






# Evaluate risk tolerance

04/04/2019 • 8 minutes to read • Contributors     

## In this article

[What business risks are associated with a cloud transformation?](#)

[Understanding risk tolerance](#)

[Simple use case for comparison](#)

[Risk tolerance questions](#)

[Next steps](#)

Every business decision creates new risks. Making an investment in anything creates risk of losses. New products or services create risks of market failure. Changes to current products or services could reduce market share. Cloud transformation does not provide a magical solution to everyday business risk. To the contrary, connected solutions (cloud or on-premises) introduce new risks. Deploying assets to any network connected facility also expands the potential threat profile by exposing security weaknesses to a much broader, global community. Fortunately, cloud providers are aware of the changes, increases, and addition of risks. They invest heavily to reduce and manage those risks on the behalf of their customers.

This article is not focused on cloud risks. Instead it discusses the business risks associated with various forms of cloud transformation. Later in the article, the discussion shifts focus to discuss ways of understanding the business' tolerance for risk.

## What business risks are associated with a cloud transformation?

True business risks are based on the details of specific transformations. Several common risks provide a conversation starter to understand business-specific risks.

### Important

Before reading the following, be aware that each of these risks can be managed. The goal of this article is to inform and prepare readers for more productive risk management discussions.

- **Data breach:** The number one risk associated with any transformation, is the protection of data. Data leaks can cause significant damage to your company, leading to loss of customers, decrease in business, or even legal liability. Any changes to the way data is stored, processed, or used creates risk. Cloud transformations create a high degree of change regarding data management, so the risk should not be taken lightly. [Security Baseline](#), [Data Classification](#), and [Incremental Rationalization](#) can each help manage this risk.
- **Service disruption:** Business operations and customer experiences rely heavily on technical operations. Cloud transformations will create change in IT operations. In some organizations, that change is small and easily adjusted. In other organizations, these changes could require retooling, retraining, or new approaches to support cloud operations. The bigger the change, the bigger the potential impact on business operations and customer experience. Managing this risk will require the involvement of the business in transformation planning. Release planning and first workload selection in the [incremental rationalization](#) article discuss ways to choose workloads for transformation projects. The business's role in that activity is to communicate the business operations risk of changing prioritized workloads. Helping IT choose workloads that have a lower impact on operations will reduce the overall risk.

- **Budget control:** Cost models change in the cloud. This change can create risks associated with cost overruns or increases in the cost of goods sold (COGS), especially directly attributed operating expenses. When business works closely with IT, it is feasible to create transparency regarding costs and services consumed by various business units, programs, or projects. [Cost Management](#) provides examples of ways business and IT can partner on this topic.

The above are a few of the most common risks mentioned by customers. The Cloud Governance team and the cloud adoption teams can begin to develop a risk profile, as workloads are migrated and readied for production release. Be prepared for conversations to define, refine, and manage risks based on the desired business outcomes and transformation effort.

## Understanding risk tolerance

Identifying risk is a fairly direct process. IT-related risks are generally standard across industries. However, tolerance for these risks is specific to each organization. This is the point where business and IT conversations tend to get hung up. Each side of the conversation is essentially speaking a different language. The following comparisons and questions are designed to start conversations that help each party better understand and calculate risk tolerance.

## Simple use case for comparison

To help understand risk tolerance, let's examine customer data. If a company in any industry posts customer data on an unsecured server, the technical risk of that data being compromised or stolen is roughly the same. However, a company's tolerance for that risk will vary wildly based on the nature and potential value of the data.

- Companies in healthcare and finance in the United States, are governed by rigid, third-party compliance requirements. It is assumed that personally identifiable information (PII) or healthcare-related data is extremely confidential. There are severe consequences for these types of companies, if they are involved in the risks scenario above. Their tolerance will be extremely low. Any customer data published inside or outside of the network will need to be governed by those third-party compliance policies.
- A gaming company whose customer data is limited to a user name, play times, and high scores is not as likely to suffer any significant consequences, if they engage in the risky behavior above. While any unsecured data is at risk, the impact of that risk is small. Therefore, the tolerance for risk in this case is high.
- A medium-sized enterprise that provides carpet cleaning services to thousands of customers would fall in between these two tolerance extremes. There, customer data may be more robust, containing details like address or phone number. Both could be considered PII and should be protected. However, there may not be any specific governance requirement mandating that the data be secured. From an IT perspective, the answer is simple, secure the data. From a business perspective, it may not be as simple. The business would need more details before they could determine a level of tolerance for this risk.

