Azure Service Checklist

IAM Checklist:

🗹Ensure Security is enabled on Azure Active Directory.

🗹Ensure that 'Multi-Factor Auth' is 'Enabled' for all Privileged and Non-Privileged Users.

🗹Ensure that 'Allow user to remember multi-factor authentication on devices they trust' is disabled.

🗹Ensure Multi-factor Authentication is Required for Risky Sign-ins.

🗹Ensure that 'User can create Azure AD Tenants' is set to 'NO'.

🗹Ensure Access Review is Set Up for external Users in Azure AD Privileged Identity Management.

🗹Ensure Guest Users are reviewed on a regular basis.

🗹Ensure that a custom bad password list is set to 'Enforce' for your organization.

🗹Ensure that notify all admins when other admins reset their password is set to yes.

🗹Ensure 'user consent for application' is set to 'Do not allow user consent'.

🗹Ensure that 'Guest invite restrictions' is set to "Only users assigned to specific admin roles can invite guest users".

🗹Ensure That 'Restrict access to Azure AD administration portal' is Set to 'Yes'.

🗹Ensure that 'Users can create security groups in Azure portals, API, or PowerShell' is set to 'No'.

🗹Ensure that 'Owners can manage group membership requests in the Access Panel' is set to 'No'.

Microsoft Defender Checklist:

🗹Ensure That Microsoft Defender for Servers is set.

🗹Ensure That Microsoft Defender for Databases is set.

🗹Ensure That Microsoft Defender for Azure SQL Databases, servers, Open source relational databases is set.

🗹Ensure That Microsoft Defender for Storage is set.

🗹Ensure That Microsoft Defender for Containers, container components is set.

🗹Ensure That Microsoft Defender for Azure Cosmos DB, Key Vault, DNS, is set.

🗹Ensure that Auto provisioning of 'Log Analytics agent for Azure VMs' is set.

Storage Checklist:

🗹Secure transfer is enabled.

🗹Infrastructure encryption for storage account in Azure storage is set.

🗹Key rotations for each storage account.

🗹Storage account access keys are periodically regenerated.

🗹Public access is disabled for blob containers.

🗹Ensure Default Network Access Rule for Storage Accounts is Set to Deny.

🗹Private Endpoints are used to access Storage Accounts.

🗹Storage for Critical Data is Encrypted with Customer Managed Keys.

Networking Checklist:

🗹RDP, SSH, UDP, HTTP/HTTPS access from the Internet is evaluated and restricted.

🗹Network Security Group flow log retention period is 'greater than 90 days'.

🗹Network watcher is enabled.

🗹Public IP addresses are evaluated on a periodic basis.

VM Checklist:

🗹Secured privileged access.

🗹Define and implement a well-structured VMs architecture, including subnets and IP ranges, based on your network requirements.

🗹Follow the principle of least privilege by granting only necessary permissions to users and roles.

🗹Use subnets and firewall rules to segment your VM into smaller network segments, ensuring controlled access between different components or tiers of your architecture.

🗹Implement network-level firewalls to restrict inbound and outbound traffic based on specific rules.

🗹Create and enforce VM security policies to define network-level security controls and enforce consistent security configurations across your VM.

🗹Implement network-wide policies for firewall rules, subnets, and routing.

🗹Keep your VM components, such as subnets, firewall rules, and VPN gateways, up to date with the latest security patches and updates provided by Azure.

🗹Ensure that endpoint protection and only approved extensions are installed.

🗹Ensure encryption is done on both client and VM sides.

Key Vault Checklist:

🗹Expiration date is set for all keys and secrets in RBAC, Non-RBAC vaults.

🗹Ensure key vault is recoverable.

🗹Enable RBAC for Azure Key Vault.

Azure CodeBuild Checklist:

🗹Utilize Azure Identity and Access Management (IAM) to control access to CodeBuild resources.

🗹Follow the principle of least privilege by granting only the necessary permissions to users and roles.

🗹Enable multi-factor authentication (MFA) for IAM users with access to CodeBuild.

🗹Store your source code in a secure and version-controlled repository, such as Azure CodeCommit or a trusted external source control system.

🗹Regularly update and patch the operating systems and software packages in your build environments.

🗹Use dedicated build environments for different projects to minimize the risk of code contamination.

🗹Restrict network access to build environments by placing them in private subnets and configuring security groups and network ACLs accordingly.

🗹Use separate build environments for different stages of the software development lifecycle (e.g., development, testing, production) to minimize the impact of any security breaches.

🗹Avoid hard-coding sensitive information, such as API keys or credentials, directly in build specifications or source code.

🗹Enable logging for CodeBuild builds and configure logs to be stored centrally in services like Logs or storage.

🗹Stay up to date with the latest features, patches, and updates provided by Azure for CodeBuild.

🗹Implement build-time checks and tests for security-related requirements, such as secure coding practices and adherence to security policies.

🗹Encrypt environment variables that contain sensitive data in transit and at rest.

🗹Utilize code analysis tools and security scanners to identify vulnerabilities or potential security issues in your code.

🗹Stay up to date with the latest features, patches, and updates provided by Azure for CodeBuild.

CodePipeline Checklist:

🗹Ensure IAM privileges are least privileged in CI/CD.

🗹Ensure the security of the CI/CD pipeline.

🗹The production environment should not allow manual changes or SSH access.

🗹GitHub should have proper policies in place for GitHub actions.

🗹GitHub action to create and approve pull requests should be allowed (in this GitHub itself approves the pull request).

🗹Every pull request should require approval before merging into the main branch.

Azure AD Checklist:

🗹Use RBAC (Role-Based Access Control).

🗹Review access and application permissions regularly.

🗹Adopt a "Zero Trust" approach and enforce "least privileged" access.

🗹Enable MFA.

🗹Discover and classify your documents using Azure AIP.

🗹Audit your Azure AD environment.

🗹Use Microsoft Attack Simulator to identify vulnerabilities.

🗹Secure your on-premise Active Directory.

🗹Create and enforce strong passwords for all accounts.

🗹Don't forget about guest users – restrict their access as needed.

🗹Keep an eye on your Azure AD logs.

🗹Use Azure AD Conditional Access Policies to restrict access to only approved devices and apps.

🗹Configure user settings, specifically: Restrict user access to the Azure AD admin portal.