**Section 1: Contribute to Recommending Risk Management Strategies**

**Scenario Details:** The Chief Information Security Officer (CISO) has called a meeting to discuss the bank's cyber security risks. During the meeting, the following risks are identified:

1. **Stolen or Compromised Credentials:** Phishing and Password Spray attacks targeting bank employees have led to several incidents of unauthorised access to sensitive systems and data.
2. **Identity Governance:** The bank uses temporary contractors for certain projects. There has been an issue with contractor accounts still being active after the contract has ended.

Your task is to contribute to recommending risk management strategies for these identified risks. You will need to:

**Task 1:**

After consulting with key stakeholders, provide a summary of each risk. Include what risks were identified in the meeting with the CISO and why the risks should be addressed.

**Summary of Identified Risks:**

1. **Stolen or Compromised Credentials:**
   * **Description:** Phishing and Password Spray attacks targeting bank employees have resulted in unauthorized access to sensitive systems and data.
   * **Significance:** These attacks pose a significant threat to the security of SouthernBank's systems and data. Compromised credentials can lead to unauthorized access to sensitive financial information, potentially resulting in financial loss, reputational damage, and regulatory penalties.
   * **Impact:** If attackers gain access to employee credentials, they could potentially conduct fraudulent transactions, steal customer data, or disrupt banking services, causing financial harm to the institution and its customers.
   * **Importance of Addressing:** It is crucial to address this risk promptly to prevent further unauthorized access and mitigate the potential consequences of compromised credentials. Proactive measures are necessary to strengthen employee awareness of phishing threats and enhance password security to prevent password spray attacks.
2. **Identity Governance:**
   * **Description:** The bank employs temporary contractors for specific projects, and there have been instances where contractor accounts remain active after the contract has ended.
   * **Significance:** This issue poses a risk to the bank's identity governance and access management practices. Active contractor accounts beyond the contract duration can lead to unauthorized access to systems and data, increasing the risk of insider threats or external breaches.
   * **Impact:** Inactive contractor accounts present opportunities for unauthorized individuals to exploit access privileges, potentially leading to data breaches, financial fraud, or regulatory non-compliance. Failure to manage contractor access effectively could undermine the bank's overall security posture and erode customer trust.
   * **Importance of Addressing:** Addressing this risk is essential to maintain robust identity governance and ensure that access privileges are granted and revoked in a timely manner. Implementing proper procedures for managing contractor accounts, such as regular review and revocation of access upon contract termination, is critical to mitigating the risk of unauthorized access and maintaining compliance with regulatory requirements.

**Task 2:**

Research and review critical cyber risk management strategies appropriate for addressing stolen credentials and identity governance. Provide at least two possible risk management strategies.

Ref: [Security, Compliance, and Identity Fundamentals - Part 3](https://www.acitconnect.edu.au/course/view.php?id=224#coursecontentcollapse3)Ref: Password spray attacks.pdf

**Risk Management Strategies for Addressing Stolen Credentials:**

1. **Employee Training and Awareness:**
   * **Description:** Implementing comprehensive training programs to educate employees about the risks of phishing attacks and the importance of safeguarding credentials.
   * **Benefits:** Increased employee awareness can help identify and report phishing attempts, reducing the likelihood of successful attacks. Educating employees on password best practices, such as using strong, unique passwords and enabling multi-factor authentication (MFA), can enhance password security and mitigate the risk of password spray attacks.
   * **Implementation:** Conduct regular security awareness training sessions for all employees, focusing on recognizing phishing emails, avoiding suspicious links or attachments, and practicing good password hygiene. Provide clear guidelines on creating strong passwords and encourage the use of MFA wherever possible.
2. **Advanced Authentication Mechanisms:**
   * **Description:** Deploying advanced authentication solutions, such as biometric authentication or adaptive authentication, to enhance credential security.
   * **Benefits:** Advanced authentication mechanisms provide an additional layer of security beyond traditional username and password combinations, making it harder for attackers to compromise credentials. Biometric authentication methods, such as fingerprint or facial recognition, offer stronger authentication factors that are difficult to replicate or steal.
   * **Implementation:** Integrate biometric authentication options into the bank's systems and applications, allowing employees and customers to authenticate using fingerprint scanners or facial recognition technology. Implement adaptive authentication solutions that dynamically adjust authentication requirements based on risk factors such as user behavior, location, and device, providing stronger protection against unauthorized access.

**Risk Management Strategies for Addressing Identity Governance:**

1. **Automated Account Lifecycle Management:**
   * **Description:** Implementing automated processes for managing user accounts throughout their lifecycle, including provisioning, de-provisioning, and access reviews.
   * **Benefits:** Automated identity lifecycle management ensures that user accounts are created, modified, and deactivated in a timely manner, reducing the risk of inactive or orphaned accounts. Automated access reviews help identify and revoke unnecessary access privileges, minimizing the risk of unauthorized access and insider threats.
   * **Implementation:** Deploy identity governance solutions that automate account provisioning and de-provisioning processes based on predefined rules and workflows. Implement periodic access reviews to validate user access rights and identify any discrepancies or anomalies. Integrate identity governance solutions with existing identity and access management (IAM) systems to streamline account management processes and enforce consistent access controls.
2. **Role-Based Access Control (RBAC):**
   * **Description:** Implementing RBAC policies to manage user access based on job roles and responsibilities, ensuring that users have access only to the resources and data necessary for their job functions.
   * **Benefits:** RBAC reduces the risk of overprivileged access by assigning permissions based on predefined roles, minimizing the likelihood of unauthorized access or data breaches. By enforcing least privilege principles, RBAC helps prevent the proliferation of excessive access rights and reduces the attack surface.
   * **Implementation:** Define role-based access policies that align with the bank's organizational structure and job roles. Assign users to appropriate roles based on their job functions and responsibilities, ensuring that access permissions are tailored to their specific needs. Regularly review and update RBAC policies to reflect changes in organizational roles or access requirements, maintaining effective access controls and reducing the risk of unauthorized access.

**Task 3:**

Prepare a presentation outlining the options for risk management strategies for each risk, which you will present to the CISO and other relevant stakeholders. Using the template, (SouthernBank Risk Management Presentation.pptx) create a power point presentation with slides that include:

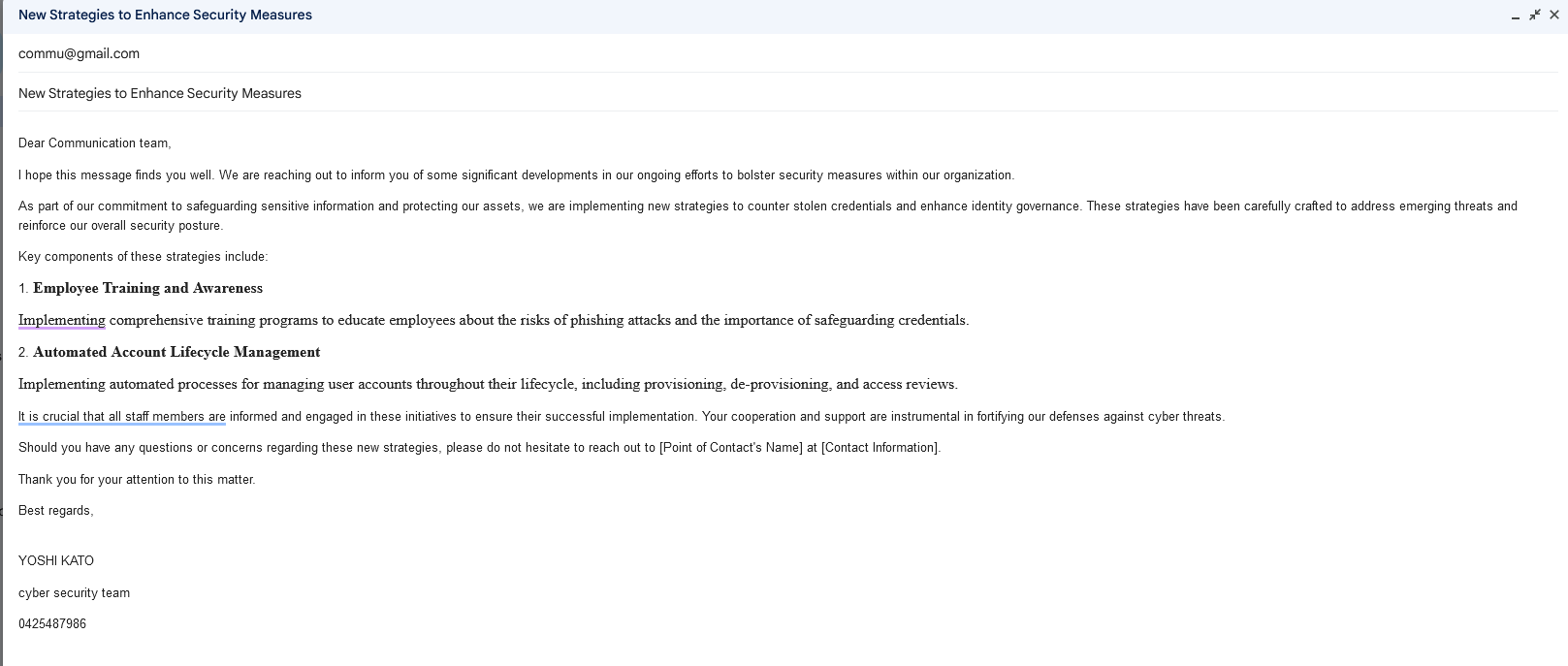
* + - summary of identified risks
    - risk response
    - recommended risk management solution(s) for each risk
    - next steps

**Section 2: Support Implementation of Approved Risk Management Strategies**

**Scenario Details:** The CISO has approved the risk management strategies for stolen credentials and identity governance. Your responsibilities include:

**Task 4:**

Collaborate with the communication team to ensure relevant staff are informed about the new strategies to counter stolen credentials and improve identity governance. Provide the communication team with a draft email to inform the stakeholders what strategies will be implemented.



**Task 5:**

The IT Team needs to monitor cyber security risks based on the implemented strategies. Refer to Assessment 1, Part 3 “**Monitor and manage security posture with Identity Secure Score”** and provide an executive summary that describes how this tool can support managing identity security posture.

