

Red Pill or Blue Pill? Navigating Compliance in Azure DevOps Security

Craig Forshaw

Craig Forshaw

- Cloud Architect at Atea
- Working with Microsoft Cloud technologies since 2014
- Organiser: [Microsoft Security User Group](#)
- Blog: [Medium](#)



What we will talk about

Not Azure DevOps...



Azure Regulatory Compliance for DevOps Security



Regulatory compliance

Microsoft cloud security benchmark

53 of 65 passed controls

Lowest compliance regulatory standards
by passed controls



No additional standards are currently monitored.

[Open policy settings to manage additional compliance policies](#)

[Improve your compliance >](#)



Compliance in the infrastructure as code (IaC) matrix

How do we govern what is being actually being deployed to our environments?

- Blue pill – assume all is ok?
- Red pill – go down the rabbit hole. Investigate, establish governance policies and remediation actions that can be used to protect our cloud environments

Typical compliance challenges with DevOps Security in the cloud

Configuration vulnerabilities	Configuration drift	Security control enforcement	Validating compliance	Documenting and tracing
<ul style="list-style-type: none">• IaC Templates• Hardcoding sensitive information• Missing security related components or features	<ul style="list-style-type: none">• State storage encryption• State divergence• Out of band changes• Code analysis	<ul style="list-style-type: none">• Evolving landscape• Incident response and recovery• Responsibility for remediation	<ul style="list-style-type: none">• Assigning compliance remediation tasks• Measuring success• Compliance automation	<ul style="list-style-type: none">• Implementing logging and tracking of changes• Reporting challenges

Microsoft Compliance Frameworks for DevOps

Cloud Adoption Framework

- Security strategy
- Microsoft Cybersecurity reference architecture
- Microsoft Cloud security benchmark

Microsoft Security Development lifecycle (SDL)

- Guidelines and practices for security in the development lifecycle



Microsoft Cloud Security Benchmark

- Best practice recommendations to improve security of workloads, data, and services on Azure
- Covers multi-cloud environments
 - AWS guidance
 - GCP guidance
- Part of Defender for Cloud CSPM licence 'security governance'
- Includes Purview integration
- MCSB Controls (v1)
 - Network
 - Identity management
 - Privileged access
 - Data protection
 - Asset management
 - Logging and threat detection
 - Incident response
 - Posture and vulnerability management
 - Endpoint security
 - Backup and recovery
 - **DevOps Security**
 - Governance and strategy

Security control

DS-1: Conduct threat modeling

DS-2: Ensure software supply chain security

DS-3: Secure DevOps infrastructure

DS-4: Integrate static application security testing into DevOps pipeline

DS-5: Integrate dynamic application security testing into DevOps pipeline

DS-6: Enforce security of workload throughout DevOps lifecycle

DS-7: Enable logging and monitoring in DevOps

Defender for Cloud Security control: DevOps security



[Microsoft cloud security benchmark - DevOps Security | Microsoft Learn](#)

Defender for Cloud regulatory compliance

- Dashboard for regulatory compliance is in Defender for Cloud
- Includes the cloud security benchmark controls
- Standardised way to drive remediation actions via governance rules
- Allows for resource owners to remediate security recommendations removing the overhead on the security team
- **Security admin role** on subscription level required to define rules

The screenshot displays the Microsoft Defender for Cloud Regulatory Compliance dashboard. At the top, a navigation bar includes a search bar and links for 'Download report', 'Manage compliance policies', 'Open query', 'Compliance over time workbook', 'Audit reports', and 'Compliance offerings'. A message states: 'You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above. →'. The main content area is divided into three sections: 1. 'Microsoft cloud security benchmark' showing '55 of 65 passed controls' with a progress bar. 2. 'Lowest compliance regulatory standards' with a message: 'No additional standards are currently monitored.' and a link 'Open policy settings to manage additional compliance policies' and 'Manage compliance policies >'. 3. A sidebar notification: 'Cloud compliance data now integrated in Microsoft Purview Compliance Manager' with a link 'Open'. Below these sections is a feedback bar: 'Is the regulatory compliance experience clear to you? Yes No'. The bottom section, 'Microsoft cloud security benchmark', includes a disclaimer: 'Recommendations from Microsoft Defender for Cloud - Regulatory Compliance should not be interpreted as a guarantee of compliance. It is up to you to evaluate and validate the effectiveness of customer controls per your regulatory environment. These services are subject to the terms and conditions in the licensing terms.' and a note: 'Microsoft cloud security benchmark is applied to the subscription VS Enterprise Sub'. A checkbox 'Expand all compliance controls' is present. A list of compliance categories follows: NS. Network Security, IM. Identity Management, PA. Privileged Access, DP. Data Protection, AM. Asset Management, LT. Logging and Threat Detection, IR. Incident Response, PV. Posture and Vulnerability Management, and ES. Endpoint Security.

