigger:** Teams “DSAR” keyword / Shared mailbox “dsar@barborawy.com”.

**Actions:**

1. Create ticket in ServiceNow/DevOps.
  2. Query Purview for subject’s identifiers (email/hash keys).
  3. Export relevant artifacts to evidence container (read-only link).
  4. Notify DPO for review/approval.
  5. Track SLA (GDPR Art. 12: one month).
- 

## 10) Sentinel – Core PCI/GDPR/revDSG Analytics & Playbooks

### 10.1 Example Analytic Rules (KQL sketches)

- **Excessive Key Vault Denies (PCI 3.5 / revDSG 9)**

AzureDiagnostics

```
| where Category == "AzureKeyVaultAuditEvent"
| where operationName_s has "SecretGet" and ResultSignature !in ("OK","Succeeded")
| summarize count() by bin(TimeGenerated, 1h), identity_claim_appid_g
| where count_ > 20
```

- **Public IP Drift in CDE** (backstop detection)

AzureActivity

```
| where OperationNameValue ==
"MICROSOFT.NETWORK/PUBLICIPADDRESSES/WRITE"
```

| join kind=inner (

ResourceContainers

```
| where type == "microsoft.resources/subscriptions/resourcegroups"
| where tags.CDE == "true"
) on $left.ResourceGroup == $right.name
```

## 10.2 SOAR Playbooks (Logic Apps)

- **BreachNotify:** On Sentinel “High” incident tagged PII/CHD → compile incident summary → email **DPO**, **FDPIC contact**, **Acquirer** template; attach evidence links.
  - **ContainUser:** Disable user, revoke refresh tokens, require password reset.
  - **IsolateVM:** Apply NSG rule deny all inbound; tag Quarantine=true.
- 

## 11) Vulnerability & Patch Management

### 11.1 VMs & Servers

- Enable **Defender for Servers (P2)** → MDE + TVM (Threat & Vulnerability Management).
- Weekly assessment schedule; **Critical ≤7 days**, **Medium ≤30 days** SLA.
- Connect **Update Management Center** and create maintenance configurations.

### 11.2 Containers & Registries

- Enable **Defender for Containers** for AKS/ACR; enforce image scanning at ACR push; deny deployment of images with **High** CVEs via admission controller (AKS policy).
- 

## 12) Backup, DR, and Restore Validation

### 12.1 Recovery Services Vaults (CLI)

```
az backup vault create -g rg-backup -n rsv-bbw-prod -l westeurope --backup-storage-redundancy GeoRedundant
```

```
# Enable soft delete & immutability for backups
```

### 12.2 Restore Tests

- Semi-annual scripted restores (Automation Runbook) of representative workloads; export **restore-success** logs to evidence store.
- 

## 13) Tagging & Resource Governance

### 13.1 Mandatory Tags

- Owner, DataCategory (CHD|PD|Internal|Public), Environment (Prod|NonProd), CDE (true|false).

- Enforce with **Deny** policies; **Modify** policies can auto-append where possible (with defaults for non-CDE).

## 13.2 Resource Graph Queries (Evidence/Reports)

resources

```
| where tags.CDE == "true"  
| where type has "storageAccounts" or type has "sqlServers"  
| project name, type, location, tags.DataCategory
```

---

## 14) Cross-Border & Localization Controls

- Assign **AllowedLocations** initiative at **/barborawy** with EU/CH only.
  - For exceptions: documented business case, DPO + CISO approval, expiry ≤ 90 days, compensating controls (encryption, tokenization, anonymization).
- 

## 15) Automation: Weekly Compliance Export

### 15.1 Logic App Outline

- **Trigger:** Recurrence (weekly).
  - **Actions:**
    1. **Resource Graph:** export Policy compliance (policyresources, complianceResources).
    2. **Defender for Cloud:** “Secure Score / Regulatory” API call.
    3. Generate CSV/JSON, save into **evidence** container (immutability on).
    4. Send **Teams** summary to Governance channel.
- 

## 16) IaC – Terraform Examples

### 16.1 Policy Assignment

```
resource "azurerm_policy_assignment" "pci_core" {  
  name      = "pac-pci-core"  
  scope     = "/providers/Microsoft.Management/managementGroups/barborawy-  
prod"
```

```

policy_definition_id =
"/providers/Microsoft.Authorization/policySetDefinitions/Barborawy-PCI-Core"

location      = "westeurope"

parameters = jsonencode({
  workspaceId = {
    value = "/subscriptions/0000.../resourceGroups/rg-
monitoring/providers/Microsoft.OperationalInsights/workspaces/law-bbw-prod"
  }
})
}

```

## 16.2 Private Endpoint (Storage)

```

resource "azurerm_private_endpoint" "st_pe" {
  name      = "pe-stcde"
  location   = azurerm_resource_group.rg.location
  resource_group_name = azurerm_resource_group.rg.name
  subnet_id    = azurerm_subnet.pe_subnet.id

  private_service_connection {
    name          = "pe-stcde-blob"
    private_connection_resource_id = azurerm_storage_account.stcde.id
    subresource_names     = ["blob"]
    is_manual_connection = false
  }
}

```

## 17) Acceptance Tests (Gate Controls)

- **Pre-prod pipeline gates:**
  - **Policy compliance ≥ 98%** (Resource Graph query).

