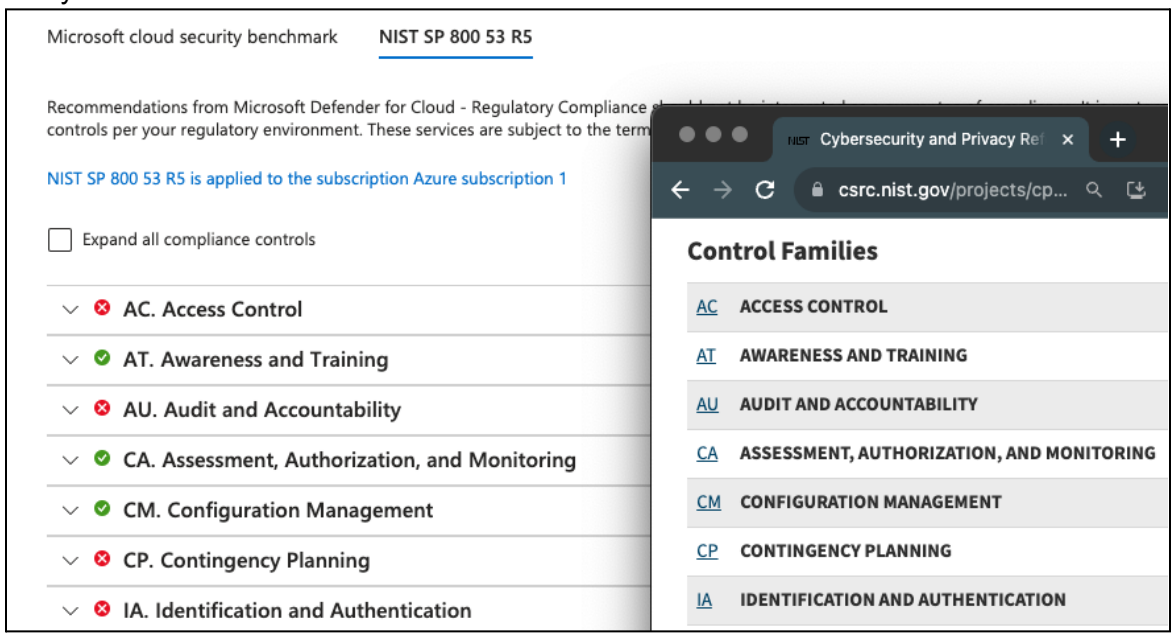
Lab #17: **Regulatory Compliance (Enable NIST 800-53)**

Purpose:

- NIST SP 800-53 has control families (see example screenshot below) containing recommended [generalized] security controls for improving the security posture of an organization.

  Source: *https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home*

  - Microsoft added this 800-53 policy to map those general controls to our Azure environment easily.



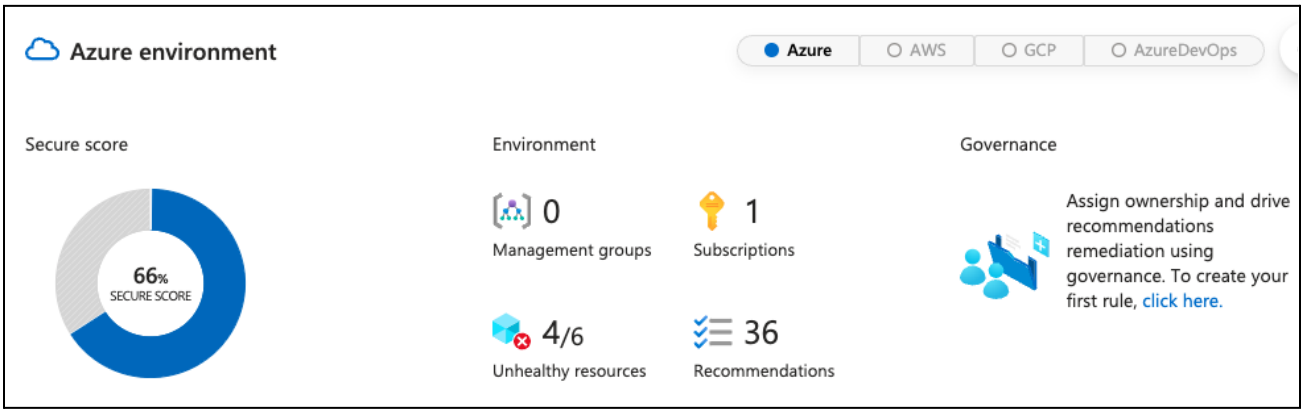
- We'll be enabling the NIST SP 800-53 option to the **Regulatory Compliance** section of **Microsoft Defender for Cloud**. This'll allow us to view security controls that we can apply to be 800-53 compliant.

