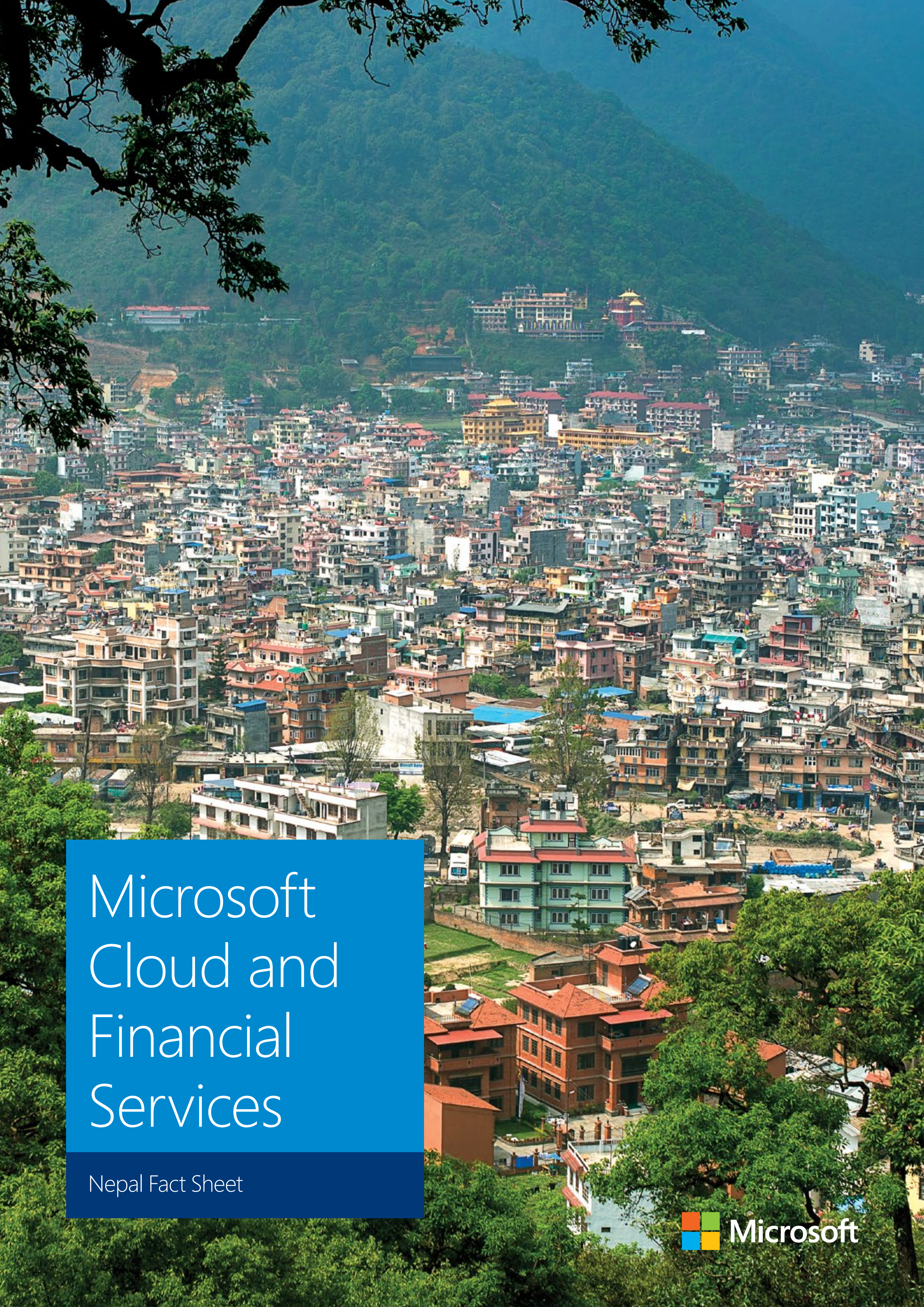

Microsoft Cloud and Financial Services

Nepal Fact Sheet

Navigating your way to the cloud

We believe that no other cloud services provider (CSP) has more experience in delivering compliant solutions to financial services institutions (FSIs) around the world than Microsoft. Microsoft actively facilitates compliance through transparent and proactive engagement both with the FSI community and with regulators.

Can banks use Microsoft cloud services in Nepal?

Yes. Nepal Rastra Bank (NRB), the central bank of Nepal, has specific guidelines that permit the use by banks of cloud computing with data centres located overseas.

Is approval needed?

No. Under the IT Guidelines 2012, banks must follow their internal outsourcing policies and assessments but do not need external approval.

Who is the regulator and what are the relevant laws and guidelines for banks in Nepal?

NRB is the regulator for banks in Nepal, from 'commercial banks' to 'finance companies' and 'micro-finance companies'.

The IT Guidelines 2012 provide banks with a framework for IT outsourcing and the Electronic Transaction Act 2008 (ETA) applies to data exchange and electronic communications.[1]

There are no specific industry requirements in relation to insurance companies or other non-bank FSIs.

What internal policies and assessments are required?