- No **Public IP** on CDE resources.
  - All resources have required **tags**.
  - Diagnostics connected to **LAW**.
  - Fail pipeline on non-compliance; require **risk waiver** to proceed.
- 

## 18) KPIs & SLOs (Ops Runbook)

| KPI                         | Target               | Tool               |
|-----------------------------|----------------------|--------------------|
| PCI compliance score        | ≥ 90%                | Defender for Cloud |
| Policy compliance           | ≥ 98%                | Azure Policy       |
| Mean time to contain (MTTC) | < 30 min             | Sentinel SOAR      |
| Key rotation compliance     | 100% within 365 days | Key Vault          |
| Restore test success        | 100% semi-annual     | RSV reports        |

---

## 19) Documentation & Evidence Pointers

- **Evidence Storage:** stbbwevidence/evidence (WORM).
  - **Quarterly Audit Pack:**
    - Policy compliance CSV + **Secure Score** export
    - PIM activation logs
    - Sentinel incident summary & playbook run logs
    - Restore test reports
    - DSAR workflow exports (Purview search log + packaged artifacts)
- 

## 20) Go-Live Checklist (Cutover)

1. MG hierarchy created; subscriptions mapped.
2. LAW + Sentinel deployed; diagnostics auto-deployed (initiative).
3. Defender plans enabled; regulatory standards visible.
4. PCI/GDPR/revDSG initiatives assigned; exemptions documented.
5. Hub firewall + DDoS configured; spokes peered; private endpoints online.

6. KV with purge protection; CMK bound to Storage/SQL/App as required.
7. PIM and CA policies enforced; legacy auth blocked.
8. DSAR & Breach Logic Apps created; test notifications completed.
9. Evidence container WORM configured; weekly export automation running.
10. KPIs/SLOs defined; dashboards shared with Governance Board.

## Part V – Policy Library (Deployable Azure Policy Baselines)

**Purpose:** Centralize *what to enforce* in Azure.

**Scope:** All subscriptions under the **/barborawy** tenant root management group.

**Assignment rule:** Assign initiatives at **MG**; grant time-boxed, documented exemptions only (CISO + DPO approval, ≤ 90 days, compensating controls).

---

### A. Library Structure (Initiatives you will assign)

| Initiative Code       | Display Name                     | Primary Coverage                                     | Default Effects                      |
|-----------------------|----------------------------------|--|--------------------------------------|
| BBW-PCI-Core          | Barborawy PCI DSS Core Controls  | PCI Req. 1–6, 10–12                                  | Deny,<br>DeployIfNotExists,<br>Audit |
| BBW-Data-Privacy      | GDPR + Swiss revDSG Data Privacy | GDPR Arts.<br>5/25/30/32/33/44;<br>revDSG 8/16/24/25 | Deny, Audit                          |
| BBW-IAM-Baseline      | Identity & Access Minimums       | PCI 7–9, ISO A.9                                     | Deny, Audit                          |
| BBW-Observability     | Diagnostics, Sentinel, Evidence  | PCI 10; GDPR 30/33;<br>revDSG 24                     | DeployIfNotExists,<br>Audit          |
| BBW-Resilience        | Backup, DR, Immutability         | PCI 12.10; GDPR 32                                   | DeployIfNotExists,<br>Audit          |
| BBW-App-Platform      | PaaS Hardening (AppSvc/AKS/ACR)  | PCI 6/11; ISO A.12                                   | Deny,<br>DeployIfNotExists           |
| BBW-Tagging-Lifecycle | Mandatory Tags & Lifecycle       | ISO A.8; GDPR 5                                      | Deny, Modify                         |

Tip: keep each initiative ≤ 50 definitions so Policy compliance pages render fast.

---

## B. Global Parameters (used across initiatives)

```
{  
  "parameters": {  
    "allowedLocations": { "type": "Array", "defaultValue":  
      ["switzerlandnorth","switzerlandwest","westeurope","northeurope"] },  
    "logAnalyticsWorkspaceld": { "type": "String" },  
    "cdeTagKey": { "type": "String", "defaultValue": "CDE" },  
    "cdeTagValue": { "type": "String", "defaultValue": "true" },  
    "requiredTags": { "type": "Array", "defaultValue":  
      ["Owner","DataCategory","Environment","CDE"] },  
    "allowedDataCategories": { "type": "Array", "defaultValue":  
      ["CHD","PD","Internal","Public"] },  
    "maxSubscriptionOwners": { "type": "Integer", "defaultValue": 2 }  
  }  
}
```

---

## C. Identity & Access (Initiative: BBW-IAM-Baseline)

### C1. Limit Subscription Owners (Deny/Audit)

- **Why:** PCI 7.1; least privilege.
- **Policy (Custom, AuditIfNotExists or Deny on create):**

```
{  
  "properties": {  
    "displayName": "Limit number of Owner role assignments per subscription",  
    "mode": "All",  
    "parameters": { "maxOwners": { "type": "Integer", "defaultValue": 2 } },  
    "policyRule": {  
      "if": { "field": "type", "equals": "Microsoft.Authorization/roleAssignments" },  
      "then": { "effect": "AuditIfNotExists",  
      "details": {
```

```

    "type": "Microsoft.Authorization/roleAssignments",
    "existenceCondition": {
        "count": { "field": "Microsoft.Authorization/roleAssignments/roleDefinitionId",
            "where": { "like": "*/roleDefinitions/*owner*" } },
        "lessOrEquals": "[parameters('maxOwners')]"
    }
}
}
}
}
}

```

## C2. Enforce PIM for High-Privilege Roles (Audit)

- **Why:** PCI 8.x; JIT elevation.
- **Note:** Enforced via Entra/PIM; track via **Audit** policy that checks for **permanent** GA/SecAdmin assignments and flags them.

## C3. Block Legacy Authentication (Audit)

- **Why:** PCI 8.3; GDPR 32.
- **Implementation:** Use Entra Conditional Access baseline + Sentinel analytic rule to alert on legacy protocol attempts.

