

Communication Compliance

Overview: [Communication Compliance](#) is part of the insider risk solution in Microsoft 365 that helps minimize communication risks by helping you detect, capture, and act on inappropriate messages in your organization. Pre-defined and custom policies allow you to scan internal and external communications for policy matches so they can be examined by designated reviewers. Reviewers can investigate scanned email, Microsoft Teams, Yammer, or third-party communications in your organization and take appropriate actions to make sure they're compliant with your organization's regulatory compliance and code of conduct standards.

This lab is designed to provide an introductory environment for Communication Compliance. As this isn't a production environment it's sometimes difficult to trigger enough information, therefore in production/live tenant you might only want to see a subset of triggered information and not all of it.

This guide will help you navigate the steps needed to walk through a basic Communication Compliance policy.

Labs steps

Communication Compliance



What is it	Where is it and what to do
<p>Detecting compliance risks in digital communications is critical to mitigating conduct, reputational, and financial risks. Many organizations require a solution that meets both business controls and regulatory compliance requirements, while also providing employees with technology that enables them to do their best work.</p> <p>Communication Compliance helps organizations minimize communication risks, such as sharing of adult imagery or threatening language by helping you detect, capture, and act on inappropriate messages in your organization. Pre-defined and custom policies allow you to scan internal and external communications for policy matches so they can be examined by designated reviewers. Reviewers can investigate scanned email, Microsoft Teams, Yammer, or third-party communications in your organization and take appropriate actions to make sure they're compliant with your organization's regulatory compliance and code of</p>	<p>No click steps.</p>




What is it	Where is it and what to do
<p>conduct standards. And to enable organizations to protect end-user privacy, strong safeguards and controls are built into the solution by default, such as pseudonymization, role-based access control, admin opt-in of users, and audit logs.</p> <p>In this lab, we will see how Communication Compliance can help, foster a healthy and inclusive work environment while mitigating communication risks.</p>	

What is it	Where is it and what to do
<p>Like Insider Risk Management, Communication Compliance has pre-configured templates to help you get started quickly and easily. Templates allow you to apply machine learning to intelligently detect communications that violate an organization's policies.</p> <p>Policy templates are pre-defined policy settings that you can use to quickly create policies to address common compliance scenarios. The templates you can choose from include:</p> <ul style="list-style-type: none"> • Inappropriate text or images – such as offensive language, and anti-harassment detects communication containing information identified by trainable classifiers, including harassment, profanity, threats, and adult, racy, or gory images • Sensitive information – detects both standard and custom sensitive information types and patterns • Regulatory compliance – detects communication containing information related to financial regulatory compliance • Conflict of interest - detects communications between groups and users to help avoid conflicts of interest <p>Let's look more closely at the template for offensive language. This template uses an abusive language machine learning model to automatically detect</p>	<p>Navigate to https://compliance.microsoft.com/ logged in as the administrator of your given lab tenant.</p> <p>Login with the credentials you have been provided for your lab tenant</p> <ol style="list-style-type: none"> 1. In the left navigation pane of the Microsoft 365 compliance center, click Show all..., then click Communication Compliance. 2. Click Create policy, hover over each of the templates as you speak. <ul style="list-style-type: none"> • Detect inappropriate text • Detect inappropriate images • Monitor for sensitive info • Monitor for regulatory compliance • Monitor for conflict of interest