1. Put in place an IT policy with detailed operational procedures and guidelines to manage all IT operations. The IT policy should address information security measures described in the IT Guidelines. (See next page.)
2. Have a risk management policy and/or operational risk policy in place.
3. Have processes in place for monitoring and control of outsourcing activities.
4. Carry out a detailed risk analysis of the proposed solution in line with these policies.

Under the IT Guidelines 2012, NRB can inspect these policies and assessments.

Microsoft is on hand to support you throughout your transition, from initial stakeholder engagement to entering into the contract through deployment and maintaining compliance.

[1] For banks that are also state-owned enterprises, the Right to Information Act 2007 also applies and contains rules on transferring certain types of sensitive information. These rules are not addressed in this fact sheet but further information is available from your Microsoft representative on request.

Steps to a successful cloud adoption

How Microsoft helps

Establish IT outsourcing policies

- Certain policies and procedures must be approved by the board in advance of an outsourcing and reviewed periodically.
- Ultimate responsibility for a proposed outsourcing rests with the bank's board.
- Banks are required to report on a regular basis and at least annually to NRB, providing certain information including detail on outsourced activities.

Microsoft has created the Cloud Services Due Diligence Checklist (available via the **Microsoft Trust Centre**[2]). The checklist is based on the recent ISO/IEC 19086 standard.

The ISO/IEC 19086 standard offers a unified set of considerations for organisations to help them make decisions about cloud adoption, as well as create a common ground for comparing cloud service offerings.

Because it is grounded in the new standard, the checklist is service- and provider-neutral, applying to any organisation requiring cloud services and any cloud service provider.

Understand the solution

A smooth cloud adoption depends on informed stakeholder involvement from the outset, with decisions based on a full understanding of the cloud solution.

Microsoft provides detailed product and service information to ensure that decision makers have everything they need to make an informed decision.

Commitments made during the due diligence and supplier assessment stages are worth little unless backed up by binding contractual commitments. Microsoft can facilitate your compliance by demonstrating how our service agreement meets policy requirements.

We have subject-matter experts available to meet with you and your core stakeholders to provide detailed information on the technical, contractual and practical aspects of your proposed cloud project.

Safeguard information security with a compliant contract

The IT Guidelines 2012 include various specific requirements on security of information in connection with an outsourcing, which should be addressed in the contract.

- Data located abroad must be subject to a suitable control mechanism including strict access controls and the segregation of data.
- Service providers must implement adequate controls to ensure compliance with the bank's information security and privacy policies.
- Banks must ensure that the outsourcing does not interfere with or obstruct NRB in the exercise of its regulatory and supervisory function.

The ETA requires that electronic data exchange and electronic communications be reliable and secure.

At Microsoft, we believe that confidentiality and security of our customers' information are core pillars of a trusted cloud environment.

- Microsoft applies strict controls on access to customer data. Personnel access to the IT systems that store customer data is strictly controlled via role-based access control and 'lock box' processes. Access control is an automated process that follows the separation of duties principle and the principle of granting least privilege.
- Microsoft isolates its customer data from its own and that of any of its other customers.
- Microsoft cloud services are compliant with a broad range of national, international, regional and industry-specific compliance standards, such as ISO/IEC 27001, ISO/IEC 27018, SOC 1 and SOC 2, and are independently audited annually.
- Microsoft makes specific commitments to financial services customers to help ensure that its contractual framework meets regulatory requirements, including express commitments to support any financial services regulators who require direct examination of Microsoft cloud services operations and controls.
- Microsoft cloud services are subject to a mandatory development process that incorporates privacy and security requirements into every phase of the development process. We also use various technological safeguards such as encrypted communication of data 'at rest' and 'in transit' to safeguard customer information.
- Data that resides in Microsoft's cloud services belongs to the customer, not Microsoft. For further information, please visit the **Microsoft Trust Centre**.

[2] www.microsoft.com/en-us/trustcenter/Compliance/due-diligence-checklist

Microsoft

Find out more

Microsoft has available a range of materials, including product fact sheets, checklists and online trust centres.

Trust Center
microsoft.com/trustcenter

Service Trust Portal
aka.ms/trustportal

Online Services Terms
microsoft.com/contracts

Service Level Agreements
microsoft.com/contracts

Financial Services Amendment
Contact your Account Manager

Compliance program for regulated financial services customers
Contact your Account Manager

SAFE Handbook
aka.ms/safehandbook

Financial services compliance program

In addition, **Microsoft's financial services compliance program** goes further to ensure that you have access to all the information needed to make an informed decision.

The program extends the compliance features of Microsoft Azure, Office 365, Dynamics and Windows Intune to provide deeper, ongoing engagement with Microsoft. Features of the program include:

- Access to additional information from Microsoft subject-matter experts (SMEs).
- Access to additional compliance-related information developed by Microsoft over time.
- The opportunity for one-to-one discussions with Microsoft's third-party auditors.
- Participation in webcast walk-throughs of ISO and SSAE audit reports with Microsoft SMEs.
- The ability to view the Microsoft control framework for the cloud services.
- The opportunity to recommend future additions to the audit scope of the cloud service.
- Access to detailed reports of external audit penetration tests conducted on the cloud service.