## C4. Mandatory Access Reviews (Informational)

- **Why:** PCI 7.2; GDPR accountability.
- **Policy:** Custom informational control verifying the existence of scheduled Access Reviews for CDE admin groups.

## D. Network & Segmentation (Initiative: BBW-PCI-Core)

### D1. Deny Public IP on NICs in CDE (Deny)

```
{
    "properties": {
        "displayName": "Deny public IP on NICs when CDE=true",
    }
}
```

```

"mode":"All",
"parameters":{

  "cdeTagKey":{"type":"String","defaultValue":"CDE"},

  "cdeTagValue":{"type":"String","defaultValue":"true"}


},

"policyRule":{

  "if":{

    "allOf":[

      { "field":"type","equals":"Microsoft.Network/networkInterfaces" },


      {

        "field":"tags[concat(parameters('cdeTagKey'))]","equals":"[parameters('cdeTagValue')]" },


      ]


      "exists":"true" }

    ]


  },


  "then":{ "effect":"deny" }

}

}
}

```

## **D2. Require NSGs on All Subnets & NICs (Deny)**

- Built-in: *Audit/deny network interfaces and subnets without NSG.*

## **D3. Require Private Endpoints for Storage/SQL/Key Vault/App Service (CDE) (Deny)**

- Custom policy that checks resource type + CDE tag and denies if privateEndpointConnections is empty.

## **D4. DDoS Protection Standard on Prod VNets (DeployIfNotExists)**

- Deploy association to a central DDoS plan.

## **D5. Flow Logs + Traffic Analytics (DeployIfNotExists)**

- Target all NSGs; parameters: logAnalyticsWorkspaceId.
-

## **E. Data Protection & Encryption (Initiative: BBW-PCI-Core + BBW-Data-Privacy)**

### **E1. Enforce HTTPS-Only & TLS 1.2+ on Storage (Deny)**

- Built-in policy: **Secure transfer required; Minimum TLS version.**

### **E2. Require CMK for CDE & PD Data Stores (Audit/Deny)**

- Applies to: Storage Accounts, SQL DB/MI, Disk Encryption Sets, Cosmos DB.
- **Compensating control option:** tokenization vendor + BYOK proof.

### **E3. Key Vault Soft Delete & Purge Protection (Deny)**

```
{  
  "properties": {  
    "displayName": "Require Key Vault soft delete and purge protection",  
    "mode": "Indexed",  
    "policyRule": {  
      "if": { "field": "type", "equals": "Microsoft.KeyVault/vaults" },  
      "then": {  
        "effect": "deny",  
        "details": [  
          { "field": "Microsoft.KeyVault/vaults/enableSoftDelete", "equals": true },  
          { "field": "Microsoft.KeyVault/vaults/enablePurgeProtection", "equals": true }  
        ]  
      }  
    }  
  }  
}
```

### **E4. Data Residency – Allowed Locations (EU/CH) (Deny)**

- Parameterize allowedLocations for prod; dev/test may include West Europe/North Europe only.

### **E5. Object-Level Storage Protections (Audit/DeployIfNotExists)**

- **Blob public access disabled, SAS expiry limits, versioning + change feed.**

---

## F. Logging, Monitoring & Evidence (Initiative: BBW-Observability)

### F1. Deploy Diagnostic Settings to LAW (DeployIfNotExists)

- Use **built-in** for broadest resource coverage. Parameter:  
logAnalyticsWorkspaceId.

### F2. Enable Microsoft Defender for Cloud Plans (DeployIfNotExists)

- Virtual Machines, SQL, Storage, Containers, App Services, AKS, ACR.

### F3. Sentinel Connection (Audit)

- Audit that each prod subscription is connected to a Sentinel-enabled workspace.

### F4. Log Retention & Immutable Evidence (Audit)

- LAW ≥ 365 days; export weekly compliance files to **WORM** container.
- 

## G. Vulnerability & Patch (Initiative: BBW-PCI-Core)

| Policy                                | Effect            | Notes   |
|---------------------------------------|-------------------|---|
| Defender for Servers agent on all VMs | DeployIfNotExists | Includes MDE/TVM  |
| Deny unsupported OS images            | Deny              | Gate legacy images  |
| CIS/Microsoft Baseline drift          | Audit             | Use Defender recommendations                                |
| Automatic updates for prod            | Audit             | Validate Update Mgmt configs                                |
| ACR image scanning                    | DeployIfNotExists | Block image deploy on Critical CVEs (AKS admission control) |

---

## H. Backup, DR & Immutability (Initiative: BBW-Resilience)

| Control                             | Effect            | Evidence            |
|-------------------------------------|-------------------|---------------------|
| Azure Backup on prod VMs/DBs        | DeployIfNotExists | RSV jobs inventory  |
| Backup encryption (CMK or platform) | Audit             | Vault/Key link      |
| WORM on evidence & backups          | Audit             | Immutability policy |

| <b>Control</b>                 | <b>Effect</b> | <b>Evidence</b>              |
|--------------------------------|---------------|------------------------------|
| Semi-annual restore test proof | Audit         | Runbook output & screenshots |

---

## I. PaaS Platform Hardening (Initiative: BBW-App-Platform)

| <b>Resource</b> | <b>Required Policy</b>                                       | <b>Effect</b> |
|-----------------|--|---------------|
| App Service     | HTTPS-only; latest runtime; FTPS disabled; identity required | Deny/Audit    |
| Azure SQL       | TDE with CMK; AAD auth; minimal TLS                          | Deny/Audit    |
| AKS             | Private cluster; Defender; RBAC; Azure Policy for Kubernetes | Deny/Deploy   |
| ACR             | Admin user disabled; image scan on push                      | Deny/Deploy   |
| Key Vault       | Private Endpoint; purge/soft delete; RBAC only               | Deny          |