What is it	Where is it and what to do
<p>content that may be considered threatening or harassing and is pre-configured to detect a threat, harassment, profanity, and other content classifiers to help reduce false positives in scanned messages.</p> <p>Here you can see a wizard pops up to initiate the policy creation process. You may notice that some of the settings are already populated which saves you time. To get started, all we need to do is change or keep the given policy name. Let's keep it as for now.</p> <p>Next, you will indicate which users or groups you want to supervise, for example, <i>All Users</i>.</p> <p>Then, select the users who will be reviewers. In this case, let's add two reviews.</p> <p>Notice that all the other settings have been filled in for us, including Communication locations, trainable classifiers, conditions, and percentage to review.</p> <p>But if I needed to adjust this policy, I can click <i>Customize Policy</i>.</p> <p>Let's do that so you can see how to add machine learning classifiers to detect additional content.</p> <p>Let's keep the name as is, same with the supervised users and reviewers, and we'll continue to detect violations across all communication locations. While we will look at data connectors later in this lab, once they are configured you can also add connectors to other 3rd party communication channels so your compliance policies will also detect violations in those channels.</p> <p>On the <i>Choose conditions and review percentage</i> page, click <i>Add</i> and click on <i>Trainable Classifiers</i>... ... and then select <i>Source code</i> and click <i>Add</i>.</p> <p>In addition to customizing the policy so it will detect sharing of source code, let's also look at the conditions we can add to the policy to help us refine the communications we are scanning. In the Add condition list, you can see there are a variety of conditions you can add to include or exclude different types of communications to minimize inaccurate alerts. For instance, you can exclude emails that include newsletters by adding a Message</p>	<ol style="list-style-type: none"> 3. Click Detect inappropriate text. 4. Under Users or groups to supervise, select All users. 5. Under Reviewers, enter and select Johanna Lorenz and Megan Bowen. 6. Hover over Communication to monitor (i) icon. 7. Click Customize policy. 8. Click Next until you reach Choose conditions and review percentage page, click Add located at the bottom of the Trainable classifiers list, and select Trainable classifiers. 9. On the Trainable classifiers flyout page, select Profanity, then click Add. 10. Click on Add condition to display the list of additional conditions that are available. 11. Click on Message contains none of these words and type newsletter in the text box. 12. Check the box in front of Extract printed or handwritten text from images for evaluation. 13. Click Next. 14. Click Cancel. (Note: Do not click Create policy since there was already one created with the same name.)

What is it	Where is it and what to do
<p>containing none of these words conditions and adding the word newsletter. You could also exclude communication-based on labels that have been applied.</p> <p>Let's also check the box to enable Optical character recognition so our policy can detect policy violations in extracted printed or handwritten text from images.</p> <p>Last you can set the percentage of communication you want to review. We use 100% for demonstration purposes, but in a company, you can set each policy to different percentages to manage the number of alerts that are generated from your communication compliance policies.</p> <p>From here, click <i>Next</i> and review the settings, then click <i>Create policy</i>. Because there has already been an Offensive Language policy created, I am going to cancel this wizard, and let's go review the existing policy.</p> <p>Now, let's assume we are the Investigator remediating policy violations. Let's click into the Sensitive Info policy that has already been created for you.</p> <p>This view here shows the age of pending items, users with the most policy matches, and associated alerts. Because we are logged in as a user with the investigator role, we can see users' names and email addresses. If we were logged in with the analyst role, user-identifying information would be pseudonymized to protect end-user privacy. In most organizations, Analysts will first review and triage pseudonymized communications before assigning or escalating to an Investigator to review and take action.</p> <p>By clicking into <i>Pending</i>, I can see the policy matches across communication platforms including Exchange, Teams, and Yammer.</p> <p>You can establish very detailed policies that detect specific things like violations that occur in a different language or scan images with OCR to look for embedded violations.</p>	<p>15. On the Communication Compliance home page, under Policies, click the Sensitive Info policy that has previously been created for you.</p> <p>16. Click the Pending tab.</p>