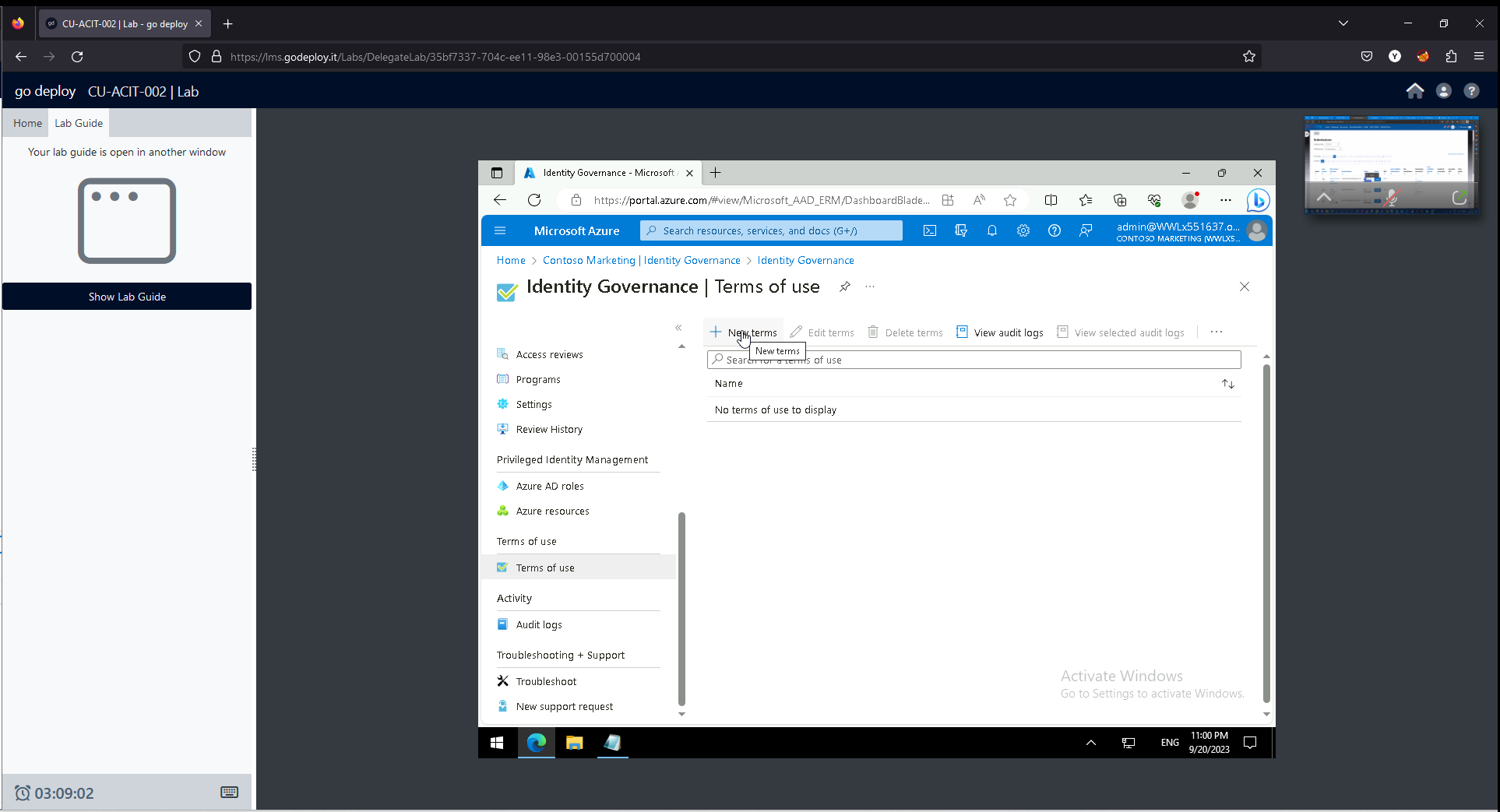
Identity Secure Score helps organizations monitor and manage their security posture by providing insights into the security health of their identity infrastructure.

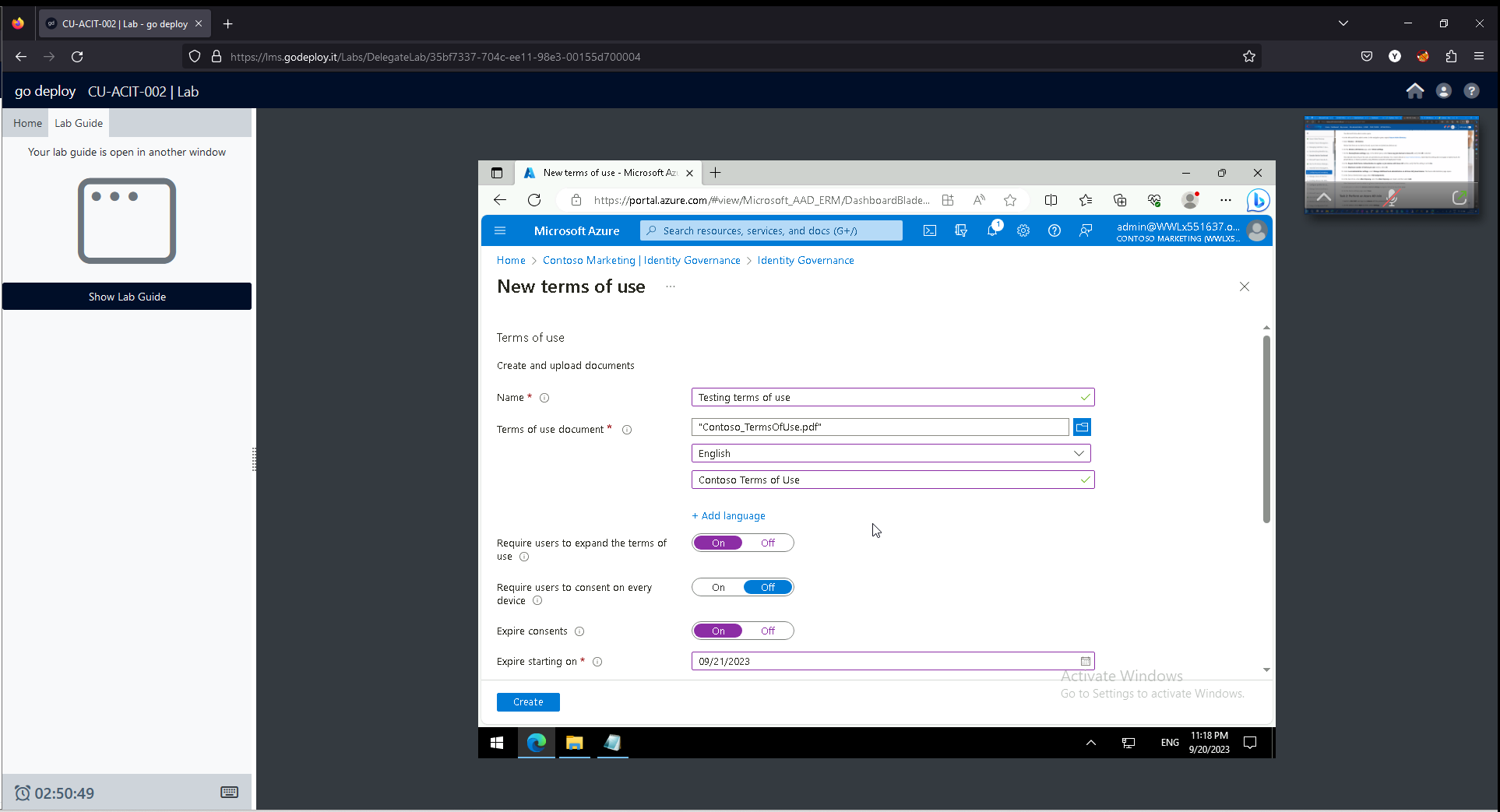
Here's how it works:

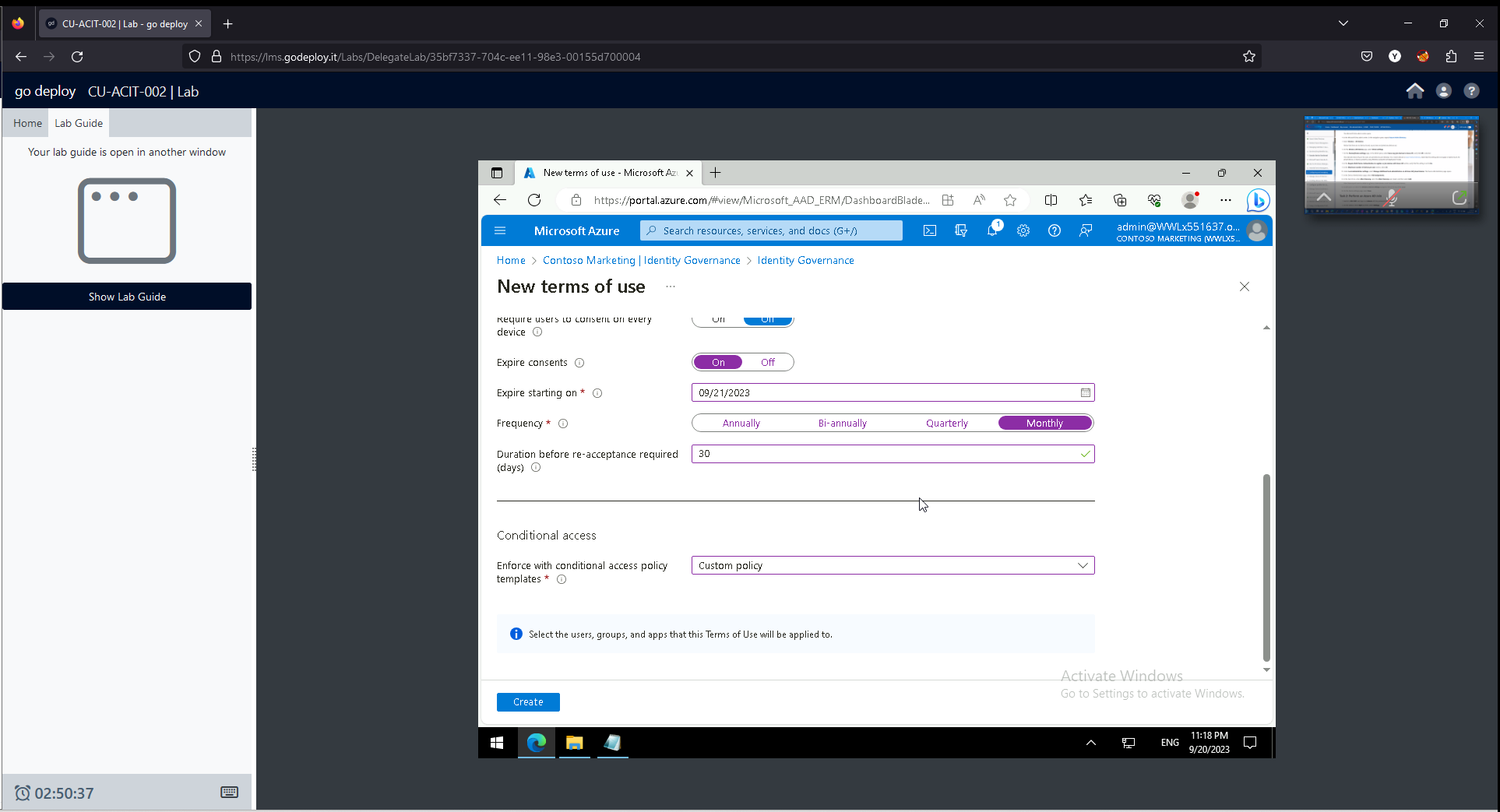
1. **Data Collection**: Identity Secure Score continuously collects data from various sources within Azure AD, such as user activities, sign-in attempts, security configurations, and more.
2. **Risk Assessment**: It then analyzes this data to assess the security risks associated with identity management. This assessment includes factors like weak passwords, suspicious sign-in activities, lack of multi-factor authentication (MFA), outdated software, and other vulnerabilities.
3. **Score Calculation**: Based on the analysis, Identity Secure Score assigns a numerical score to the organization's identity security posture. This score reflects how well the organization is implementing security best practices and mitigating identity-related risks.
4. **Recommendations**: Identity Secure Score provides actionable recommendations to improve the security posture. These recommendations are tailored to the organization's specific environment and may include enabling MFA, enforcing stronger password policies, reviewing and revoking unnecessary permissions, implementing conditional access policies, and more.
5. **Tracking Progress**: Organizations can track their progress over time by monitoring changes in their Identity Secure Score. As they implement the recommended security measures, their score should improve, indicating a stronger security posture.
6. **Prioritization**: Identity Secure Score helps organizations prioritize their security efforts by highlighting the most critical areas that need attention. It categorizes recommendations based on their impact on security and provides guidance on which actions to take first.
7. **Integration**: Identity Secure Score is integrated into the Azure portal and can also be accessed through Microsoft Graph API. This integration allows organizations to view their score alongside other security metrics and manage their identity security posture within the same interface they use for other Azure services.