Tasks:

1. **Inspect our Security Posture score (in Microsoft Defender for Cloud (MDC))**
2. **Enable Regulatory Compliance (in MDC)**
   - Add NIST SP 800-53 Security Controls
   - Wait for 800-53 Controls to Appear

Task 1: **Inspect our Security Posture score (Microsoft Defender for Cloud)**

1. **Azure** portal > **Microsoft Defender for Cloud** > **Security Posture**



2. We see that our **Secure Score** increased to 66% after we hardened our NSGs (in previous lab).
3. Select **Recommendations** to view the recommended remediations to improve our secure score.

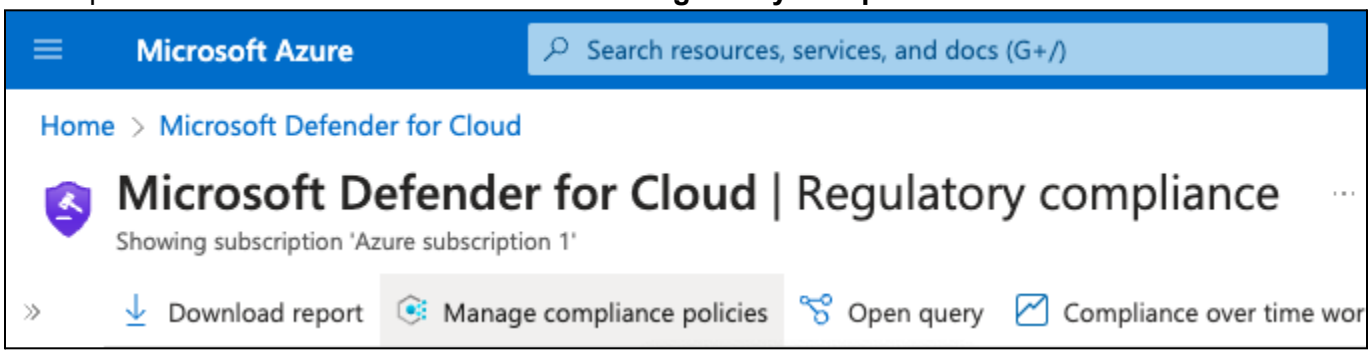
***Note**: These recommendations follow NIST SP 800-53.*

Name	Max sc...	Current score	Potential score increase	Status	Unhealthy resources
Apply adaptive application control	3	2.00	+ 2%	Unassigned	1 of 3 resources
Apply system updates	6	2.00	+ 7%	Unassigned	2 of 3 resources
Enable MFA	10	10.00	+ 0%	Completed	0 of 1 resources
Enable auditing and logging	1	1.00		Completed	0 of 1 resources
Enable encryption at rest	4	0.00	+ 7%	Unassigned	3 of 3 resources
Enable endpoint protection	2	0.00	+ 4%	Unassigned	2 of 3 resources
Enable enhanced security features	Not scored	Not scored		Unassigned	1 of 5 resources
Encrypt data in transit	4	4.00		Completed	0 of 1 resources
Implement security best practices	Not scored	Not scored		Unassigned	1 of 10 resources
Manage access and permissions	4	4.00		Completed	0 of 5 resources

