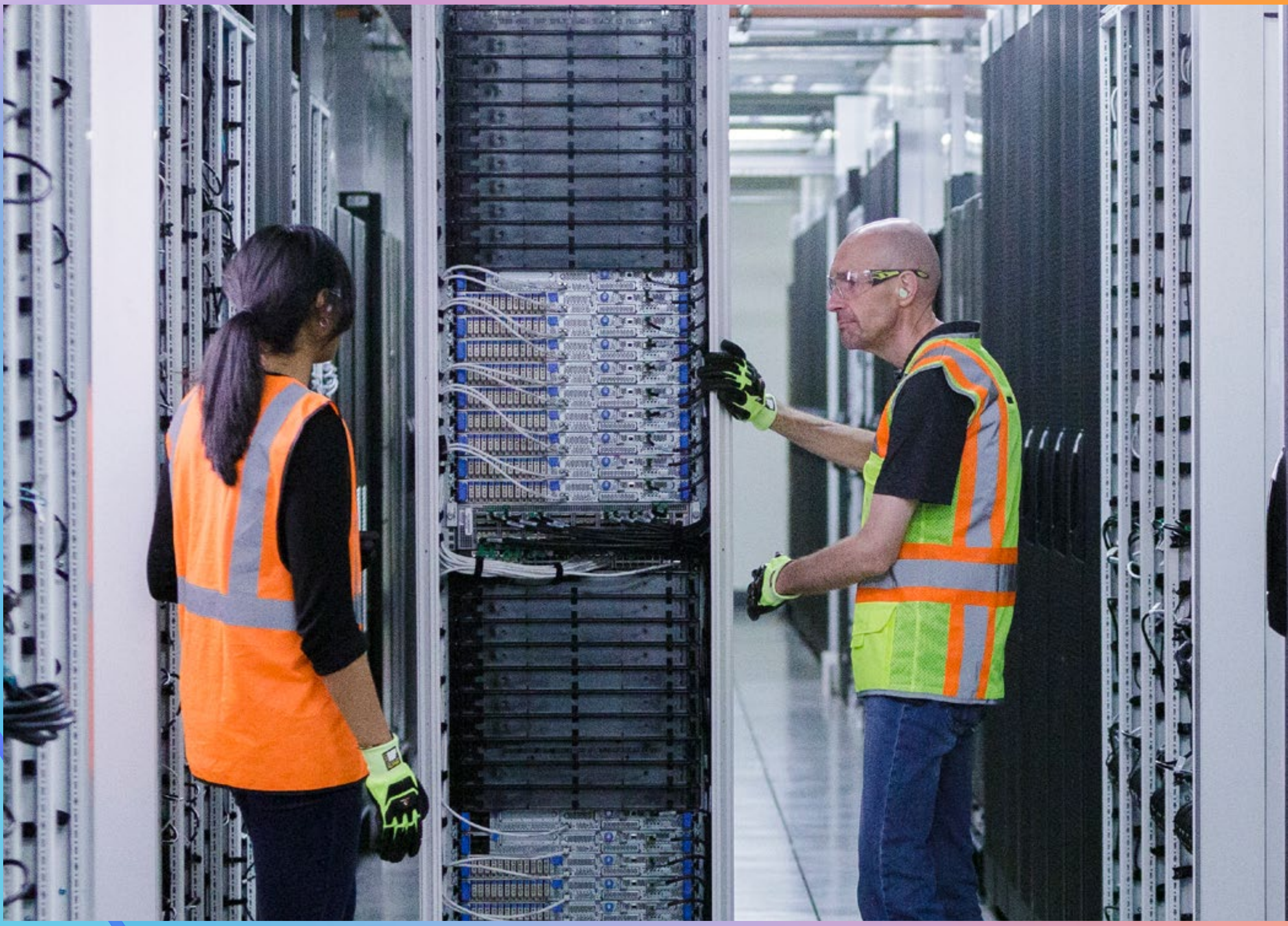
Security considerations for New Zealand North

Key points:

- Security for New Zealand North is the same as other Azure regions.

Azure regions all meet the same stringent security requirements, including physical access to datacenters, network security, and hardware- and software-layer security throughout the entire Azure environment. Whether you use New Zealand North or any other region, there's nothing different from a security perspective.

Ensure that you understand how services are deployed to New Zealand North and to other regions. Strategic services might not be available in New Zealand North at all. If you use specific security products, you might need to consider running those services in other regions, and will need to determine how this approach can meet your data residency requirements.



Data residency

Key points:

- New Zealand North provides in-country data residency. However, there are some situations where your data might leave the geography, and you need to make informed decisions about whether to allow this to happen.
- New Zealand-based customers' Microsoft 365 tenancies can be migrated to the New Zealand North region. You must purchase the Microsoft 365 Advanced Data Residency add-on to have your Microsoft 365 data migrated.

You might choose to use New Zealand North to meet data residency requirements for your workloads in the Microsoft cloud.

It's important to be aware that, in some narrow situations, data might be stored outside of your selected geography. For more information, see Data residency in Azure.

Also, if you use a wide range of Azure services, you might need to use multiple regions because not all services are available in all regions. You should carefully consider whether your services will be available in New Zealand North. For more information, see Service availability and timelines. If you depend on services that aren't available in the region, you should determine which other regions provide a good balance between your data residency requirements, resource cost, and latency.

Microsoft 365 Advanced Data Residency

Microsoft has recently improved its data residency commitments for Microsoft 365 services with the opening of new regions. This enhancement is particularly beneficial for the public sector and regulated industries, which often have stricter data residency requirements than other customers.

