Microsoft

Reduce cost and manage risk with Microsoft 365

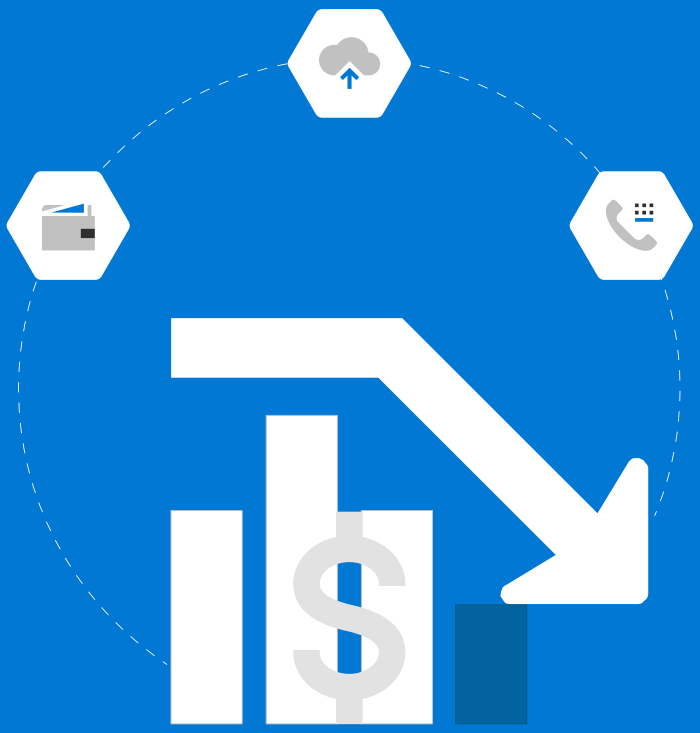

Table of Contents

How to use this guide

This telesales guide provides call scripts, proof points, questions, and guidelines you can use to drive sales conversations with small and medium-sized business (SMB) customers.

The purpose of this call is to discuss subscribing or upgrading to Microsoft 365 with a business decision maker (BDM) at a company up to 300 employees. Present Microsoft 365 with Microsoft Teams to spark interest with customers:

- Explain how the cost savings and enhanced security features available in Microsoft 365 can help customers save money while protecting their devices and data.
- After the call, connect them with a partner to help them buy and deploy Microsoft 365 with Teams.

Call objectives

The **primary objective** of this call is to sell Microsoft 365.

Additional objectives include:

- Inform SMB decision makers how Microsoft 365 can help them reduce costs and manage risk.
- Focus on SMB business needs and how Microsoft 365 helps mitigate challenges presented by global economic changes.

Call flow

1. Empathize with customer on uncertainty of global economic situation.
2. Seek to understand what kinds of productivity and security challenges customer is facing.
3. Discuss Microsoft 365 features and benefits and see if customer is interested.
4. If relevant, share customer-facing content (e.g. product pages, toolkits, reports, etc.).
5. Close out with relevant next steps.
6. Qualify Lead to Opportunity in MSX and follow up with partner.

Background

Before you make your call, here is some context around the challenges SMBs face today as they react to changes in the marketplace. Global pandemic and economic changes have negatively impacted the SMB sector and created a need among SMBs to enable a remote working model while they are unable to operate onsite. SMBs also face financial pressure to keep costs low while maintaining a high level of security to protect their data and assets. Microsoft 365 can help address these challenges.

General trends and challenges are affecting the business priorities for BDMs who need to stay productive while minimizing risks and costs.

- SMBs are focused on addressing internal challenges brought on by changes in the global economic landscape. Challenges include boosting employee productivity, improving remote collaboration, empowering employees with secure access to data, and managing costs and cashflow.

- Security risks are an ever-present concern, but especially so for businesses trying to manage new remote work models. Cyberattacks and phishing threats have increased, and the average cost of a security attack is $149K[1].
- SMBs are reducing their workforce, with many expected to have 40%[2] fewer employees now than in the beginning of 2020.
- Economic downturn is forcing businesses to be extra cost conscious, as an estimated 68%[3] of US SMBs have reduced business spending.
- Regardless of whether an SMB is experiencing growth or a downturn financially, they may be interested in investing in tools for secure remote and onsite work to maintain operations.