Drive remediation with governance rules

- Governance rules identify resources that require remediation according to specific recommendations or severities.
- define rules that assign an owner and a due date n on a timeframe of 7, 14, 30, or 90 days
- Can apply a grace period so that the resources given a due date don't affect the secure score.
- Owners emailed weekly

[Remediate security recommendations with governance - Microsoft Defender for Cloud | Microsoft Learn](#)



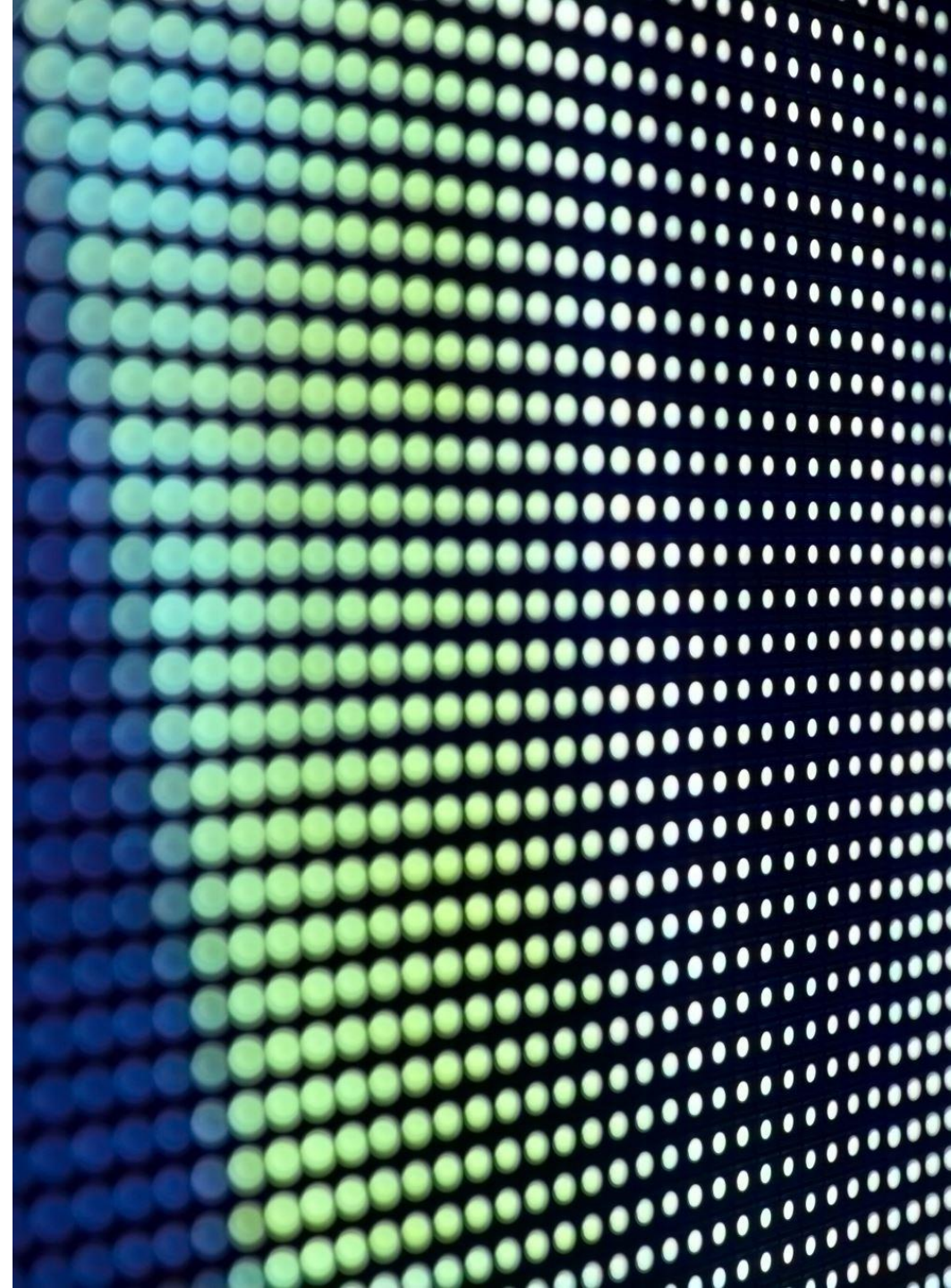
Defender for Cloud regulatory compliance

Demo



My Recommendations

Discover	Create	Implement
Discover what alerts are being generated from Defender for Cloud and where the vulnerabilities lie	Create governance rules for alerting that removes responsibility from the Security team, for example, per developer team in a subscription	<p>Always implement alerting for high value assets</p> <p>Ensure governance routines actually work as intended</p> <p>Have a plan issue handling and isolation of vulnerabilities</p>



Thank you!