The next section shares a few sample questions that could help the business determine a level of risk tolerance for the use case above or others.

## Risk tolerance questions

This section lists conversation provoking questions in three categories: loss impact, probability of loss, and remediation costs. When business and IT partner to address each of these areas, the decision to expend effort on managing risks and the overall tolerance to a particular risk can easily be determined.

**Loss impact:** Questions to determine the impact of a risk. These questions can be difficult (sometimes impossible) to answer. Quantifying the impact is best, but sometimes the conversation alone is enough to understand tolerance. Ranges are also acceptable, especially if they include assumptions that determined those ranges.

- Does this risk violate third-party compliance requirements?

- Does this risk violate internal corporate policies?
- Could this risk cost customers or market share? If so, can this cost be quantified?
- Could this risk create negative customer experiences? Are those experiences likely to affect sales or revenue realization?
- Could this risk create new legal liability? If so, is there a precedence for damage awards in these types of cases?
- Could this risk stop business operations? If so, how long would operations be down?
- Could this risk slow business operations? If so, how slow and how long?
- At this stage in the transformation, is this a one-off risk or will it repeat?
- Does the risk increase or decrease in frequency as the transformation progresses?
- Does the risk increase or decrease in probability over time?
- Is the risk time sensitive in nature? Will the risk pass or get worse, if not addressed?

These basic questions will lead to many more. After exploring a healthy dialogue, it is suggested that the relevant risks be recorded and when possible quantified.

**Risk remediation costs:** Questions to determine the cost of removing or otherwise minimizing the risk. These questions can be fairly direct, especially when represented in a range.

- Is there a clear solution? What does it cost?
- Are there options for preventing or minimizing this risk? What is the range of costs for those solutions?
- What is needed from the business to select the best, clear solution?
- What is needed from the business to validate costs?
- What other benefits can come from the solution that would remove this risk?

These questions oversimplify the technical solutions needed to manage or remove risks. However, these questions communicate those solutions in ways the business can quickly integrate into a decision process.

**Probability of loss:** Questions to determine how likely it is that the risk will become a reality. This is the most difficult area to quantify. Instead it is suggested that the Cloud Governance team create categories for communicating probability, based on the supporting data. The following questions can help create categories that are meaningful to the team.

- Has any research been done regarding the likelihood of this risk being realized?
- Can the vendor provide references or statistics on the likelihood of an impact?
- Are there other companies in the relevant sector or vertical that have been hit by this risk?
- Look further, are there other companies in general that have been hit by this risk?
- Is this risk unique to something this company has done poorly?

After answering these questions along with questions as determined by the Cloud Governance team, groupings of probability will likely emerge. The following are a few grouping samples to help get started:

- No indication: Not enough research has been completed to determine probability.
- Low risk: Current research indicates realizing the risk is unlikely.
- Future risk: The current probability is low. However, continued adoption would require a fresh analysis.
- Medium risk: It's likely that the risk will affect the business.
- High risk: Over time, it is increasingly likely that the business will realize this risk.
- Declining risk: The risk is medium to high. However, actions in IT or the business are reducing the likelihood of an impact.

### **Determining tolerance:**

The three question sets above should fuel enough data to determine initial tolerances. When risk and probability are low, and risk remediation costs are high, the business is unlikely to invest in remediation. When risk and probability are high, the business is likely to consider an investment, as long as the costs don't exceed the potential risks.

# Next steps

This type of conversation can help the business and IT evaluate tolerance more effectively. These conversations can be used during the creation of MVP policies and during incremental policy reviews.

Define corporate policy