Microsoft Privacy Requirements

Please be sure to follow the guidelines below on your calls, as required by Microsoft Privacy standards. For a full breakdown of privacy considerations for field sales calls, see the Privacy notes section at the end of this document.

1. The caller **must always state that they are calling on behalf of Microsoft.**
2. The caller **must present the customer with options to opt out of the call if requested.** If the customer requests to opt out, the caller must honor it and steps must be followed in MSX to ensure that the customer is not called again.
3. The customer **must be referred to the Microsoft Privacy Statement** if requested. Use the below statement to guide the customer:

   "Upon request, if customers want to verify the legitimacy of this call, we can provide information about where to find the Microsoft privacy statement and whom to contact (https://aka.ms/privacy)."

4. The **contact for the call should be called out** (i.e. Sales Manager, IT Manager, Operations Manager, etc.).

5. The caller **must always collect consent from the customer before sharing their data with a partner.**

[1] US and Canada avg recovery costs, Kaspersky Lab Report 2018

[2] Harvard Business School Survey

[3] McKinsey, AnalysysMason

Understand the customer's cost and security concerns

Call script

Hello, my name is <*insert name*>. I'm calling on behalf of Microsoft to talk with you as a <*contact role*> about reducing cost and managing risk for your business in the current economic landscape. Would you mind if I ask you some questions to better understand how you manage costs?

Pause.

If they decline, ask if they are interested in learning more about Microsoft 365.

- *If they say **yes**, proceed to the value prop section.*
- *If they say **no**, thank them for their time and update their record in MSX if required (see Privacy notes).*

If they wish to continue talking, proceed with the following:

Many companies find it difficult to enable remote work and maintain data security while keeping costs down. With impacts to workforces and supply chains on a global scale, reducing operational costs has become a top priority for many. Have you faced any of these struggles?

Pause.

*If **yes**:*

You're not the only one. I'm interested in learning about your experience with controlling cost and security challenges.

Would you mind if I ask you some questions to better understand your challenges and business needs?

*If **no**:*

That's good to hear! I'd like to learn more about how you've overcome or prevented these challenges, and how you successfully manage your costs and minimize risk currently.

Would you mind if I ask you some questions to better understand your challenges and business needs?

Pause.

*If they **accept**: proceed by asking the questions below.*

*If they **decline**: ask if they are interested in learning more about Microsoft 365.*

- *If they say **yes**, proceed to the value prop section.*
- *If they say **no**, thank them for their time and update their record in MSX if required (see Privacy notes).*

The following questions are designed to help you understand the contact's business and challenges. Ask the questions on the left and follow up with questions on the right, adjusting as needed based on their responses. Ensure the contact feels heard.

Reduced costs and increased ability to save

Do you maintain any physical office locations?	• Are you experiencing any financial pressure from managing physical work sites while employees work remotely? • Have you had to downsize or reduce your physical work sites at all?
What applications or tools do you use to communicate, collaborate, and keep your data secured?	• Have you had to acquire new tools or solutions to maintain productivity? • Is the cost of adopting new productivity tools preventing you from implementing them? • Are you struggling with managing the invoices for multiple tools? • Do your applications or tools work well together? • Do you ever wish you had one integrated solution that had all the productivity tools you need in one place?

Protection from unseen risks

Has the risk of potential data breaches and cyberattacks been a concern for you?	• *If **yes**, reassure them.* You're not alone. Our research shows that 50% of small businesses have experienced an attack in the past year[4]. • *If **no**, congratulate them, and ask them about what they are doing that is giving them peace of mind.*
What sort of technology does your company use to protect sensitive information? **Note:** *Sensitive information could include personally identifiable information, the credit card numbers of customers, and data that is vital to running the business—like intellectual property or financial information.*	• Do you encrypt data? • Do you have cloud backups for all your data, or is everything backed up on-premises?
How do you protect the information when your employees are using personal devices?	• What processes do you have in place and what technology do you use to control access to company data?
What is your strategy for protecting your business from security attacks?	• What sorts of products and vendors do you use to protect against attacks? How do they work together? Is this a big expense for your company?

[4] Microsoft commissioned Forrester Research, 2020

	• Is constantly managing your security time consuming for you and your staff? This could include time spend daily, time training staff on new products, and so on. • Are you concerned about the security risks of running old software on computers and other devices?