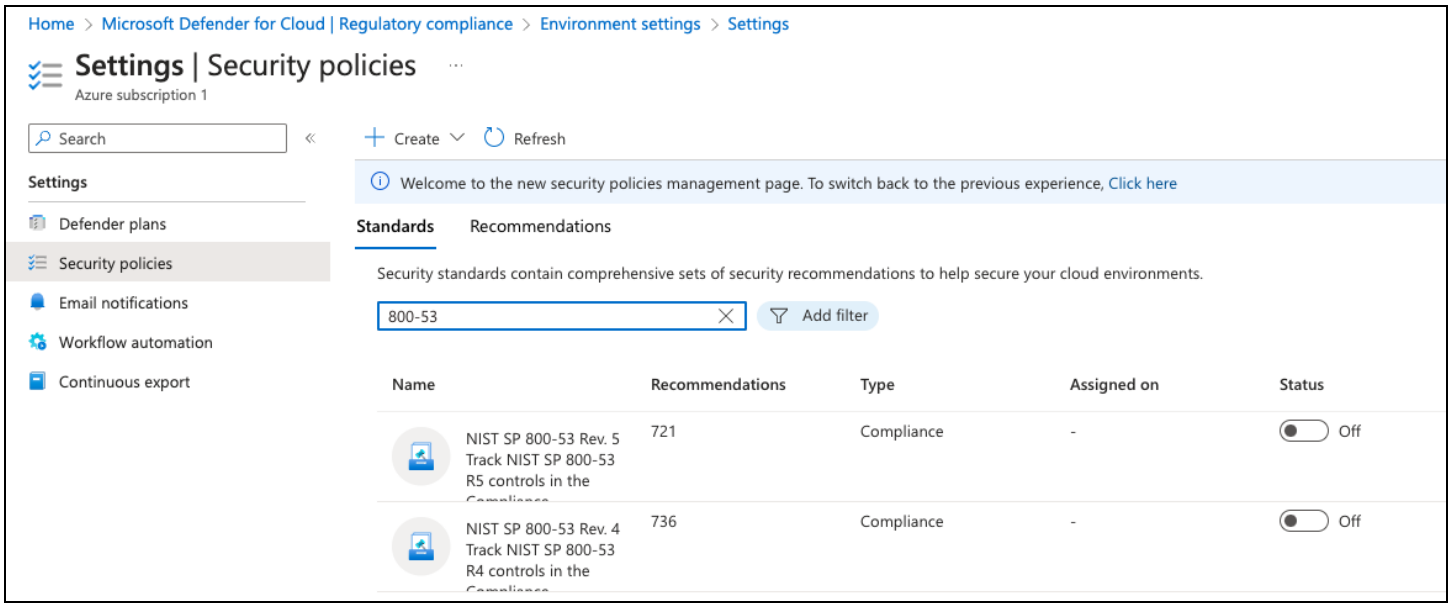
Task 2: Enable Regulatory Compliance (in MDC)

Add NIST SP 800-53 Security Controls:

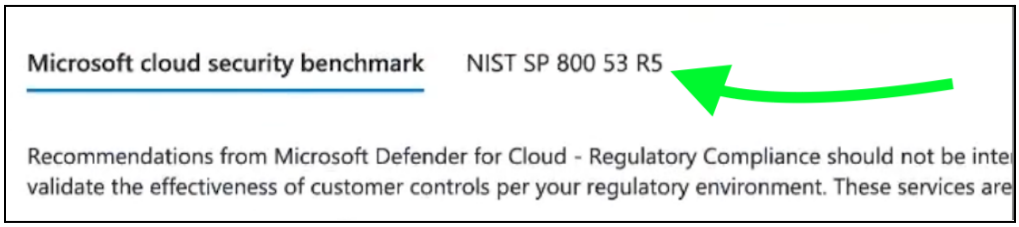
1. **Azure** portal > **Microsoft Defender for Cloud** > **Regulatory Compliance** > **Policies** >



2. Select your subscription > **Security Policies** > add **NIST SP 800-53 (R5)** > select **Edit Initiative Assignment**