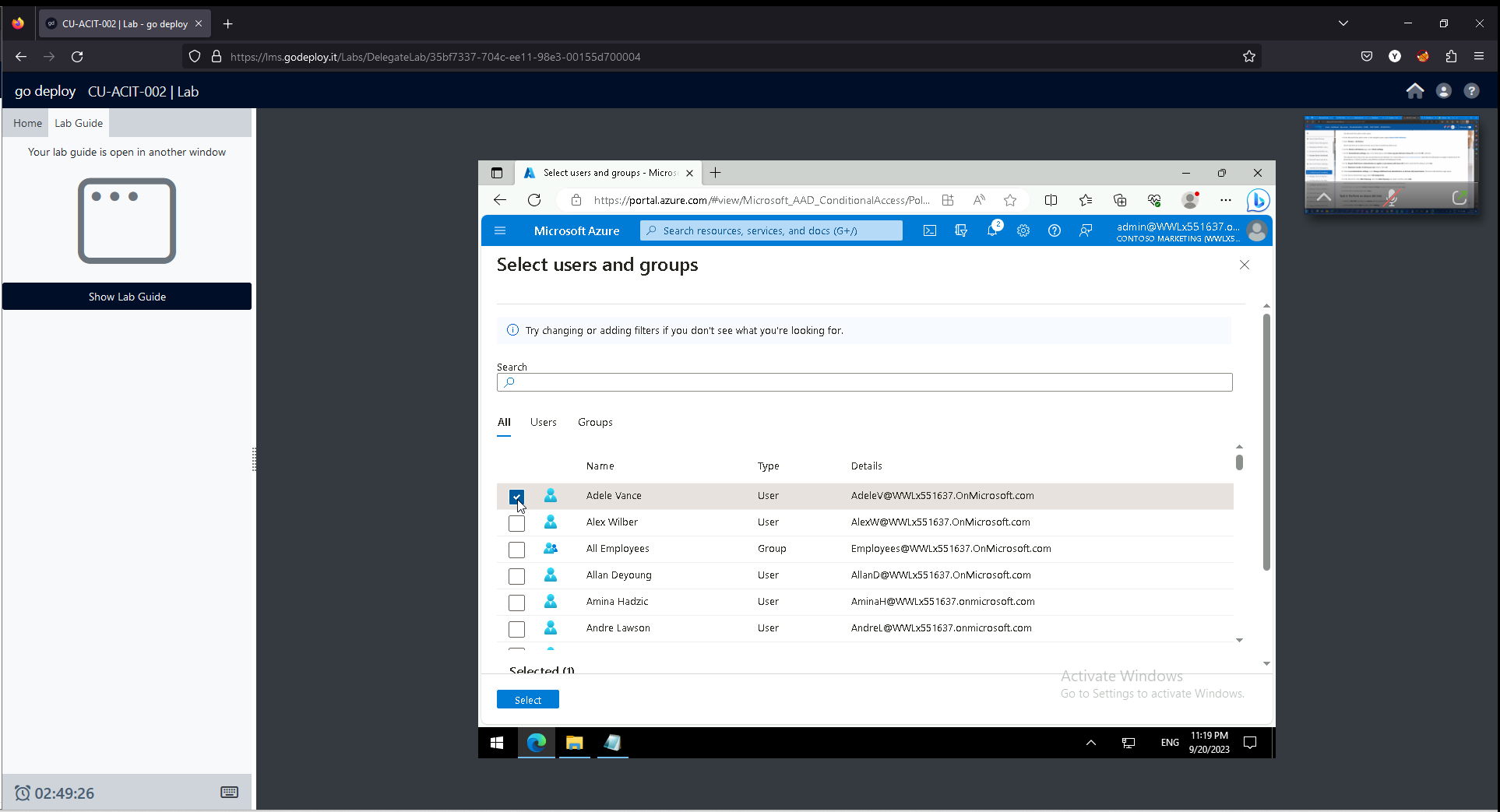
**Task 6:**

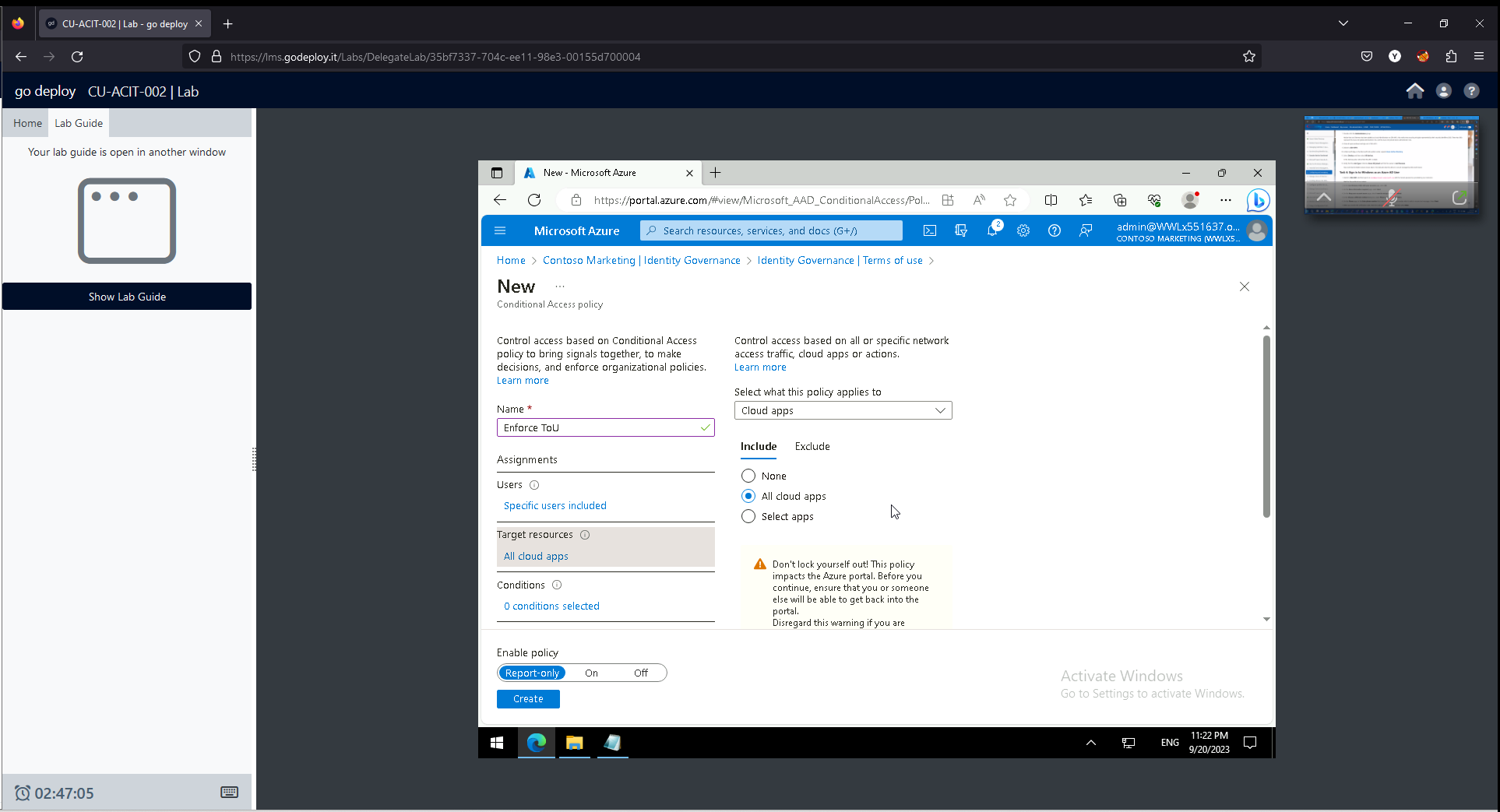
Assist in evaluating compliance with the new strategies, such as ensuring employees follow secure authentication practices. Provide screenshots of the lab “**Add terms of use and acceptance reporting**” and provide an executive summary that describes how this feature can support compliance with the security strategy.