---

## J. Tagging & Lifecycle (Initiative: BBW-Tagging-Lifecycle)

### J1. Require Mandatory Tags (Deny/Modify)

```
{
  "properties": {
    "displayName": "Require mandatory tags",
    "mode": "Indexed",
    "parameters": {
      "requiredTags": { "type": "Array", "metadata": { "displayName": "Required tags" } }
    },
    "policyRule": {
      "if": { "anyOf": [
        { "field": "tags['Owner']", "exists": "false" },
        { "field": "tags['DataCategory']", "exists": "false" },
        { "field": "tags['Environment']", "exists": "false" },
        { "field": "tags['CDE']", "exists": "false" }
      ]},
    }
  }
}
```

```

        "then": { "effect":"deny" }

    }

}

}

```

## J2. Restrict Tag Values (Deny)

- DataCategory must be one of: CHD|PD|Internal|Public.
  - Environment must be one of: Prod|NonProd|Dev|Test|QA.
- 

## K. Privacy Automation (Initiative: BBW-Data-Privacy)

| Control                      | Description   | Effect            |
|------------------------------|---|-------------------|
| DSAR Workflow Presence       | Audit existence of Logic App named pattern la-dsar-* in tenant                              | Audit             |
| Breach Notification Playbook | Require Logic App la-breachnotify-* and Sentinel rule tied                                  | DeployIfNotExists |
| ROPA/DPIA Register           | Audit Purview account + collections for systems in scope                                    | Audit             |
| Data Anonymization in Test   | Enforce tag DataCategory=PD/CHD ⇒ deny deployment to NonProd unless masking flag is present | Deny              |

---

## L. Example: Initiative Definition Skeleton

```
{
  "name": "BBW-PCI-Core",
  "properties": {
    "displayName": "Barborawy PCI DSS Core Controls",
    "policyType": "Custom",
    "parameters": {
      "allowedLocations": { "type": "Array" },
      "logAnalyticsWorkspaceId": { "type": "String" }
    }
  }
}
```

```
},  
"policyDefinitions": [  
{  
    "policyDefinitionReferenceId": "denyPublicIpOnNicCde",  
    "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/deny-  
public-ip-nic-cde"  
,  
{  
    "policyDefinitionReferenceId": "requireNSGSubnets",  
    "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/builtin-  
require-nsg-on-subnet"  
,  
{  
    "policyDefinitionReferenceId": "deployDiagToLAW",  
    "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/builtin-  
deploy-diagnostics",  
    "parameters": { "workspaceId": { "value": "[parameters('logAnalyticsWorkspaceId')]" } }  
,  
{  
    "policyDefinitionReferenceId": "allowedLocations",  
    "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/builtin-  
allowed-locations",  
    "parameters": { "listOfAllowedLocations": { "value": "[parameters('allowedLocations')]" } }  
,  
]  
}  
}
```

---

## M. Assignment Examples

### M1. Bicep – Assign to Management Group

```
param mgId string = 'barborawy-prod'

param lawId string

param allowed array

resource assign 'Microsoft.Authorization/policyAssignments@2022-06-01' = {
    name: 'assign-bbw-pci-core'
    location: 'westeurope'
    scope: tenantResourceId('Microsoft.Management/managementGroups', mgId)
    properties: {
        displayName: 'Assign BBW-PCI-Core'
        policyDefinitionId:
            tenantResourceId('Microsoft.Authorization/policySetDefinitions','BBW-PCI-Core')
        parameters: {
            logAnalyticsWorkspaceld: { value: lawId }
            allowedLocations: { value: allowed }
        }
        nonComplianceMessages: [
            { message: 'Policy enforced by Barborawy PCI Core. Request exemption via CISO/DPO.' }
        ]
    }
}
```

### M2. Terraform – Assign Initiative

```
resource "azurerm_policy_assignment" "bbw_pci_core" {
    name      = "assign-bbw-pci-core"
    scope     = "/providers/Microsoft.Management/managementGroups/barborawy-prod"
```

```

policy_definition_id = "/providers/Microsoft.Authorization/policySetDefinitions/BBW-
PCI-Core"

location      = "westeurope"

parameters = jsonencode({
    logAnalyticsWorkspaceId = { value = "/subscriptions/<sub>/resourceGroups/rg-
monitoring/providers/Microsoft.OperationalInsights/workspaces/law-bbw-prod" }

    allowedLocations     = { value =
["switzerlandnorth","switzerlandwest","westeurope","northeurope"] }

})
}

```

---

## N. Default Effects by Environment

| Control Type                         | Prod                     | NonProd                              |
|--------------------------------------|--------------------------|--------------------------------------|
| Network exposure (public IP, no NSG) | <b>Deny</b>              | <b>Deny</b>                          |
| Private Endpoint for CDE             | <b>Deny</b>              | <b>Deny</b>                          |
| Diagnostics to LAW                   | <b>DeployIfNotExists</b> | <b>DeployIfNotExists</b>             |
| TLS/HTTPS minimums                   | <b>Deny</b>              | <b>Deny</b>                          |
| Tagging completeness                 | <b>Deny</b>              | <b>Modify → Deny</b> (grace 14 days) |
| Defender plan enablement             | <b>DeployIfNotExists</b> | <b>DeployIfNotExists</b>             |
| Data residency (EU/CH)               | <b>Deny</b>              | <b>Deny</b>                          |
| Backup/Immutability                  | <b>Audit (report)</b>    | <b>Audit</b>                         |

---

## O. Exemptions (Process Snippet)

- **Inputs:** control, asset scope (subscription/RG/resource), business reason, compensating control, expiry date.
- **Approvals:** CISO + DPO (and QSA where PCI impact exists).