What is it	Where is it and what to do
<p>This view here shows a list of messages that have been flagged. Along with identifying who was involved, you can also tell from the message type if the communication happened in Exchange, Teams, or Yammer.</p> <p>This provides context as to whether this is a policy violation. Messages that are exact matches for the terms of a policy or a near duplicate will also be flagged. It is important to note, that offensive messages in other languages, as well as images of offensive text, can be flagged as a policy violation.</p> <p>It's possible to also remove messages from Teams chats and channels so that recipients won't be upset or offended. Communication Compliance solution is best with Microsoft Teams because it can simplify the adoption, management, and cost. It leverages native Teams, shared and private channels and reviews communication in the context of the conversations. Remediation options that include removing the offensive message are a key advantage of the Communication Compliance solution.</p> <p>Let's go ahead and remove the message from their Teams chat so that they don't have to continue to see things like threats and offensive language or remove the sensitive info from the chat. If we wanted to take further steps to remediate this issue, we could notify the user directly, or escalate the issue to their manager.</p> <p>In some cases, a message may be flagged that does not necessarily violate a corporate policy. In Communication Compliance, we could report false positives that the built-in classifiers detect, effectively helping to improve the detection algorithm over time, making the model more accurate, and reducing false positives.</p>	<ol style="list-style-type: none"> 17. Click on one of the items with the Teams icon  (a preview of the message will appear on the right). 18. Click on one of the messages located in Teams 19. Click Conversation 20. Hover over the messages highlighted in red 21. Click the X in the upper right corner 22. Select one of the messages, click the Remove icon  in the menu above the alert list, then click Remove messages. 23. On the Pending alert page, select a Message

What is it	Where is it and what to do
<p>We could also automate workflows which gives us the ability to tailor the process to automate what to do when I catch employees that are violating my business processes.</p> <p>For example, we could create a new flow by notifying a manager through this template. This becomes especially relevant with remote work because HR managers are no longer in the same office as employees and need to be the first ones to handle out-of-line behavior remotely. Through Power Automate, we can use this pre-built automation to notify the HR manager of a violation. This feature helps save time during the review and remediation process.</p> <p>Another action you can take is to notify the user to say, "Hey, this is not acceptable," especially if it's a first-time offender.</p> <p>You can pre-configure your templates. As you see here, a template for regulatory violations has been created for you. But this can also be used to send notifications about Code of Conduct violations.</p> <p>A blind carbon copy that person's manager and use a pre-canned customizable template that can inform the employee that their message violated the organizational policies.</p> <p>Another remediation action we can take is to escalate this to another person in our review team. Perhaps this is a repeat offender, and it's not your responsibility to decide what to do next. We could escalate this to another person on my team. In this case, I'm going to click on Escalate, and the list of users that I can escalate to pops up.</p>	<p>24. Click the Automate icon  in the menu above the alert list or in the buttons below the preview pane. (If this is the first time opening the Automate menu, you will need to click Get Started)</p> <p>25. Click Cancel to close</p> <p>26. Click the Notify Manager tile to review the different steps of the flow.</p> <p>27. Click Continue</p> <p>28. Scroll down to show the complete Flow</p> <p>29. Click Cancel.</p> <p>30. Click on the Use a notice template to send an email to the sender of the specified messages. Icon: </p> <p>Note: Notice you can send a templated email to the user, without knowing the identity of the individual.</p> <p>31. Click Cancel.</p> <p>32. Click on the Escalate for investigation button. Icon: </p> <p>33. Type the name of the investigation "Case 143: Sensitive data compliance"</p> <p>34. In the note field copy and paste or type "Repeat offender, please handle."</p> <p>35. Click Cancel. (Note: Do not click Create case since there was already one created with the same name.)</p>

What is it	Where is it and what to do
<p>After triaging and remediating alerts, you can also review the reports to gain additional insight into the users and policy matches that are flagged by Communication Compliance. If we click on the Reports tab, we can review different reporting that is automatically created including Recent policy matches, resolved items or escalations by policy, and rankings on the policies and users with the most matches. There are also detailed reports available to allow you to view things like policy settings and summaries by user, location, and sensitive information type.</p>	<p>36. Click Communication compliance in the left navigation pane of the</p> <p>37. Click the Reports tab</p> <p>Scroll Down to Users with most policy matches</p>

Conclusion

What is it	Where is it and what to do
<p>Whether you are looking to assess and remediate harassing and threatening employees or are only looking to help prevent sensitive financial information from falling into the wrong hands; Communication Compliance helps bring these types of scenarios into a new level of visibility. We were able to see the different forms of communication that matched our Communication Compliance policies, it's possible to quickly respond, and, in this case, we could also see regulatory non-compliant activities and alert the employee's manager right away. This automated and proactive approach has helped our organization stop and quickly respond to insider risk activities.</p>	<p>No click steps.</p>