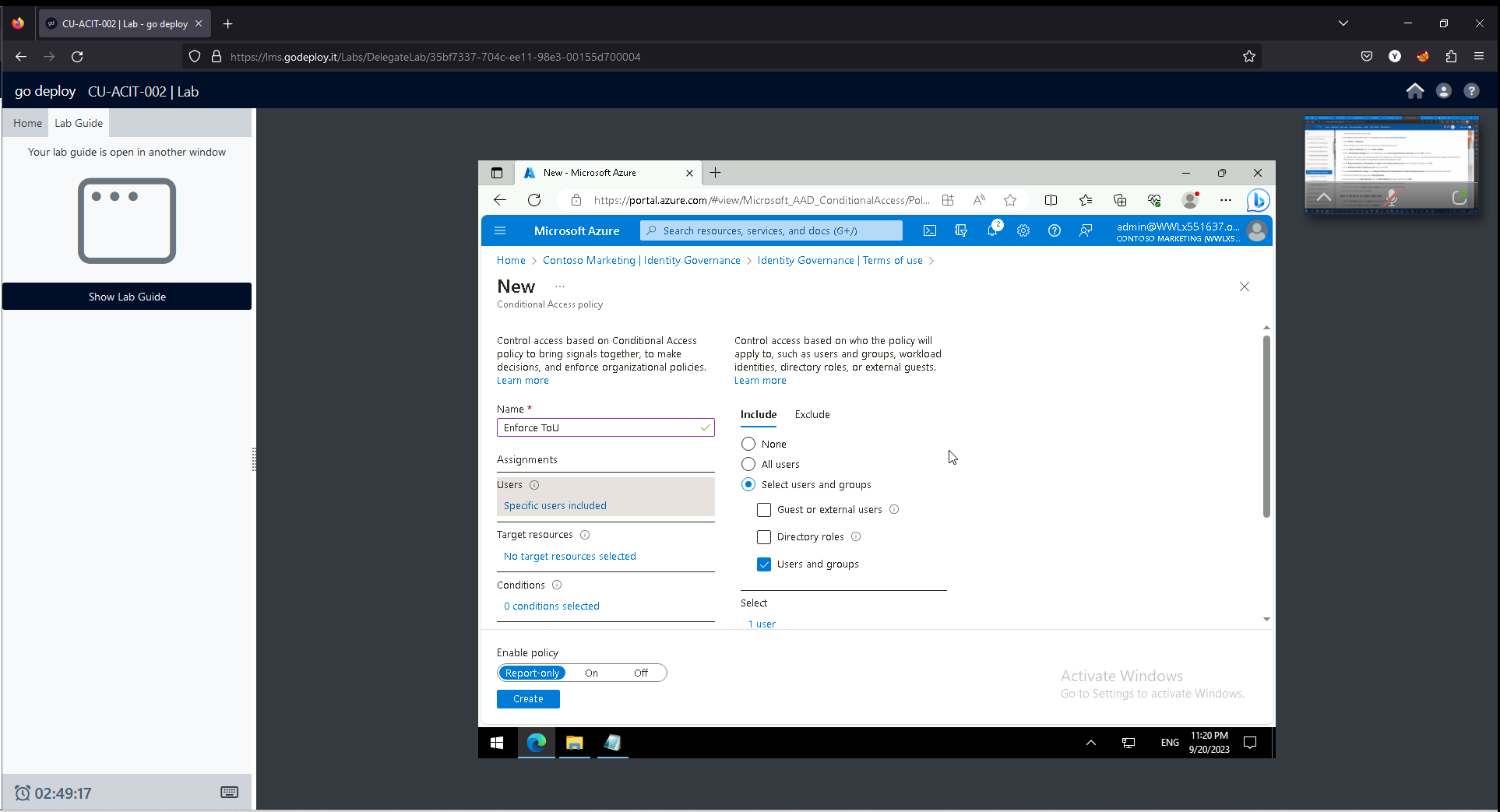


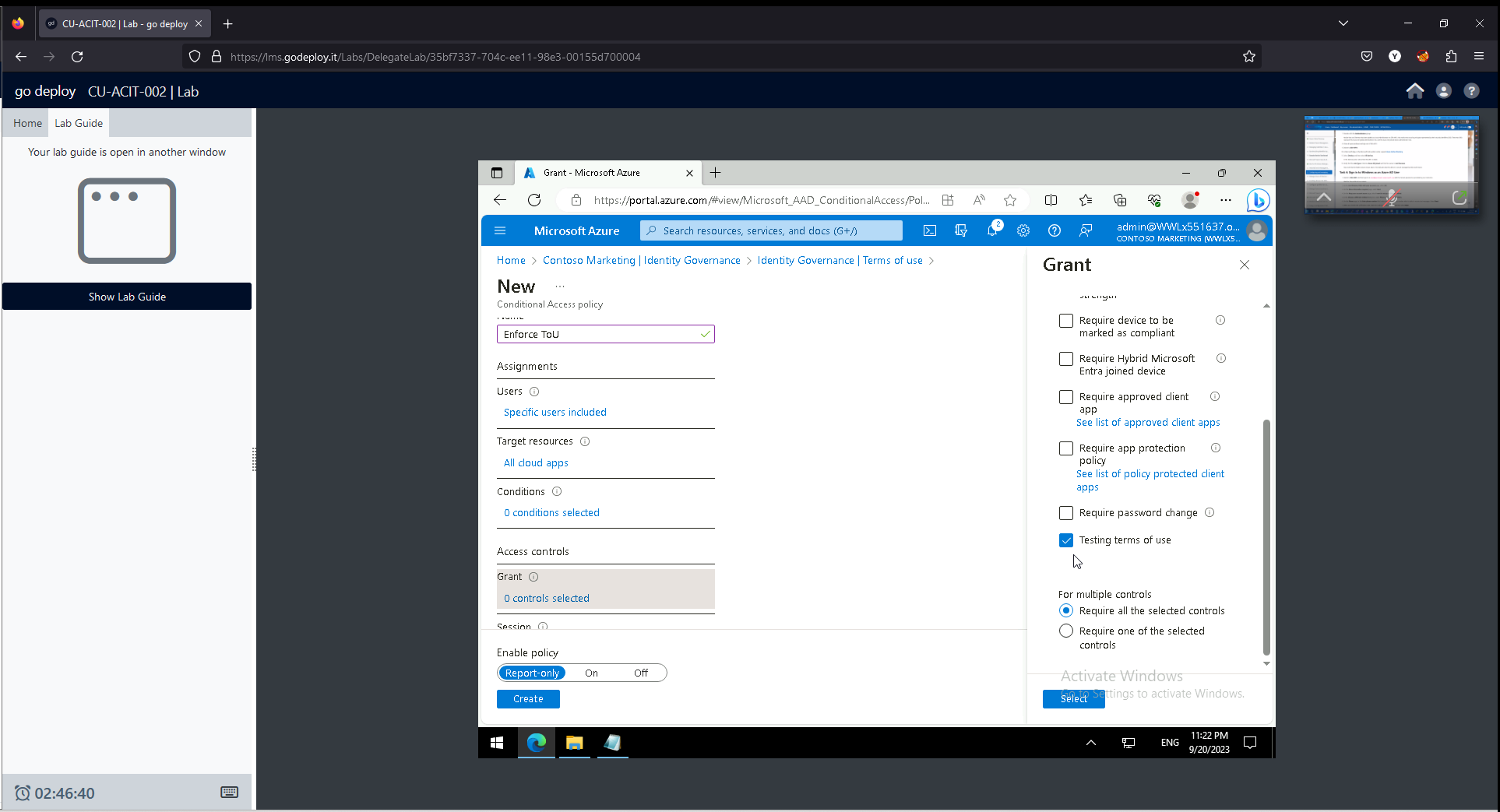


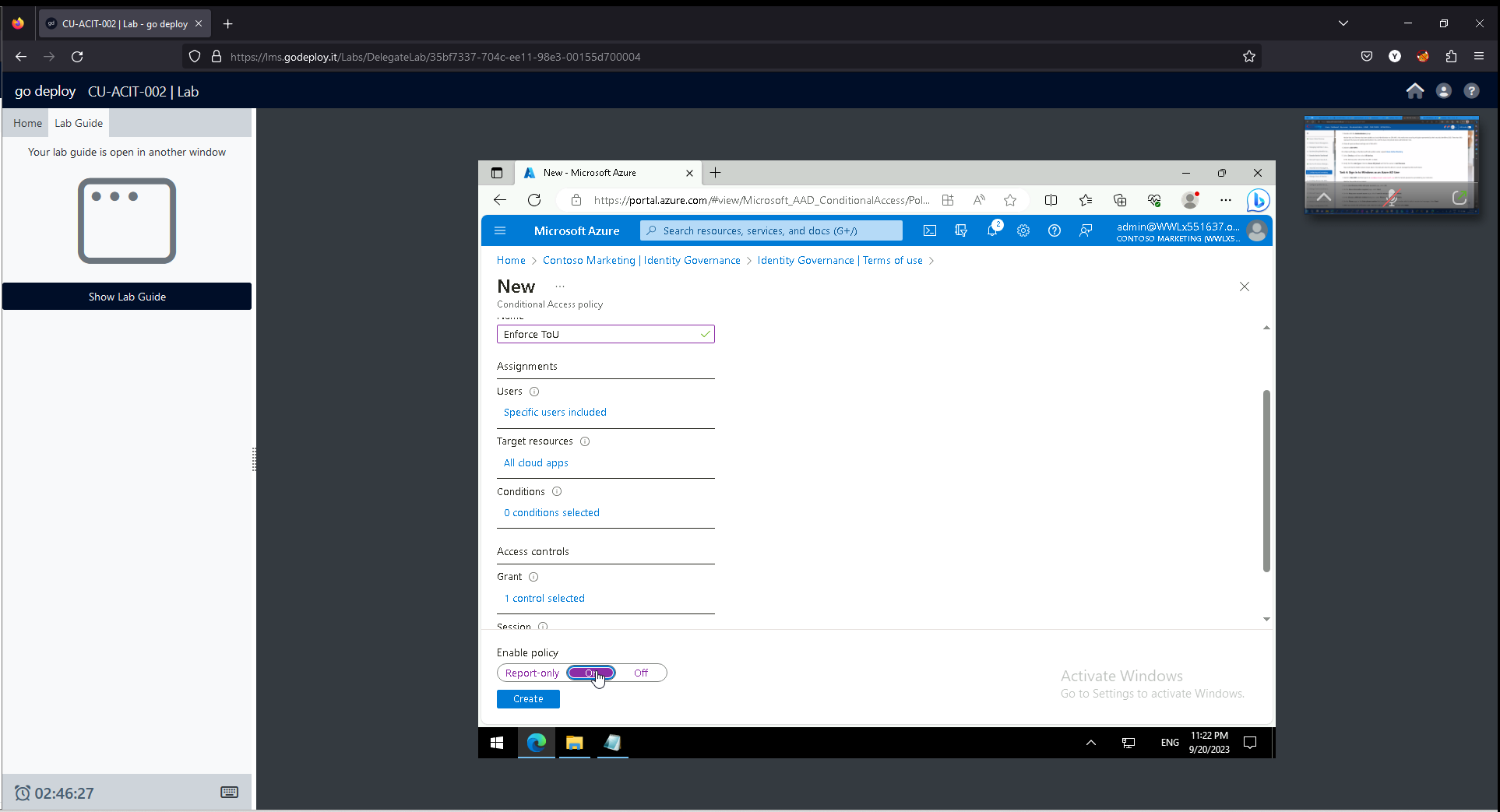