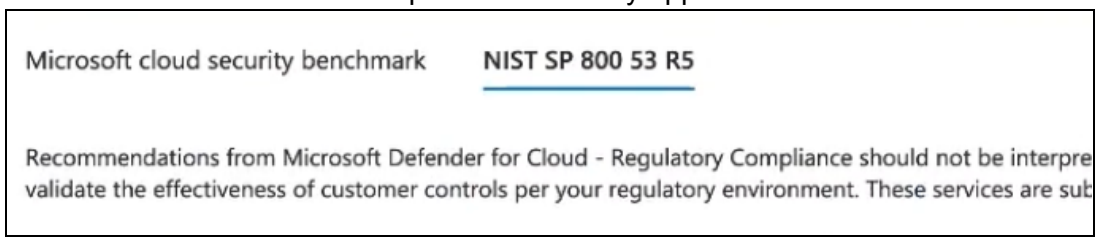


Wait for 800-53 Controls to Appear:

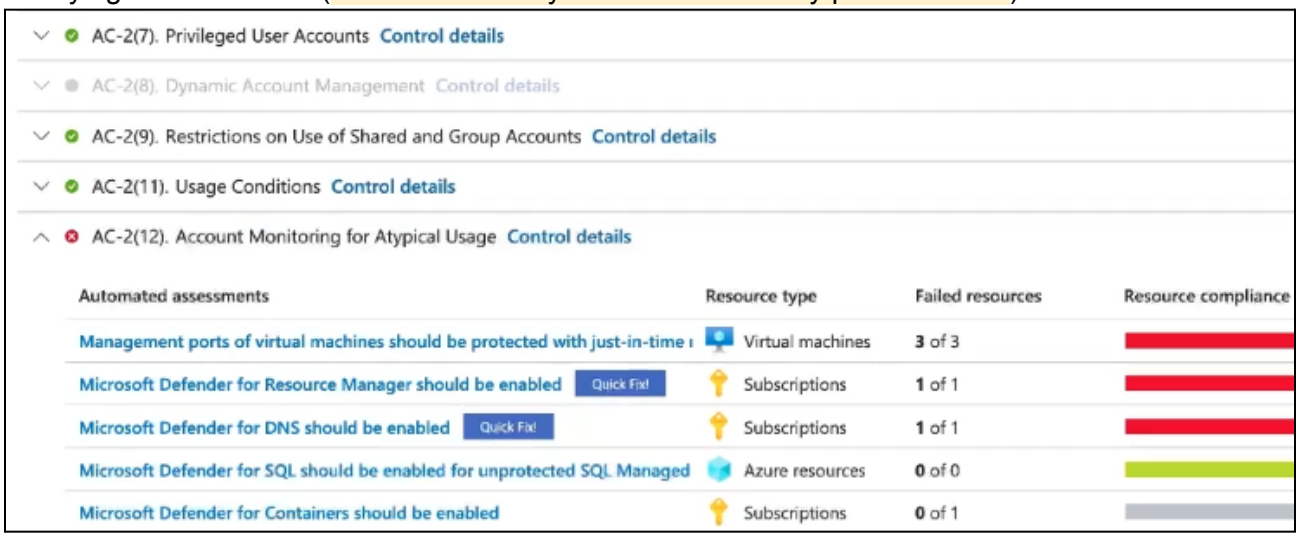


***Note**: It can take 24 hours for the 'NIST SP 800-53 controls' to appear in the **Regulatory Compliance** section of MDC. It took 15 hours for mine to appear.*

1. **Azure** portal > **Microsoft Defender for Cloud** > **Regulatory Compliance**.
2. Select the **Nist SP 800 53 R5** option that recently appeared.



3. You're now able to view the 800-53 controls & sub-controls, as well as the recommended actions for satisfying those controls (which increases your tenant's security posture score).



End:

- We added NIST 800-53 controls to our Regulatory Compliance section of Microsoft Defender for Cloud.
- In the next lab, we'll be implementing the SC-7 control ("Boundary Protection").