- **Tracking:** exemption ID in Policy **Exemption** object; **Sentinel** alert on expiry ≤ 14 days.
  - **Max window:** 90 days.
- 

## P. Compliance Mapping (quick lookups)

| Policy Area                    | PCI DSS | GDPR     | revDSG |
|--------------------------------|---------|----------|--------|
| Segmentation (NSG/Firewall/PE) | 1–2     | 32       | 8      |
| Encryption (CMK/TLS)           | 3–4     | 32       | 8/9    |
| IAM (RBAC/MFA/PIM)             | 7–9     | 25/32    | 8      |
| Logging/Monitoring             | 10      | 30/33    | 24     |
| Backup/DR                      | 12.10   | 32       | —      |
| Residency/Transfers            | —       | 44–49    | 16     |
| DSAR/Breach                    | —       | 15–17/33 | 25/24  |

---

## Q. Ready-to-Use Built-Ins (add these to initiatives)

- **Storage:** secure transfer required; minimum TLS; public blob access disabled; private link required (custom).
- **Key Vault:** purge + soft delete; firewall enabled/private endpoint required (custom).
- **SQL:** TDE enabled; auditing to LAW; disabled public endpoint; AAD authentication.
- **Compute:** managed disks encryption; endpoint protection installed; AMA installed; update management configured.
- **Networking:** NSG on subnet/NIC; deny RDP/SSH from Internet; DDoS Standard configured.
- **Containers:** Defender for Containers enabled; ACR image scanning; AKS private cluster; policy add-ons enabled.
- **Monitoring:** deploy diagnostic settings; Sentinel data connectors enabled (AAD, AADSignin, Key Vault, Firewall, MDE).

- **Governance:** allowed locations; required tags; allowed SKUs (optional cost control).

**Note:** Built-in GUIDs change over time; reference by display name in IaC variables, or centrally alias GUIDs in a versioned variable file.

---

## R. Quality Gates (pre-prod pipeline)

- Policy compliance  $\geq 98\%$
  - **0** CDE resources without Private Endpoint
  - **0** public IPs on CDE
  - Diagnostics on  $\geq 98\%$  resources
  - Owner, DataCategory, Environment, CDE tags present on **100%** of new deployments
- 

## S. Rollout Plan

1. **Dry-run Audit:** assign initiatives in **Audit** only to barborawy-nonprod; fix false positives.
  2. **Phased Enforce:** switch critical controls to **Deny** (public IPs, HTTPS/TLS, Key Vault protections).
  3. **Auto-Remediate:** enable **DeployIfNotExists** for diagnostics/agents.
  4. **Prod Assignment:** assign to barborawy-prod with agreed parameter set.
  5. **Monitor & Tune:** weekly drift review; open CAPAs.
  6. **Freeze Window:** for any control shifting from Audit→Deny, communicate change window and rollback plan.
- 

## T. Packaging for Git

/policy

/definitions

deny-public-ip-nic-cde.json

require-nsg-subnet.json

require-kv-purge-softdelete.json

```
enforce-https-storage.json  
require-private-endpoint-storage.json  
...  
  
/initiatives  
bbw-pci-core.json  
bbw-data-privacy.json  
bbw-iam-baseline.json  
bbw-observability.json  
bbw-resilience.json  
bbw-app-platform.json  
bbw-tagging-lifecycle.json  
  
/assignments  
assign-bbw-pci-core.bicep  
assign-bbw-data-privacy.bicep  
assign-bbw-iam-baseline.bicep
```

/ci

```
validate-policy.ps1  
pipeline-gates.yml
```

## **Part VII – Appendices (Templates, Snippets, Queries, Checklists & Executive Pack)**

Cut-paste friendly material you can drop into Git/Confluence. Everything assumes deployment at **/barborawy** tenant root MG with prod/non-prod child MGs.

---

### **Appendix A – Master Regulatory Mapping (Deep Cut)**

| Area                 | PCI         |         |        | Swiss<br>revDSG | Primary Azure Controls  |
|----------------------|-------------|---------|--------|-----------------|---|
|                      | DSS         | GDPR    | 4.0    |                 |   |
| Network segmentation | Req.<br>1–2 | Art. 32 | Art. 8 |                 | Hub/Spoke + Azure Firewall<br>Premium, NSGs, Private Endpoints,<br>DDoS Std |