Productivity and remote work

Is remote work disrupting your employee's productivity?	• Do you need to acquire new tools or software solutions to maintain productivity? • Is constantly managing your security time consuming for you and your staff?
Have you noticed any decrease in your employees' efficiency or morale when working remotely?	• Does collaborating with them raise challenges for you—in sharing files and communicating securely or in the tools you use? • Do you feel like your employees have the tools they need to get their work done?
How do you handle the security of the devices that your employees use to access company data? **Note:** *Devices include mobile phones, tablets, and PCs and different operating systems like iOS, macOS, Windows, or Android.*	• How do you control access to those devices, particularly when they are remote? • What policies or security measures do you have in place to control which devices, users, and apps can access company data?
Are you concerned about new security risks that might arise with remote work?	• Have you taken steps to enable secure remote work for your employees? • What tools, if any, are you using to enable secure remote work?

Explain the value of Microsoft 365 as a cost-effective productivity solution

Note – *Promote the parts of the value proposition that align with the customer's top concerns voiced in response to your questions. Support it with the corresponding benefit statements.*

Microsoft 365 value proposition

Thanks for answering my questions. Based on our conversation, I think Microsoft 365 could help you to reduce costs and manage risk. Would you like to hear more about it and what it can do for your company?

*If **no**, thank them for their time and update their record in MSX if required (see Privacy notes).*

*If **yes**, proceed with the value prop below.*

Microsoft 365 with Microsoft Teams is a cost-effective cloud solution for real-time collaboration and secure work from anywhere. It includes Microsoft Teams, cloud storage, and familiar Office apps with advanced security options. People can use it to chat, call, host online meetings, and collaborate in real time for remote and onsite work. **It is an integrated solution that allows your team to get work done securely, all in one place.**

Microsoft 365 offers one complete toolset that can help you accomplish your goals. You can reduce costs and administration with one subscription that includes videoconferencing, chat, online storage, and familiar productivity apps like Word, Excel, and PowerPoint. Built-in security is also featured across all Microsoft 365 plans, including regulatory standards, data encryption, and account protection.

In addition to these built-in features, advanced security options are available with Microsoft 365 Business Premium, such as remote desktop access, device management, and identity protection that can help safeguard your business and minimize risk in a changing economic environment.

This single, scalable productivity platform is easy to deploy, manage, and use—and is typically more cost effective than individual technologies you might purchase from separate vendors. In short, it offers enterprise-grade value at an affordable price for many small and medium-sized businesses.

Here are some ways our clients are managing cost and risk with Microsoft 365:

- Reducing vendor license cost by consolidating to a single platform versus buying standalone products for different capabilities.
- Lowering risk of breaches with enhanced privacy, remediation, and compliance.
- Eliminating or limiting physical costs like real estate, utilities, travel, and entertainment through secure remote work.
- Saving money by streamlining business processes with workflows, dashboards, and automation.
- Optimizing cash flow management by changing upfront license payments to operating expenses.

Supporting benefit statements

Note – *The content below allows you to dive deeper into the features and capabilities that may be relevant to your customer. Use as needed based on the direction of the conversation.*

Features	Benefits of Microsoft 365 Business
Vendor license cost consolidation. Consolidate to a single platform versus buying standalone licenses for different capabilities.	• Lower your overall cost by using one integrated solution and reducing the number of vendor licenses and overall business expenses. • Simplify the user experience with fewer "learning curves" and interfaces, less training, and a more integrated experience for end users. • Simplify your billing by only getting one bill from a trusted technology partner. • Streamline IT setup and make management easier with fewer admin centers and tech support relationships to manage.
Reduce total cost of risk. Reduce breaches and enhance privacy and remediation with better security. Help reduce risk through improved compliance.	• Get fewer risks for end users by reducing the number of successful security attacks and cyberthreats targeting end users, like phishing, viruses, and ransomware attacks. • Protect your business by helping prevent data loss resulting from employee mistakes, hardware failures, and unauthorized access with enterprise-grade value at an affordable price. • Focus on managing your business, not IT, by relying on technology from a trusted provider designed to safeguard businesses and their data.
Physical and travel cost displacement. Reduce hard costs like real estate, utilities, travel, and entertainment through secure remote work.	• Reduce traditional business costs associated with physical operations like real estate and utilities through secure remote work. • Save on travel and entertainment expenses with virtual events and online meetings.
Save on automation and process improvements. Transform business processes and save using workflows, dashboards, and AI while increasing employee productivity.	• Save time and money with improved business processes like digitizing paper workstreams and automating manual processes. • Take advantage of the opportunity to customize with Microsoft Teams, an extensible platform that offers a solution for building low-code apps with Power Apps and makes it easy to directly integrate third-party apps.
Capex to Opex cash flow. Optimize cash flow management by changing upfront license payments to operating expenses.	• Lower your capex licensing fees and avoid costs associated with on-premise software purchases by switching to a subscription-based license plan.