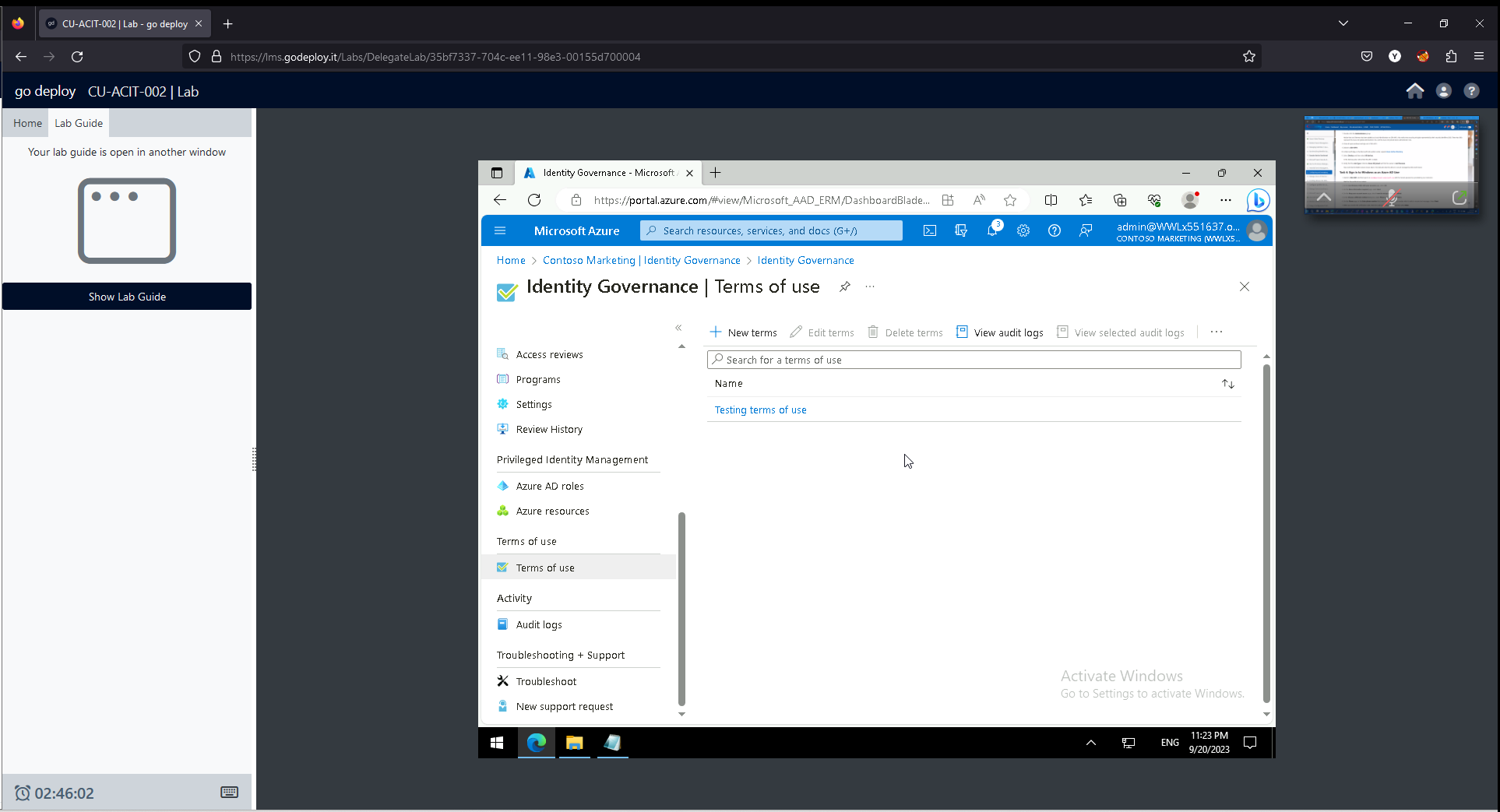


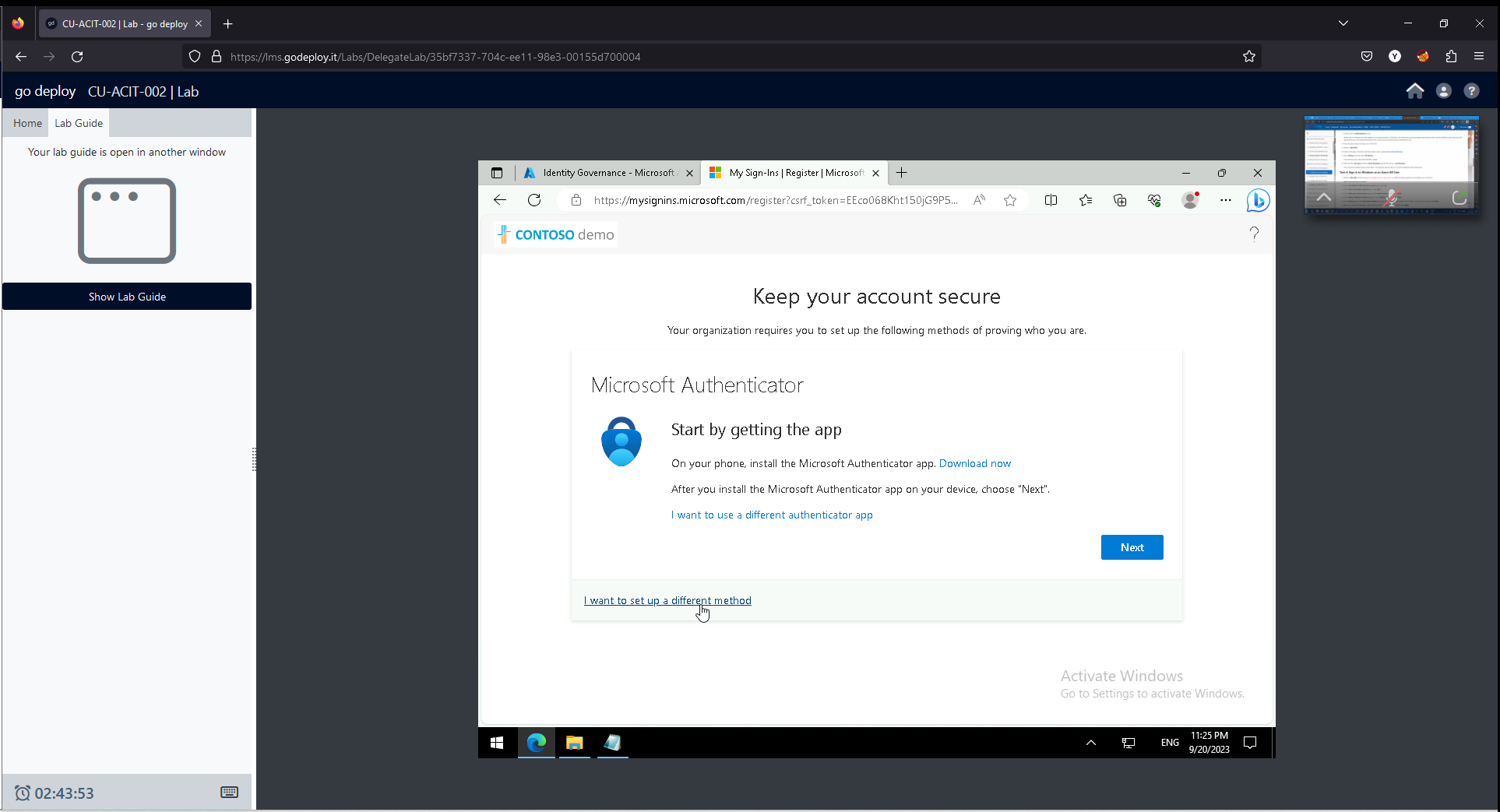


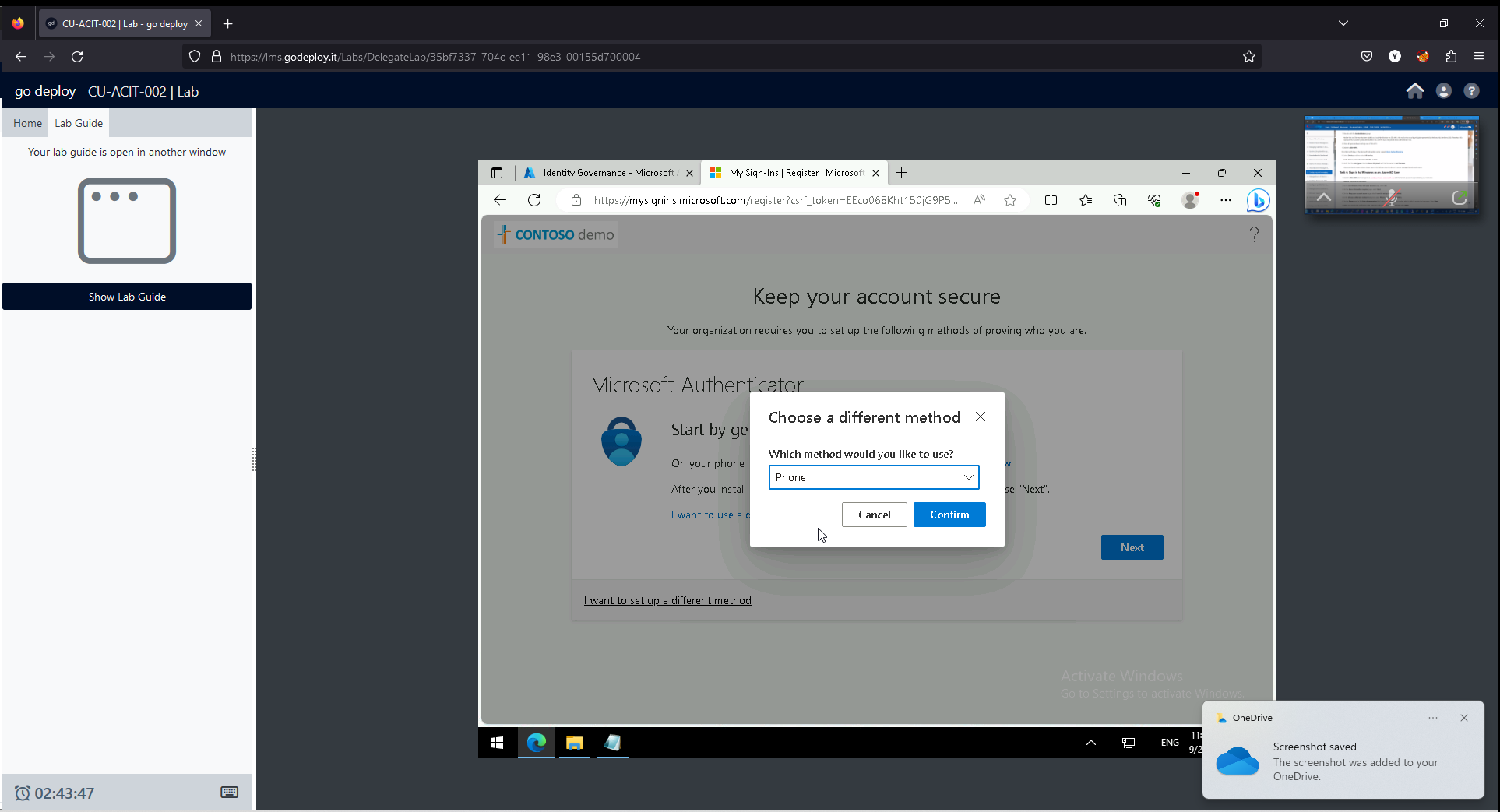


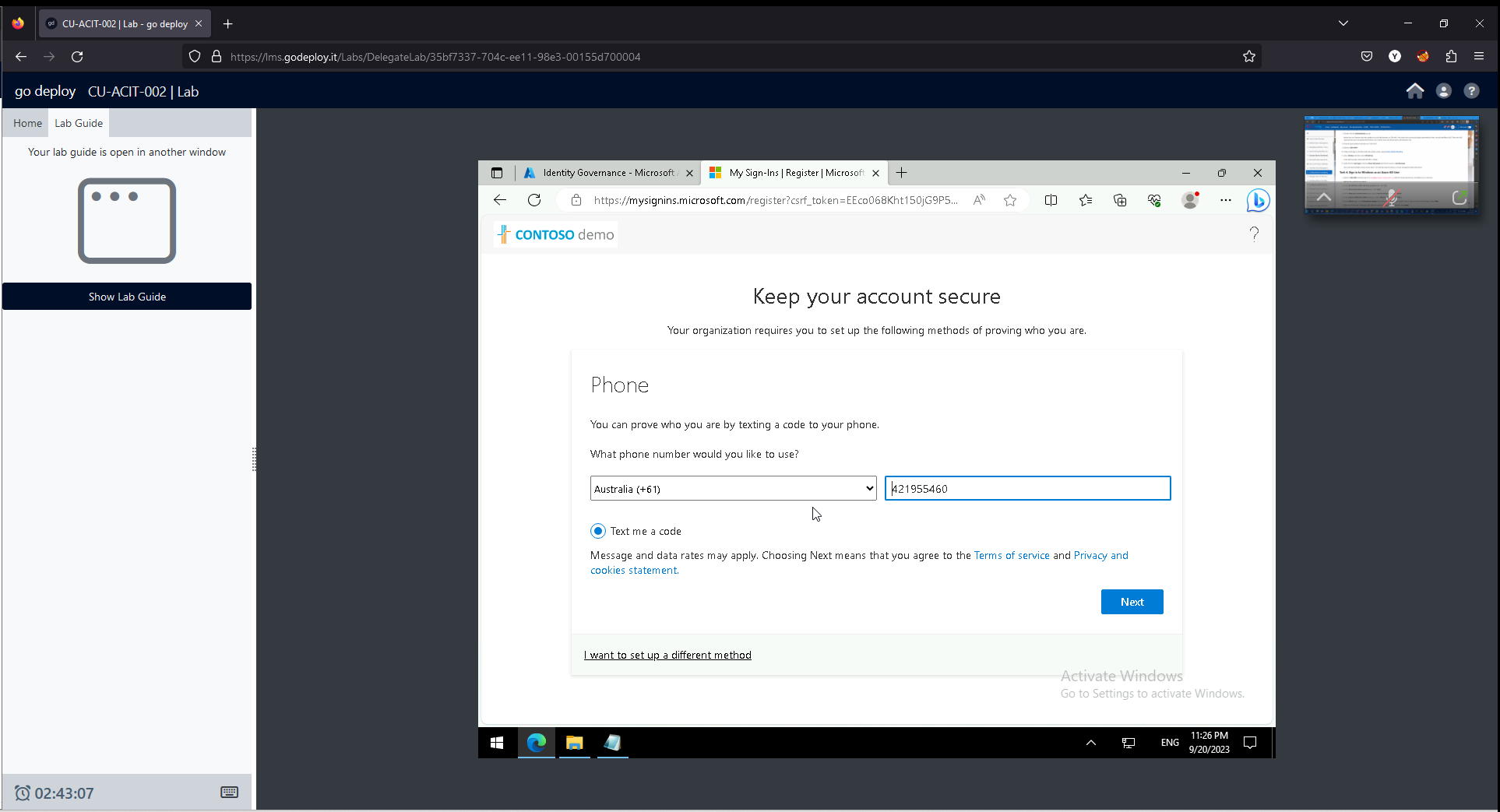