| Area                          | PCI DSS 4.0 | GDPR         | Swiss revDSG | Primary Azure Controls  |
|-------------------------------|-------------|--------------|--------------|---|
| Config hardening              | Req. 2      | Art. 25      | Art. 8       | Azure Policy baselines, Defender Benchmarks                                     |
| Encrypt data at rest          | Req. 3.5    | Art. 32      | Art. 9       | Storage/SQl/Disks with <b>CMK</b> in Key Vault (soft delete + purge protection) |
| Encrypt in transit            | Req. 4.1    | Art. 32      | Art. 8       | HTTPS-only, TLS ≥ 1.2, AppGW/WAF  |
| Malware protection            | Req. 5      | Art. 32      | Art. 8       | Defender for Endpoint/Servers, MDE TVM  |
| Vulnerability/Patching        | Req. 6      | Art. 32      | Art. 8       | Defender for Cloud, Update Mgmt Center  |
| Access control (need-to-know) | Req. 7      | Art. 25      | Art. 8       | Entra ID RBAC, custom roles, resource-level RBAC                                |
| Strong auth, MFA              | Req. 8      | Art. 32      | Art. 8       | Conditional Access (MFA), PIM JIT   |
| Physical security             | Req. 9      | —            | —            | CSP scope (Microsoft)   |
| Logging & monitoring          | Req. 10     | Arts. 30, 33 | Art. 24      | Diagnostic settings → LAW, Sentinel, retention ≥ 12m                            |
| Testing & scans               | Req. 11     | Art. 32      | Art. 8       | Defender assessments, ASV scans, PenTests                                       |
| Security policy & IR          | Req. 12     | Arts. 33–34  | Art. 24      | IR playbooks, breach notify Logic Apps  |
| Records of processing         | —           | Art. 30      | —            | Microsoft Purview (ROPA), Data Map  |
| Data subject rights           | —           | Arts. 12–23  | Art. 25      | DSAR Logic App + Purview export   |
| Cross-border transfers        | —           | Arts. 44–49  | Art. 16      | <b>AllowedLocations</b> (EU/CH), exception workflow                             |

## Appendix B – Azure Policy: Ready-to-Use JSON Snippets

**Tip:** Keep each file in /policy/definitions/; reference by name in initiatives.

### B1. Deny Public IP on NICs (CDE)

```
{  
  "properties": {  
    "displayName": "Deny public IP on NICs when CDE=true",  
    "policyType": "Custom",  
    "mode": "All",  
    "parameters": {  
      "cdeTagKey": { "type": "String", "defaultValue": "CDE" },  
      "cdeTagValue": { "type": "String", "defaultValue": "true" }  
    },  
    "policyRule": {  
      "if": {  
        "allOf": [  
          { "field": "type", "equals": "Microsoft.Network/networkInterfaces" },  
          { "field": "[concat('tags[', parameters('cdeTagKey'), ']')]", "equals": "[parameters('cdeTagValue')]" },  
          { "field": "  
Microsoft.Network/networkInterfaces/ipconfigurations[*].publicIPAddress.id", "exists":  
"true" }  
        ]  
      },  
      "then": { "effect": "deny" }  
    }  
  }  
}
```

### B2. Require NSG on Subnets

```
{
```

```

"properties": {

    "displayName": "Require NSG on all subnets",
    "policyType": "BuiltIn",
    "mode": "All",
    "policyRule": { /* use built-in: "Subnets should have a Network Security Group" */ }

}
}

```

### **B3. Require Private Endpoint (Storage in CDE)**

```

{
    "properties": {

        "displayName": "Require Private Endpoint for Storage when CDE=true",
        "policyType": "Custom",
        "mode": "Indexed",
        "parameters": {

            "cdeTagKey": { "type": "String", "defaultValue": "CDE" },
            "cdeTagValue": { "type": "String", "defaultValue": "true" }

        },
        "policyRule": {

            "if": {

                "allOf": [

                    { "field": "type", "equals": "Microsoft.Storage/storageAccounts" },
                    { "field": "[concat('tags[', parameters('cdeTagKey'), ']')]", "equals": "[parameters('cdeTagValue')]" },
                    { "field": "Microsoft.Storage/storageAccounts/privateEndpointConnections[*]", "exists": false }

                ]
            },
            "then": { "effect": "deny" }

        }
    }
}

```

```
}
```

```
}
```

#### B4. HTTPS-Only + TLS ≥ 1.2 (Storage)

```
{
```

```
  "properties": {
```

```
    "displayName": "Storage accounts must enforce HTTPS and TLS1.2+",
```

```
    "policyType": "BuiltIn",
```

```
    "mode": "Indexed",
```

```
    "policyRule": { /* use built-ins: secureTransferRequired + minimumTlsVersion */ }
```

```
}
```

```
}
```

#### B5. Key Vault: Soft Delete & Purge Protection

```
{
```

```
  "properties": {
```

```
    "displayName": "Key Vault must enable soft delete and purge protection",
```

```
    "policyType": "Custom",
```

```
    "mode": "Indexed",
```

```
    "policyRule": {
```

```
      "if": { "field": "type", "equals": "Microsoft.KeyVault/vaults" },
```

```
      "then": {
```

```
        "effect": "deny",
```

```
        "details": [
```

```
          { "field": "Microsoft.KeyVault/vaults/enableSoftDelete", "equals": true },
```

```
          { "field": "Microsoft.KeyVault/vaults/enablePurgeProtection", "equals": true }
```

```
        ]
```

```
      }
```

```
    }
```

```
}
```

## **B6. Allowed Locations (EU/CH)**

```
{  
  "properties": {  
    "displayName": "Allowed locations (EU/CH only)",  
    "policyType": "BuiltIn",  
    "mode": "All",  
    "parameters": {  
      "listOfAllowedLocations": { "type": "Array" }  
    },  
    "policyRule": { /* built-in "Allowed locations" */ }  
  }  
}
```

## **B7. Deploy Diagnostic Settings to LAW**

```
{  
  "properties": {  
    "displayName": "Deploy diagnostics to Log Analytics",  
    "policyType": "BuiltIn",  
    "mode": "Indexed",  
    "parameters": { "workspaceId": { "type": "String" } },  
    "policyRule": { /* built-in "Deploy Diagnostic settings..." */ }  
  }  
}
```