Answer questions and address concerns

Note – *The below content is designed to provide you with answers and context to common questions and concerns. This list is not exhaustive. Work with your team to ensure you are prepared for questions relevant to your area/focus.*

Question/Concern	Caller response
We are already using a competitor tool/solution, so I'm not sure we would benefit from switching. What makes your solution different, and/or why should I consider switching?	**Note:** *These resources are for the education of the caller only and are **NOT to be shared externally or with the customer**. Use the below resources to help overcome any compete objections and differentiate Microsoft 365 from other products in the marketplace.* • Security Overcoming Objections (SMB resource) • Modern Work Compete (all commercial resources) • Zoom Battlecard (commercial resource) • Google Battlecard (commercial resource)
A lot is changing in the market right now. I'm not sure we can afford to start using a new tool.	The changing market landscape has forced many businesses to find solutions that enable them to stay productive while working remotely, so there's no better time to find a tool that can help you operate efficiently and securely. There are many good productivity tools available, but Microsoft 365 offers an integrated solution with the productivity solutions customers need – and the price is potentially lower than the collection of comparable products from other vendors.
I'm concerned about the subscription-based price compared to the one-time expense I'm used to. I'm not sure I want a monthly subscription or an annual contract.	Microsoft 365 plans are less expensive and easier to manage than a comparable collection of third-party solutions from other vendors, as any Microsoft 365 plan provides an all-in-one solution for collaboration, communication, and security. In fact, our subscriptions start at $5/user/month (with an annual commitment) with Microsoft 365 Business Basic. And even Microsoft 365 Business Premium – which offers advanced security including remote access and identity protection, security for devices, and data protection – costs $20/user/month, whereas the estimated monthly cost of similar third-party solutions is closer to $40.[5]

[5] **Estimates based on published prices;** File Storage and Productivity apps – GSuite $12 (unlimited storage) Online chat-based collaboration – Slack $6.67; Single Sign On– Okta $2; Adaptive MFA (Conditional Access+ MFA) – Okta $6; Device Management - IBM MaaS360- $4.00, Endpoint Protection – Kaspersky - $3.38, Proofpoint email protection - $5; Remote Access: Windows Terminal server CAL ($199 perpetual per user; over 3 years – per month would be around $5); TeamViewer - $49 per user per month

	You also get more value from subscription-based cloud services than you do from locally installed software: • Regular updates with the latest capabilities. • Billing options both monthly or annually; the subscription fee doesn't require access to credit.
I'm not sure that the costs of a security breach warrant the expense of new software.	Research shows that the average cost of a security attack for small businesses is around $149,000.[6] That is a significant financial impact. Another concern is that 50% of small businesses have experienced an attack in the last year.[7] It's certainly understandable to be wary of new expenses, especially now, but the cost of a cyberattack or data breach can far outweigh the additional expense of the robust security features included in Microsoft 365 Business Premium. **Note:** *You can also direct customers to the ROI calculator to give them a more tangible amount for their return on investment.*
I'm concerned about training and implementation costs.	Office integration enables your workers to use the Office apps that are deeply familiar to many—like Word, Excel, PowerPoint, Outlook, etc. New software makes remote work more available to employees, which is critical for maintaining productivity in the current economic landscape. Microsoft 365 brings together videoconferencing, chat, file storage, and document editing all in one place with Microsoft Teams – which makes training easier when compared to using separate applications from different vendors. **Note:** D*irect customers to https://aka.ms/SmallBusinessHelpAndLearning for additional help and learning resources.*

[6] US and Canada avg recovery costs, Kaspersky Lab Report 2018

[7] Microsoft commissioned Forrester Research, 2020

Relevant actions and next steps

Connecting with a partner

From our conversation, it sounds like the features of Microsoft 365 could help you reduce costs and enhance your team's ability to collaborate securely.