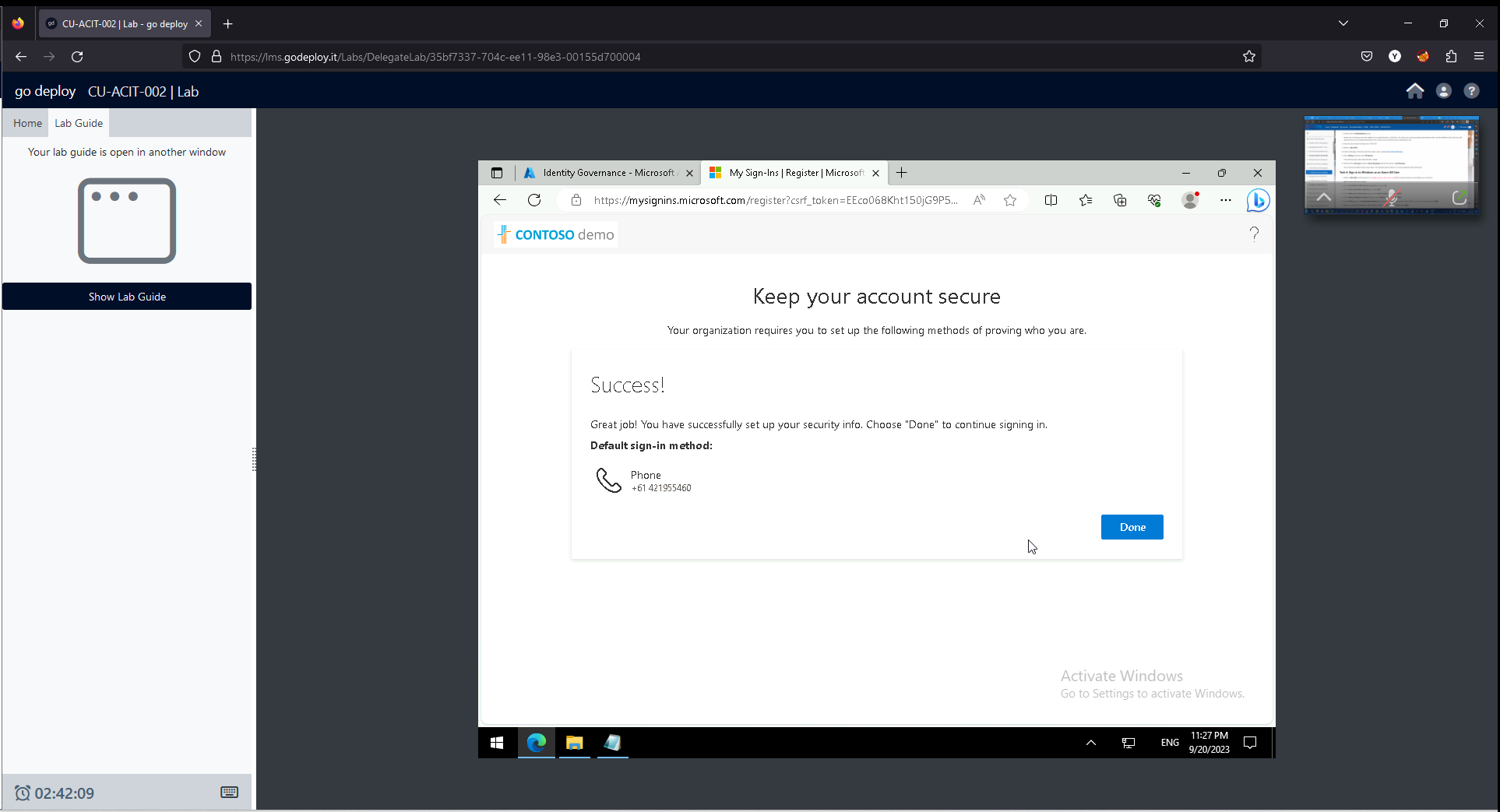


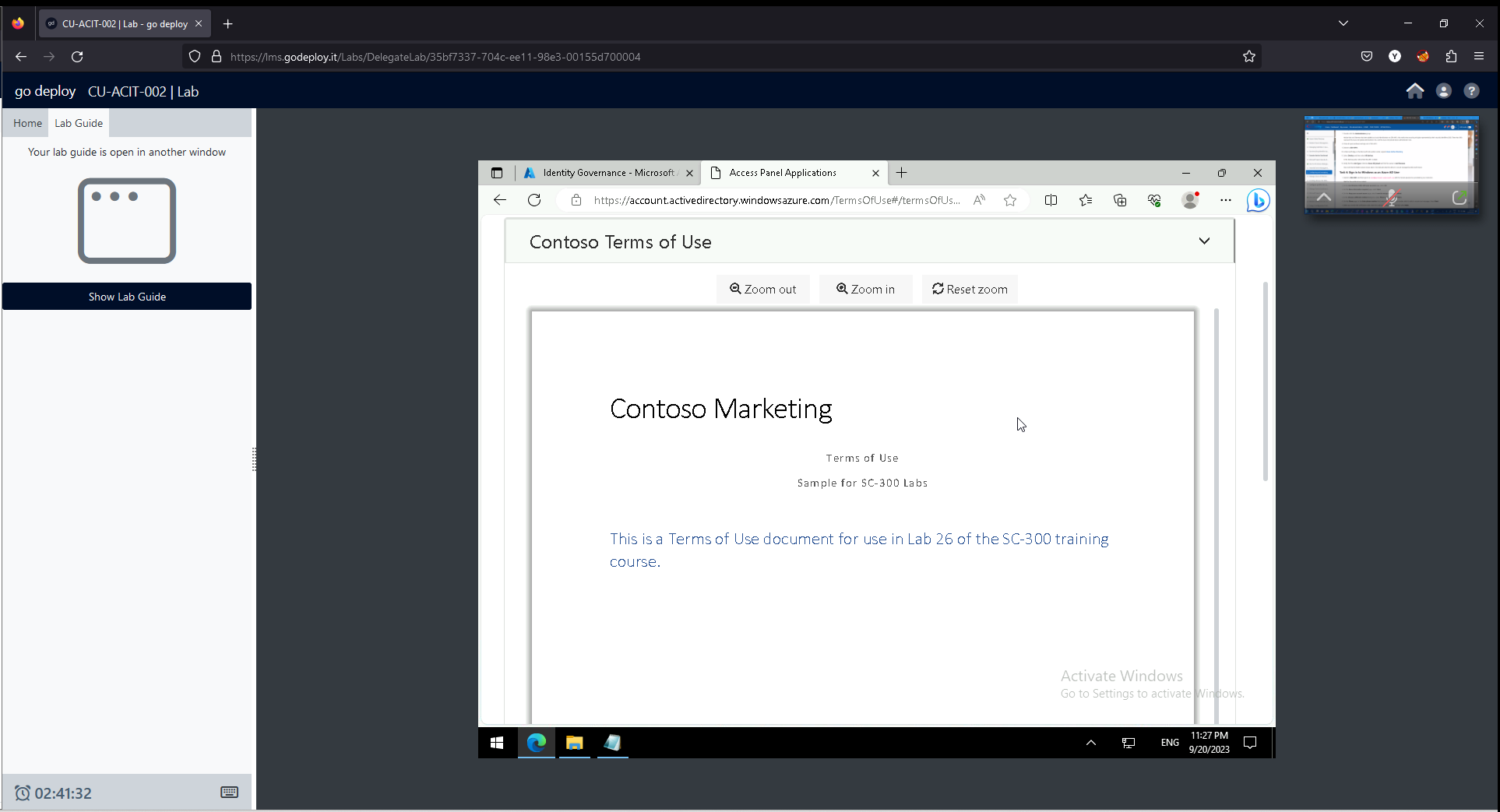


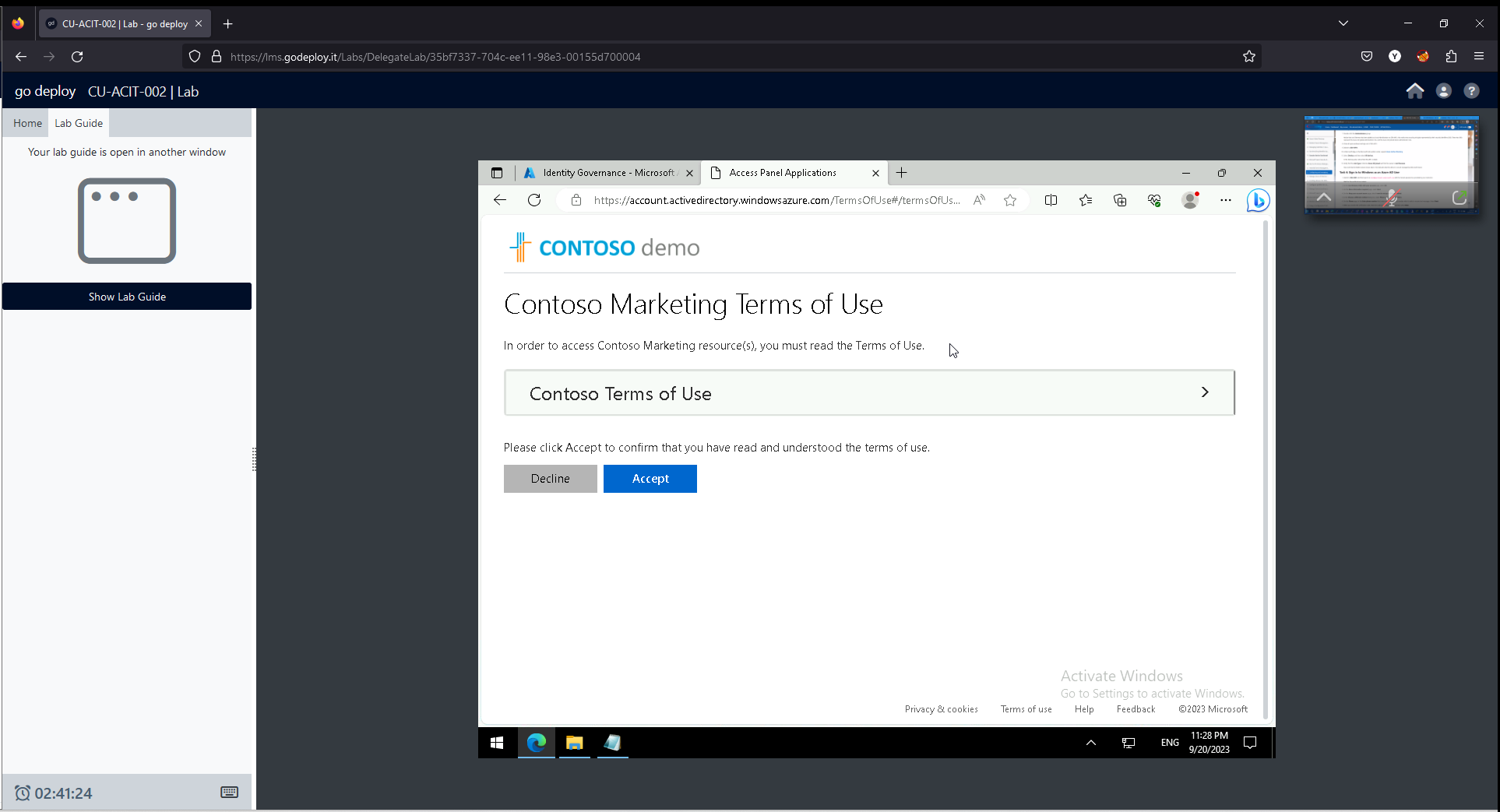