## **B8. SQL Public Network Access Disabled (AAD Auth Required)**

```
{  
  "properties": {  
    "displayName": "SQL servers: public network disabled, AAD auth required",  
    "policyType": "Custom",  
    "mode": "All",  
    "policyRule": {
```

```

"if": { "field": "type", "equals": "Microsoft.Sql/servers" },

"then": { "effect": "AuditIfNotExists",

"details": {

"type": "Microsoft.Sql/servers",

"existenceCondition": {

"allOf": [

{ "field": "Microsoft.Sql/servers/publicNetworkAccess", "equals": "Disabled" },

{ "field": "Microsoft.Sql/servers/administrators/azureADOnlyAuthentication",

>equals": "Enabled" }

]

}

}

}

}

}

}

```

## B9. Mandatory Tags + Restricted Values

```

{

"properties": {

"displayName": "Require tags and restrict values",

"policyType": "Custom",

"mode": "Indexed",

"parameters": {

"requiredTags": { "type": "Array", "defaultValue": ["Owner","DataCategory","Environment","CDE"] },



"allowedDataCategories": { "type": "Array", "defaultValue": ["CHD","PD","Internal","Public"] },



"allowedEnvironments": { "type": "Array", "defaultValue": ["Prod","NonProd","Dev","Test","QA"] }

},


},
```

```

"policyRule": {

    "if": { "anyOf": [
        { "field": "tags['Owner']", "exists": "false" },
        { "field": "tags['DataCategory']", "exists": "false" },
        { "field": "tags['Environment']", "exists": "false" },
        { "field": "tags['CDE']", "exists": "false" },
        { "field": "tags['DataCategory']", "notIn": "[parameters('allowedDataCategories')]" },
        { "field": "tags['Environment']", "notIn": "[parameters('allowedEnvironments')]" }
    ]},
    "then": { "effect": "deny" }

}

}

```

---

## **Appendix C – Initiative Skeletons (Compact)**

### **PCI Core (BBW-PCI-Core)**

```

{
    "properties": {
        "displayName": "Barborawy PCI DSS Core Controls",
        "policyType": "Custom",
        "parameters": {
            "allowedLocations": { "type": "Array" },
            "logAnalyticsWorkspaceId": { "type": "String" }
        },
        "policyDefinitions": [
            { "policyDefinitionReferenceId": "denyPublicIpNicCde", "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/deny-public-ip-nic-cde" },
            { "policyDefinitionReferenceId": "requireNSGSubnet", "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/builtin-require-nsg-on-subnet" }
        ]
    }
}

```

```

    { "policyDefinitionReferenceId": "privEndpointStorage", "policyDefinitionId":
"/providers/Microsoft.Authorization/policyDefinitions/require-private-endpoint-storage-
cde" },
    { "policyDefinitionReferenceId": "diagnosticsLAW", "policyDefinitionId":
"/providers/Microsoft.Authorization/policyDefinitions/builtin-deploy-diagnostics",
"parameters": { "workspaceId": { "value": "[parameters('logAnalyticsWorkspaceId')]" } } },
    { "policyDefinitionReferenceId": "allowedLocations", "policyDefinitionId":
"/providers/Microsoft.Authorization/policyDefinitions/builtin-allowed-locations",
"parameters": { "listOfAllowedLocations": { "value": "[parameters('allowedLocations')]" } }
}
]
}
}

```

---

## **Appendix D – Terraform/Bicep Assignments (Quick Start)**

### **Terraform – Initiative Assignment**

```

resource "azurerm_policy_assignment" "bbw_pci_core" {
  name      = "assign-bbw-pci-core"
  scope      = "/providers/Microsoft.Management/managementGroups/barborawy-
prod"
  policy_definition_id = "/providers/Microsoft.Authorization/policySetDefinitions/BBW-
PCI-Core"
  location    = "westeurope"
  parameters = jsonencode({
    logAnalyticsWorkspaceId = { value = "/subscriptions/<sub>/resourceGroups/rg-
monitoring/providers/Microsoft.OperationalInsights/workspaces/law-bbw-prod" }
    allowedLocations     = { value =
      ["switzerlandnorth","switzerlandwest","westeurope","northeurope"] }
  })
}

```

### **Bicep – Initiative Assignment**

```
param mgld string = 'barborawy-prod'
```

```

param lawId string
param allowed array

resource assign 'Microsoft.Authorization/policyAssignments@2022-06-01' = {
    name: 'assign-bbw-pci-core'
    location: 'westeurope'
    scope: tenantResourceId('Microsoft.Management/managementGroups', mgId)
    properties: {
        displayName: 'Assign BBW-PCI-Core'
        policyDefinitionId:
tenantResourceId('Microsoft.Authorization/policySetDefinitions','BBW-PCI-Core')
        parameters: {
            logAnalyticsWorkspaceId: { value: lawId }
            allowedLocations: { value: allowed }
        }
    }
}

```

---

## **Appendix E – KQL Queries (Dashboards & Alerts)**

### **E1. CDE PaaS without Private Endpoint**

```

resources

| where tags.CDE == 'true'

| where type in~
('microsoft.storage/storageaccounts','microsoft.sql/servers','microsoft.keyvault/vaults')

| extend pe = properties.privateEndpointConnections

| where isnull(pe) or array_length(pe) == 0

| project name, type, resourceGroup, subscriptionId, location

```

### **E2. Sentinel: Repeated Key Vault Secret Access Failures**

AzureDiagnostics

```
| where Category == "AzureKeyVaultAuditEvent"  
| where OperationName == "SecretGet" and ResultType != "Success"  
| summarize failures = count() by bin(TimeGenerated, 1h), identity_claim_appid_g,  
Resource  
| where failures > 20
```