***As a way of recapping**, reference some of the features that resonated with the customer during your call.*

If this is correct, and you're interested in an upgrade/subscription to Microsoft 365, I think it makes sense to connect you with someone who has in-depth knowledge of the business issues you're facing and a broad understanding of how Microsoft 365 can help address them.

Do you already have a partner who you're comfortable working with, and who can provide additional solution expertise, pricing, and other details for this transaction? If you don't have a partner, or would like to try a new partner, I'd also be happy to provide some options for partners in your area who have the required expertise.

*If they **already have a partner**:*

That's great! May I ask for that partner's name? If it's okay with you, I'll reach out to them to discuss your interest and they will follow up with you directly.

(**Note:** *Find the partner in the Refer & Track tool and send the contact's info via this tool.*)

*If they **want other partner options**:*

No problem. May I present three other options for partners in your area who can help you?

Thanks! If you don't mind, can I make sure I have the right contact information for you? I'll send your contact info to them and they will follow up with you directly.

- Confirm contact information
- Confirm customer contact preferences (email v. call)
- Ask permission to share their information with the partner
- Set expectations for next outreach, if applicable

Thanks for talking with me today. If you have any questions at all, please reach out to me. My email address is <email> or you can call me at <xxx-xxx-xxxx>.

(**Note:** *customer and partner content links available on next page.*)

Customer-specific content

OnRamp links to customer-specific content:

- Reduce cost and manage risk overview
- Enable secure remote work overview
- Microsoft Teams overview
- Microsoft 365 Business Premium overview
- Microsoft 365 Business Voice overview

Partner-specific content

OnRamp links to partner-specific content:

- Commercial Consulting Tool

Resources to share with partner for overcoming objections and differentiating Microsoft 365 from competing products in the marketplace:

- Learn to position Microsoft Teams

Privacy notes

Sellers need to provide customers with a method to opt out, and honor any of their requests to do so. Do not discourage customers from opting out or prevent them from opting out.

If the customer isn't interested in talking but does not verbally opt out or ask to not be called again, there is no need to change their contact preference to **"do not contact" (DNC)** in MSX.

If the customer makes it clear they do not want to be contacted by Microsoft, change their contact preference as described below:

- If the customer is marked **"okay to contact" (OKC)** or **"Unknown"** in MSX, switch them to **"do not contact" (DNC)** for telesales in MSX. Explain to the customer that while they will no longer receive promotional calls from Microsoft, they may still receive service communications, such as calls related to previously purchased products reaching end of support/licensing compliance.
- If the customer is marked **DNC** in MSX, explain to the customer that they are already opted out of receiving promotional calls from Microsoft, but they may still receive service communications, such as calls related to previously purchased products reaching end of support/licensing compliance.

If the customer wants to verify the legitimacy of the call or would like to have further information in terms of the privacy statement, you can guide the customer in the following way:

"Upon request, if customers want to verify the legitimacy of this call, we can provide information about where to find the Microsoft privacy statement and whom to contact (https://aka.ms/privacy)."

Please make sure that during the initial call you follow the communication guidance listed above.

If you are making a transactional call, the initial contact and messaging with the customer must focus on the main purpose of the call, which is the transactional trigger. For example, the agent should say something like: ***"I'm calling to talk to you about xx product which is coming to its end of service."*** From there, if the customer wants to talk about a different topic, the conversation can move in that direction. At the very end of the transactional purpose of the call, you may ask the customer if they are interested in another topic, but you must accept if the customer declines. **You need to follow the Privacy/CELA Transactional messaging framework.**

If you are making a promotional call, you may only contact individuals who are an existing OK to contact "OKC" for promotional tele in MSX.

Microsoft Handling of Customer Personal Data: Microsoft employees/vendors should only be able to access customer personal data if based on explicit customer action (e.g, if the vendor is delivering an assessment and the customer is provisioning MS access to their environment via a data collection tool, or the customer providing the information to MS outside of a tool).

- In the case of an assessment, a data collection tool cannot provision Microsoft access to the customer's assessment data by default.
- If taking screenshots during a customer meeting, ask explicit customer permission before doing so. If included in a customer report, anonymize the personal data.

- If the customer provides MS employee/vendor access to personal data, delete any reports/screenshots containing personal data from all MS locations at the end of the customer engagement (not to exceed 30 days).