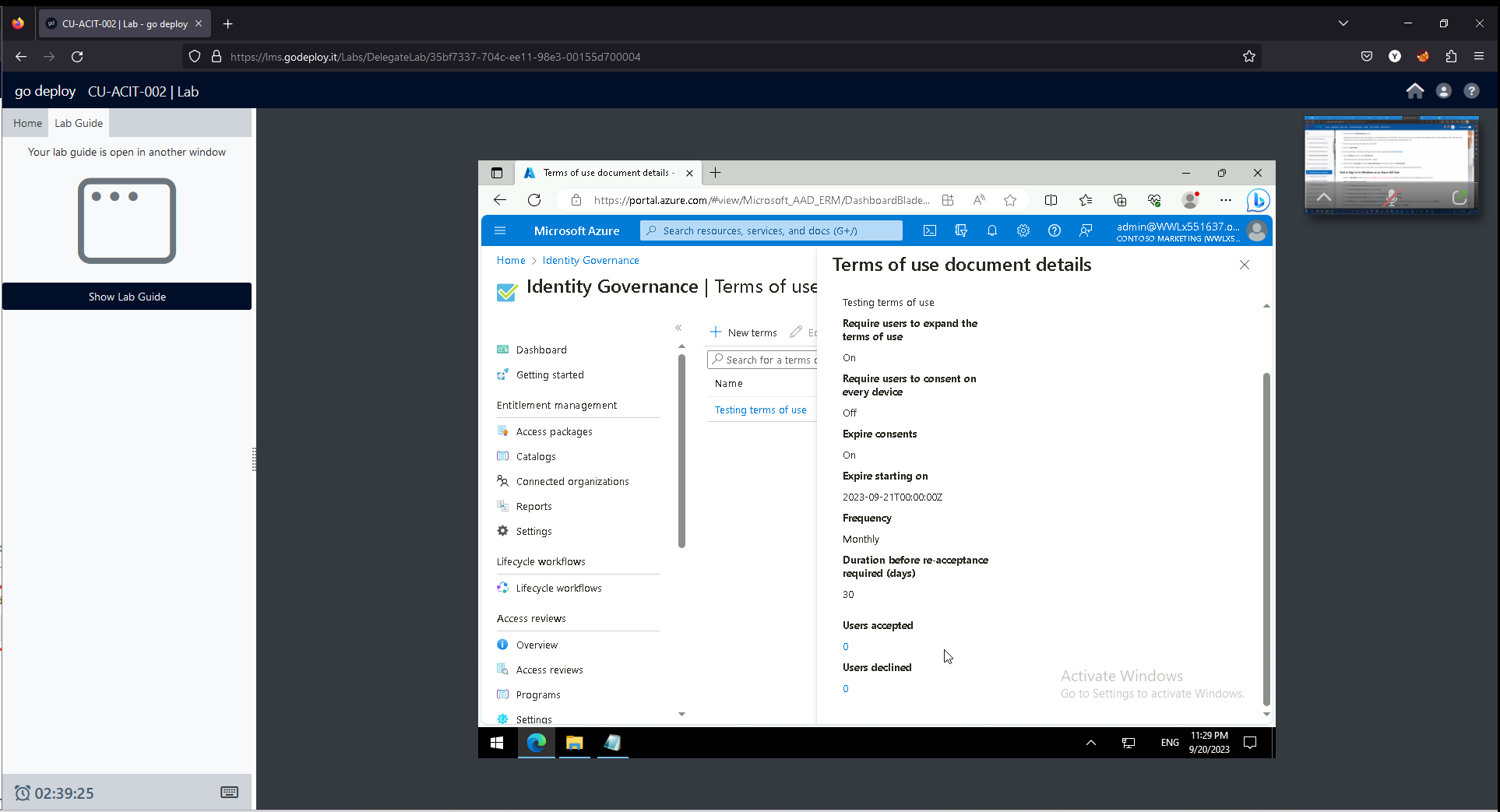


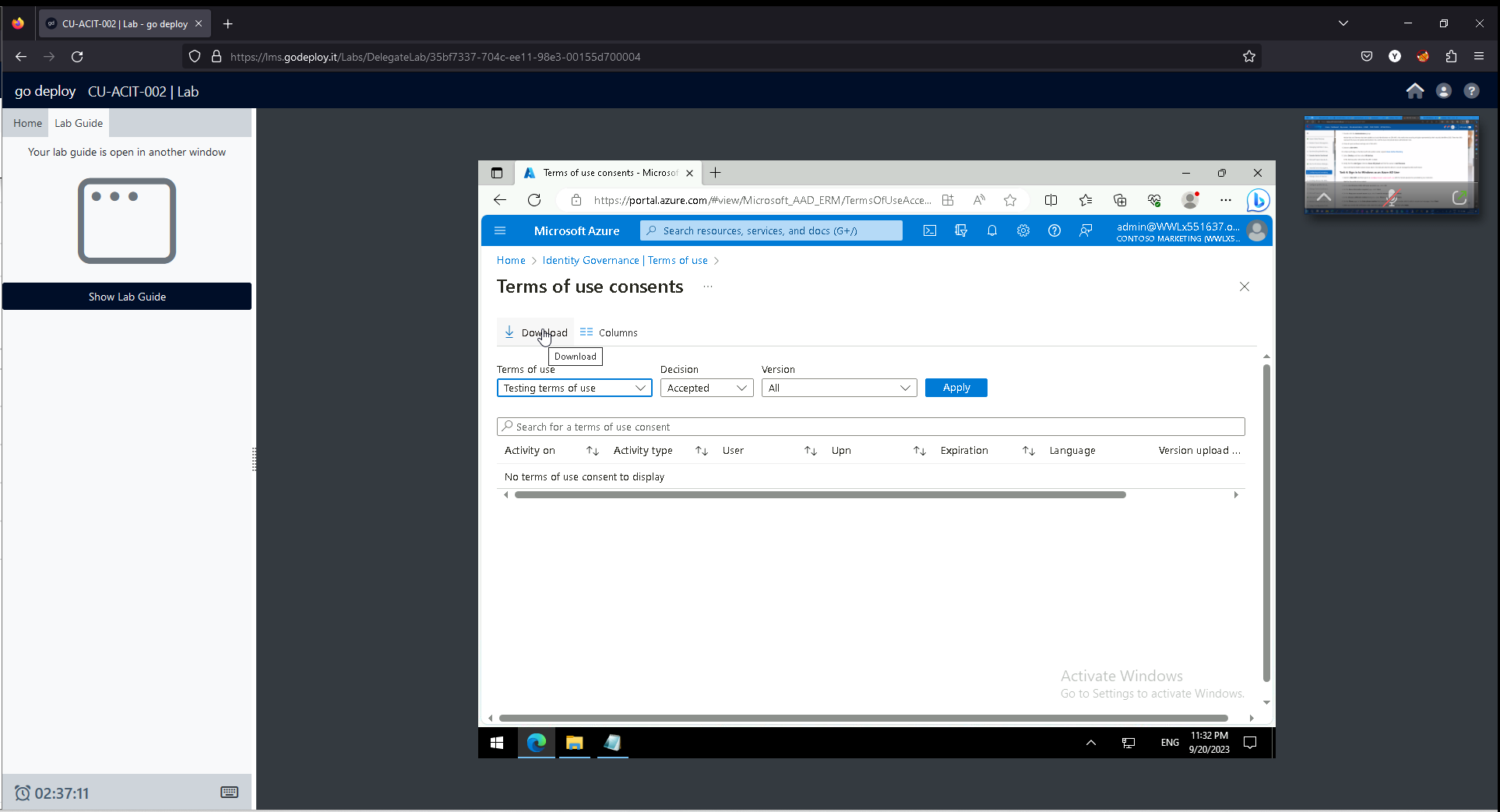


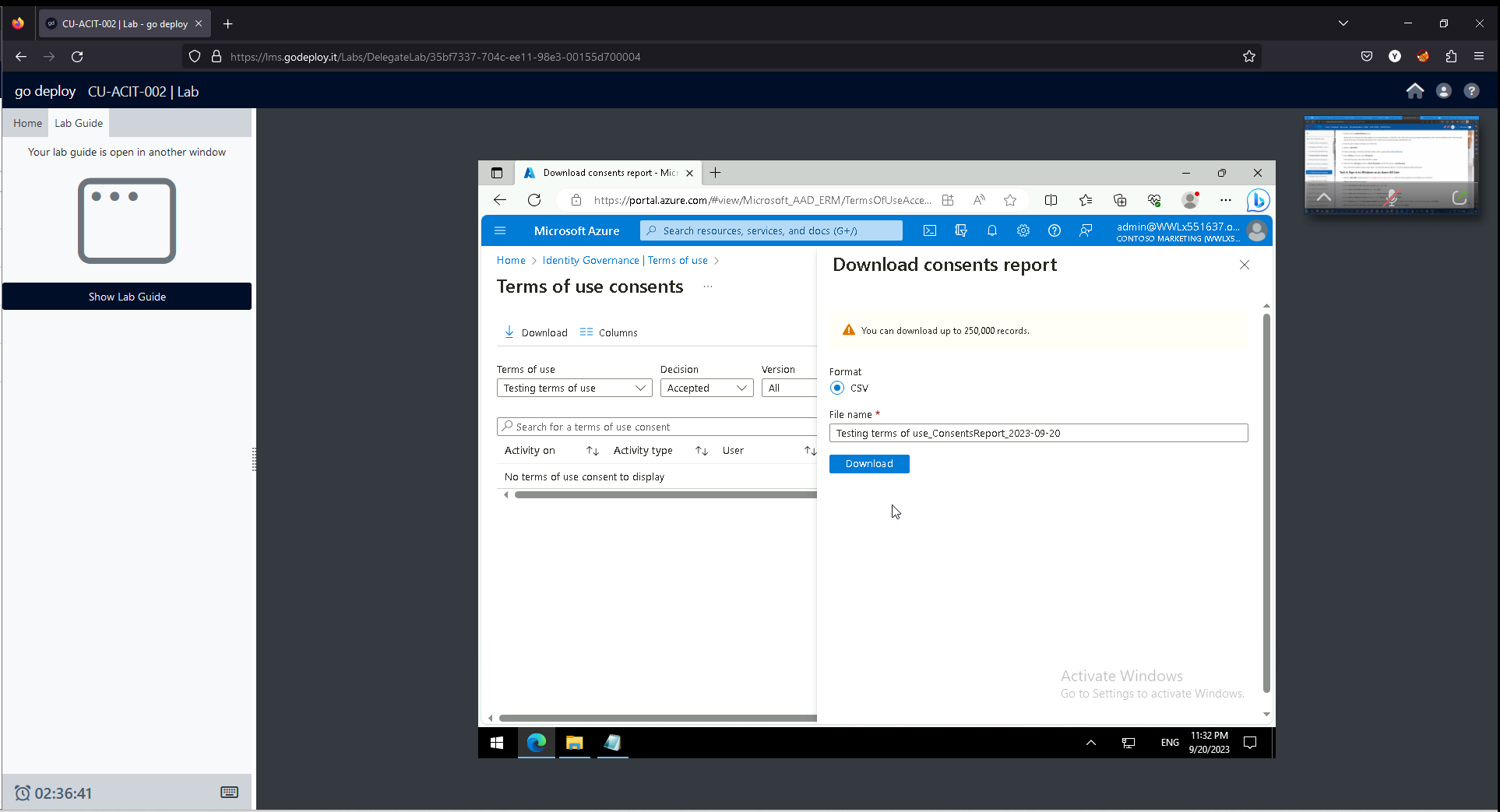


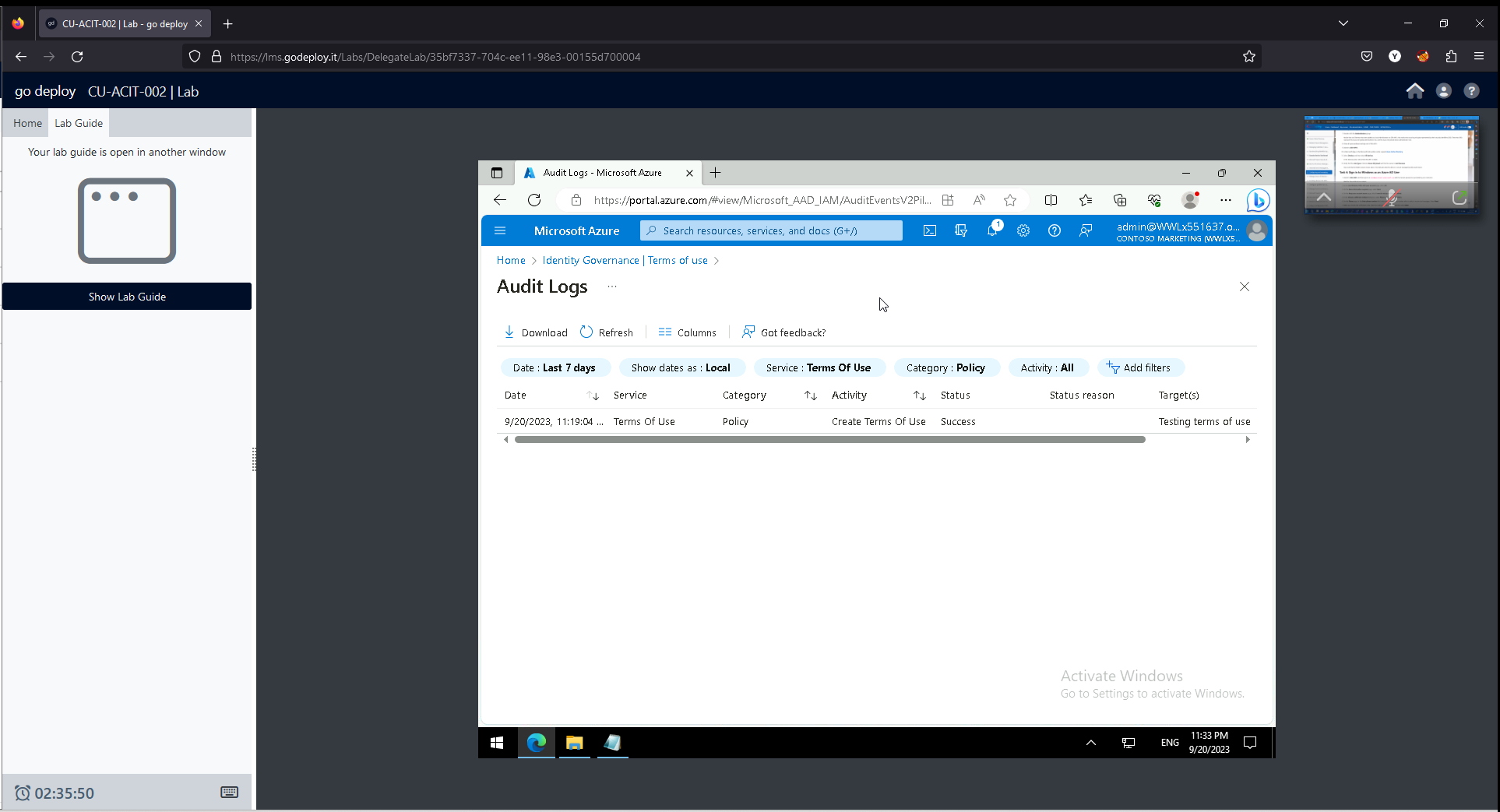