### **E3. Owner Role Count per Subscription (ARG)**

```
policyresources  
| where type =~ 'microsoft.authorization/roleassignments'  
| where properties.roleDefinitionId has 'Owner'  
| summarize owners = count() by subscriptionId
```

### **E4. Diagnostics Coverage**

```
policyresources  
| where type has 'policyAssignments'  
| // Or use Azure Policy compliance export table for nonCompliantResources
```

---

## **Appendix F – Logic App Pseudocode (DSAR & Breach)**

### **F1. DSAR Workflow**

Trigger: New email to dsar@barborawy.com OR Teams keyword "DSAR"

Actions:

1. Create ticket in ServiceNow/Azure DevOps (metadata: requester, due date +30d)
2. Purview Search: subject identifiers (email, hash)
3. Export results (paths only) to evidence container (WORM); generate signed URL
4. Notify DPO for approval (adaptive card)
5. On approve: package export bundle, send secure link to requester
6. Log completion; update ticket; archive artifacts

### **F2. Breach Notification**

Trigger: Sentinel incident with tags ["PII","CHD"] and Severity >= High

Actions:

1. Gather incident entities + timeline

2. Build regulator report template (GDPR 72h / revDSG ASAP)
  3. Email DPO, Legal, CISO + Teams channel "Incident-Bridge"
  4. If CDE impacted: notify Acquirer (PCI) using predefined template
  5. Create PIR task; capture root cause and CAPA
  6. Archive incident package to evidence (WORM)
- 

## **Appendix G – Evidence Export Automation (Outline)**

- **Weekly Logic App:**
    - ARG: Policy compliance → CSV
    - Defender: Regulatory/secure score → JSON
    - PIM activations (Graph API) → CSV
    - Sentinel incidents summary → PDF (Workbook export)
    - Save under stbbwevidence/evidence/yyyy-mm-wk##/ (immutability policy).
    - Teams notification with deltas.
- 

## **Appendix H – Exception Request Template**

Control ID: (e.g., BBW-PCI-NET-001)

Asset Scope: (Subscription/RG/Resource)

Business Justification:

Duration (≤ 90 days): From \_\_ To \_\_

Risk Assessment: (Impact/Likelihood, residual risk)

Compensating Controls:

Monitoring Plan:

Approvals: CISO \_\_ DPO \_\_ (QSA if PCI) \_\_

Ticket/Ref:

## **Appendix I – DPIA / ROPA Skeletons**

### **DPIA (Data Protection Impact Assessment)**

- Processing purpose & lawful basis (GDPR Art. 6)
- Data categories (PD/CHD), retention, minimization measures
- Risks to rights & freedoms, mitigations (technical/organizational)
- Transfers (countries, safeguards), processors list
- Outcomes & residual risk acceptance (DPO sign-off)

### **ROPA (Record of Processing Activities)**

- Controller info, processing purposes
  - Categories of data subjects/data
  - Recipients/third parties, transfers outside EU/CH
  - Retention periods, security measures
  - Systems & Azure resources involved (Purview link)
- 

### **Appendix J – One-Page Board Summary (Template)**

#### **Barborawy Cloud Compliance – Quarterly Brief (Qx YYYY)**

- **PCI Score:** 92% ( $\Delta +2$ ) – *Goal  $\geq 90\%$*
  - **Policy Compliance:** 98.6% ( $\Delta +0.3$ )
  - **CDE Private Link Coverage:** 100%
  - **Critical CVEs  $\geq 7d$ :** 3 ( $\Delta -5$ ) – *Action: hotfix sprint*
  - **Incidents (High):** 1 – contained in 18 min (MTTC  $< 30$  min)
  - **Restore Tests:** 100% success (4 of 4)
  - **Open Exceptions:** 5 (all  $< 60$  days)
  - **Decisions Required:** Budget for auto-remediation expansion; approve region constraint update.
- 

### **Appendix K – Version Control & Change Log**

| <b>Version</b> | <b>Date</b> | <b>Changes</b>                             | <b>Owner</b> | <b>Approved By</b> |
|----------------|-------------|--|--------------|--------------------|
| 1.0            | 2025-10-06  | Initial unified handbook (PCI+GDPR+revDSG) | CISO         | Board              |

| <b>Version Date</b> | <b>Changes</b>  | <b>Owner</b>   | <b>Approved By</b> |
|---------------------|---|----------------|--------------------|
| 1.1                 | YYYY-MM-DD Added DSAR automation & PE mandate               | DPO            | Governance Board   |
| 1.2                 | YYYY-MM-DD Switched diagnostics policy to DeployIfNotExists | Cloud Sec Arch | CISO               |

---

## Appendix L – Quarterly Audit Pack Checklist

- Defender Regulatory & PCI Score trend (CSV/PNG)
- Azure Policy compliance export (CSV)
- PIM activations & Access Reviews (CSV/PDF)
- Sentinel incidents summary + playbook run logs (PDF)
- Patch SLA & vulnerability status (CSV)
- Restore test evidence (screens/logs)
- DSAR log & samples (DPO-reviewed)
- Exception register with expiry & compensating controls
- DPIA/ROPA updates snapshot
- CAPA register & closure validation

---

## Appendix M – Glossary

- **CDE:** Cardholder Data Environment
- **CMK/BYOK:** Customer-Managed Keys / Bring Your Own Key
- **DPO:** Data Protection Officer
- **DSAR:** Data Subject Access Request
- **LAW:** Log Analytics Workspace
- **PIM:** Privileged Identity Management
- **ROPA/DPIA:** Record of Processing Activities / Data Protection Impact Assessment
- **SOAR:** Security Orchestration, Automation & Response
- **WORM:** Write Once Read Many (immutability)