If you wish to migrate from Australia to New Zealand North, you need to purchase the Microsoft 365 Advanced Data Residency SKU in addition to your existing licenses (for example, E3 or E5).

When the region reaches general availability, if you have purchased the additional SKU, you can specify the destination for your tenancy migration in the Microsoft 365 portal. This step is crucial to ensure that you, as the tenancy owner, have consciously decided to migrate to the chosen destination.

The migration process is managed by Microsoft. You can monitor the progress of individual service migrations through your portal. After all services have been successfully migrated, you will receive a formal notification. This approach ensures transparency and allows you to stay informed throughout the migration process. For more information, see Advanced data residency in Microsoft 365.

Compliance and regulatory standards

Key points:

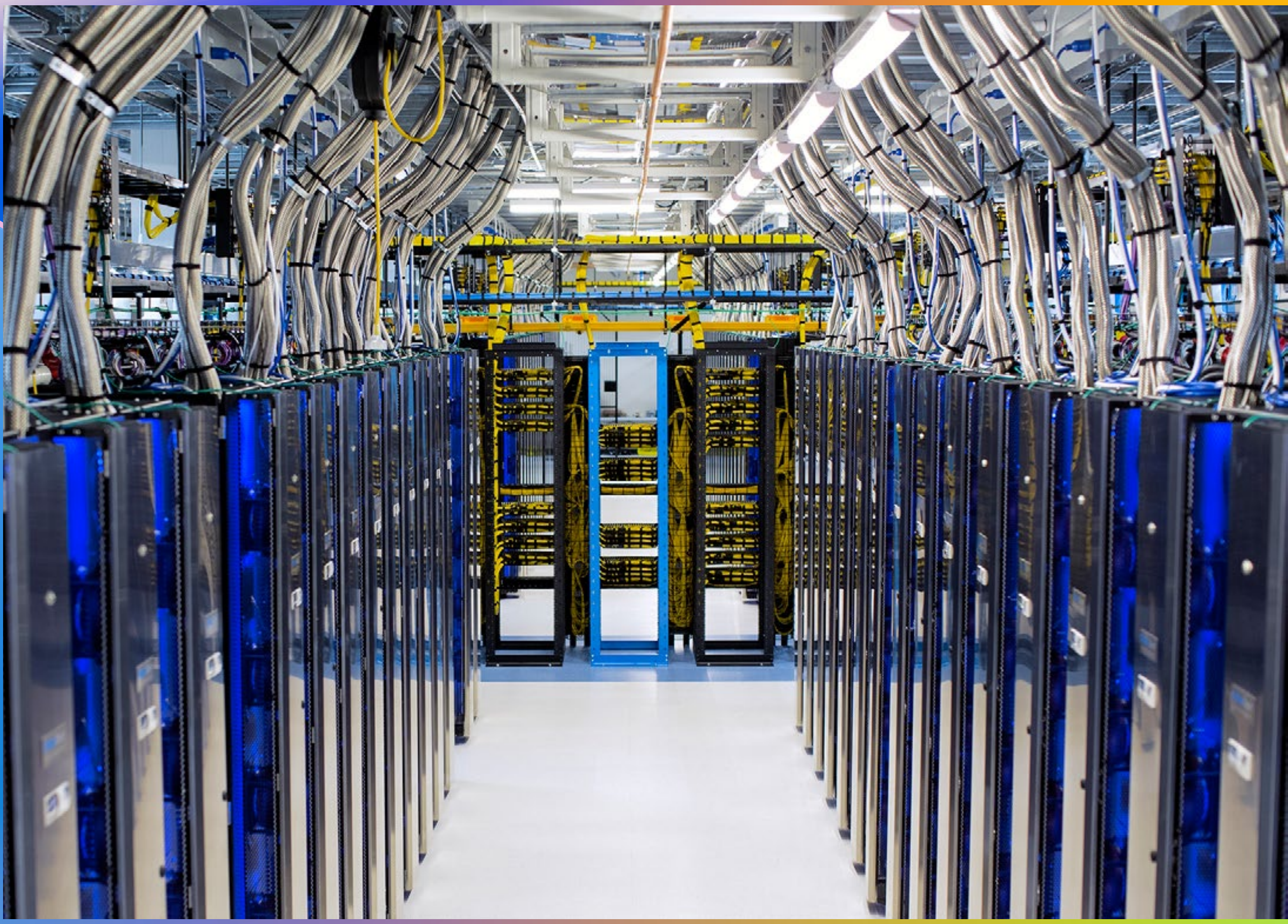
- Microsoft provides New Zealand-specific resources for compliance purposes.

Microsoft Azure and other Microsoft cloud products meet many global and New Zealand compliance and regulatory standards. See New Zealand regional guidance on the Microsoft Service Trust Portal for compliance and regulatory information here https://servicetrust.microsoft.com/ViewPage/RegionalNewZealand.

Also, for the Azure Policy initiative that corresponds to the New Zealand ISM Restricted standard, see the regularly updated download on the GCSB website here https://www.nzism.gcsb.govt.nz/resources/nzism-baseline-security-templates/ or the Azure code repository here https://github.com/Azure/Community-Policy/tree/main/policySetDefinitions/regulatorycompliance-nzism.

If you're a government agency customer, you'll need to use the Cloud Risk Discovery Tool to identify risks and controls for your workload. Microsoft provides information about the Azure platform to support this process which can be found here https://learn.microsoft.com/en-us/compliance/regulatory/offering-nz-cc-framework-nz.

If you require more information, speak to your Microsoft account team.



Microsoft Azure

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. Microsoft makes no warranties, express or implied, in this document.