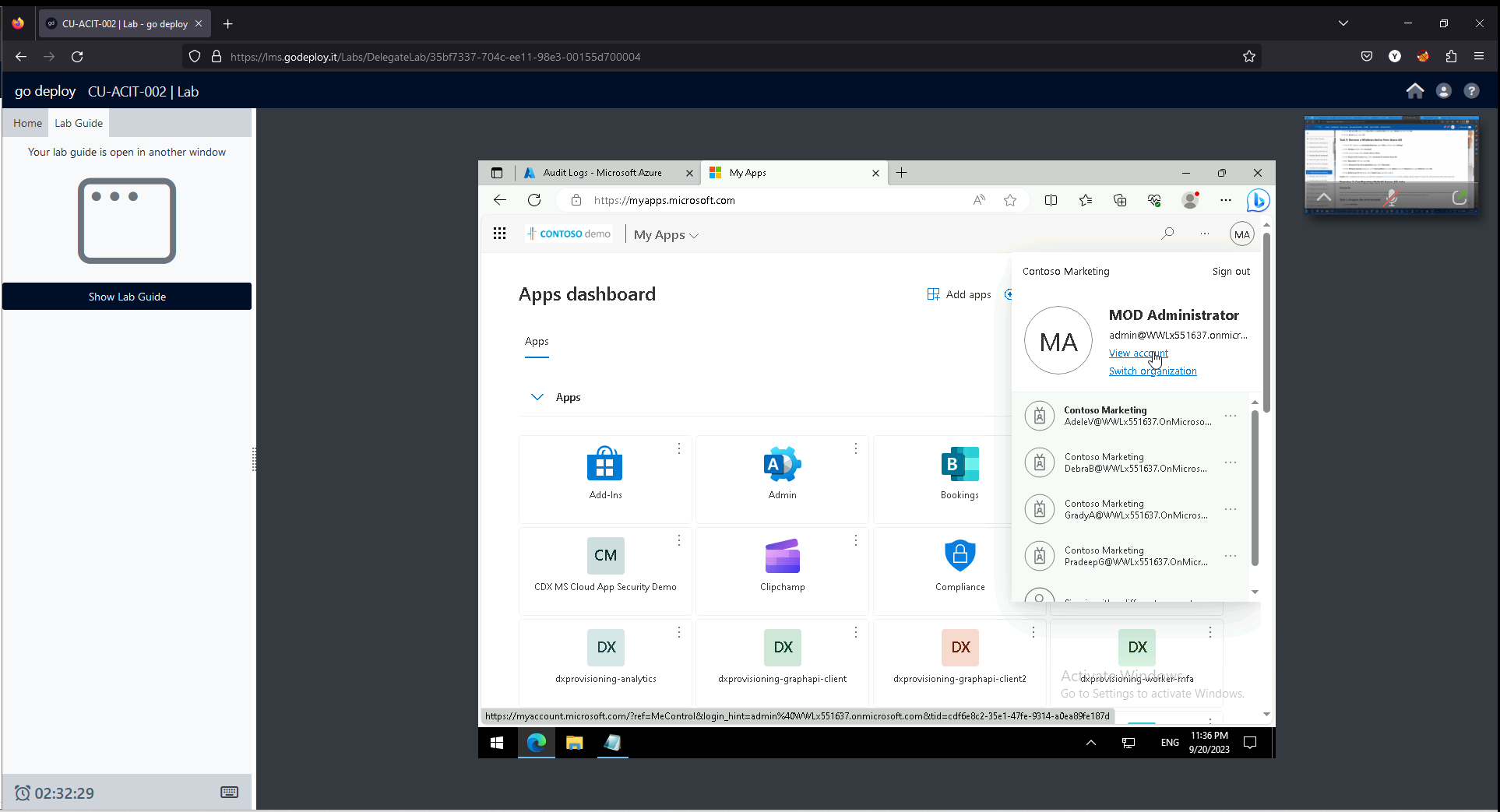


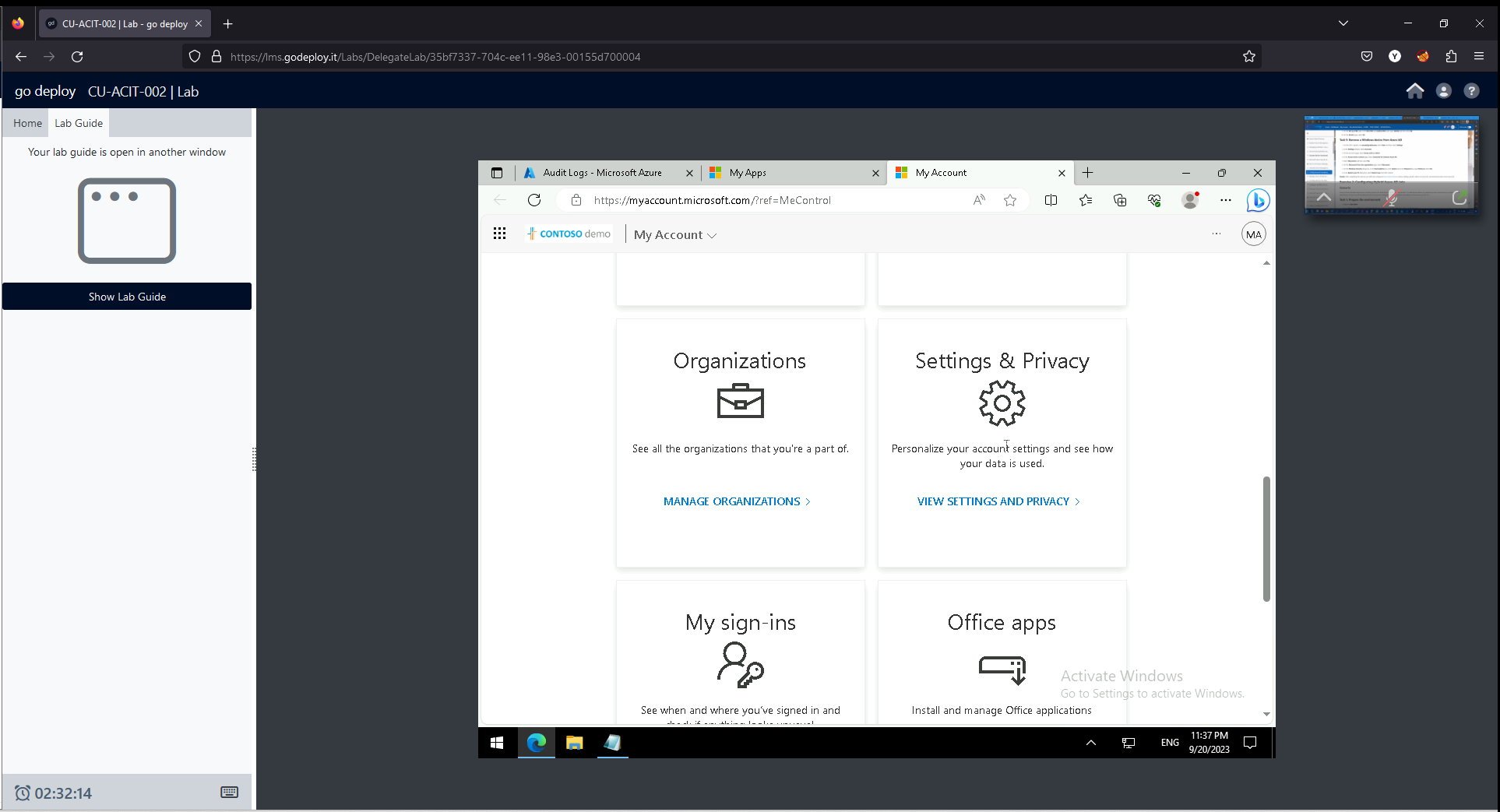


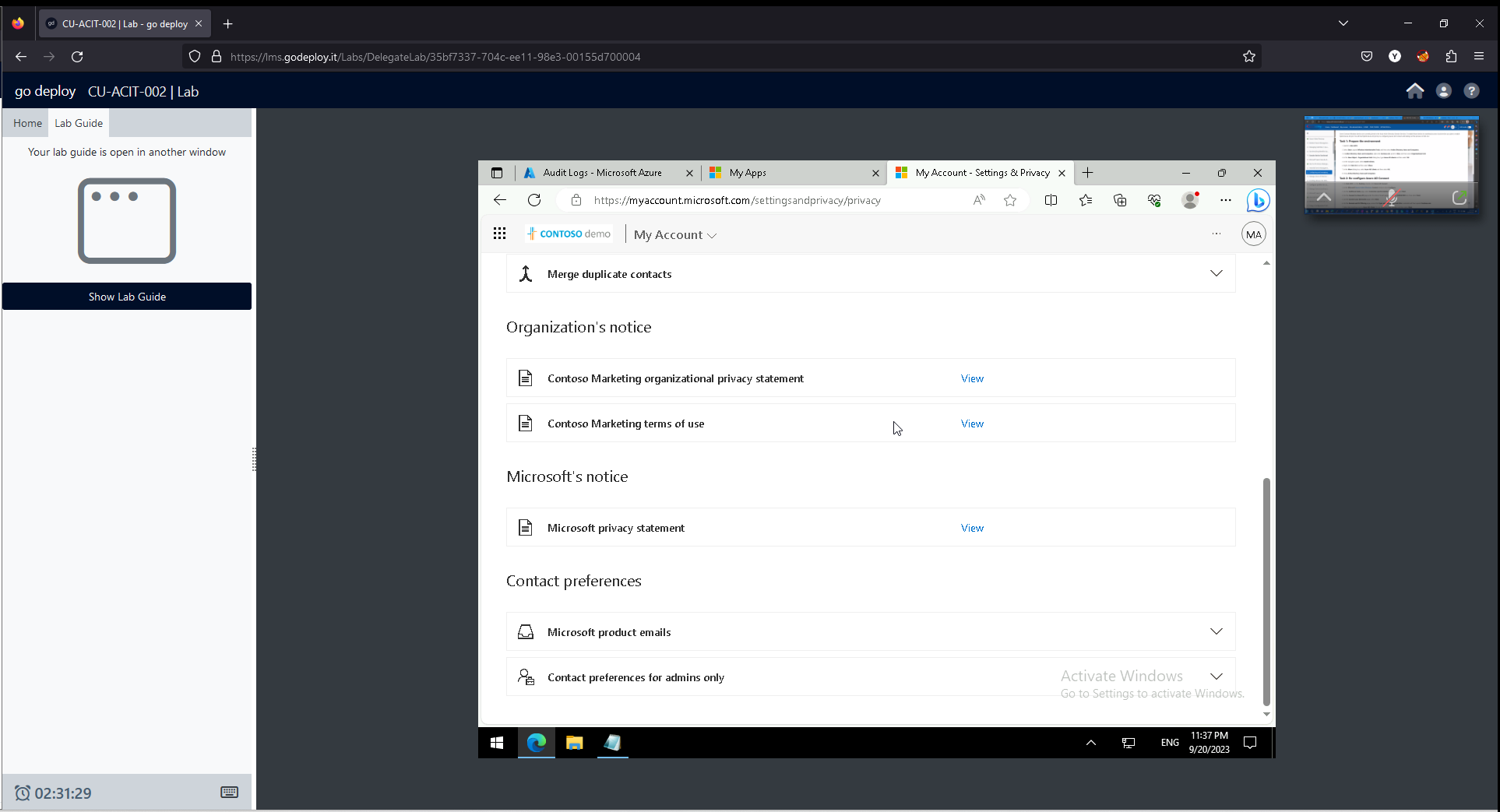


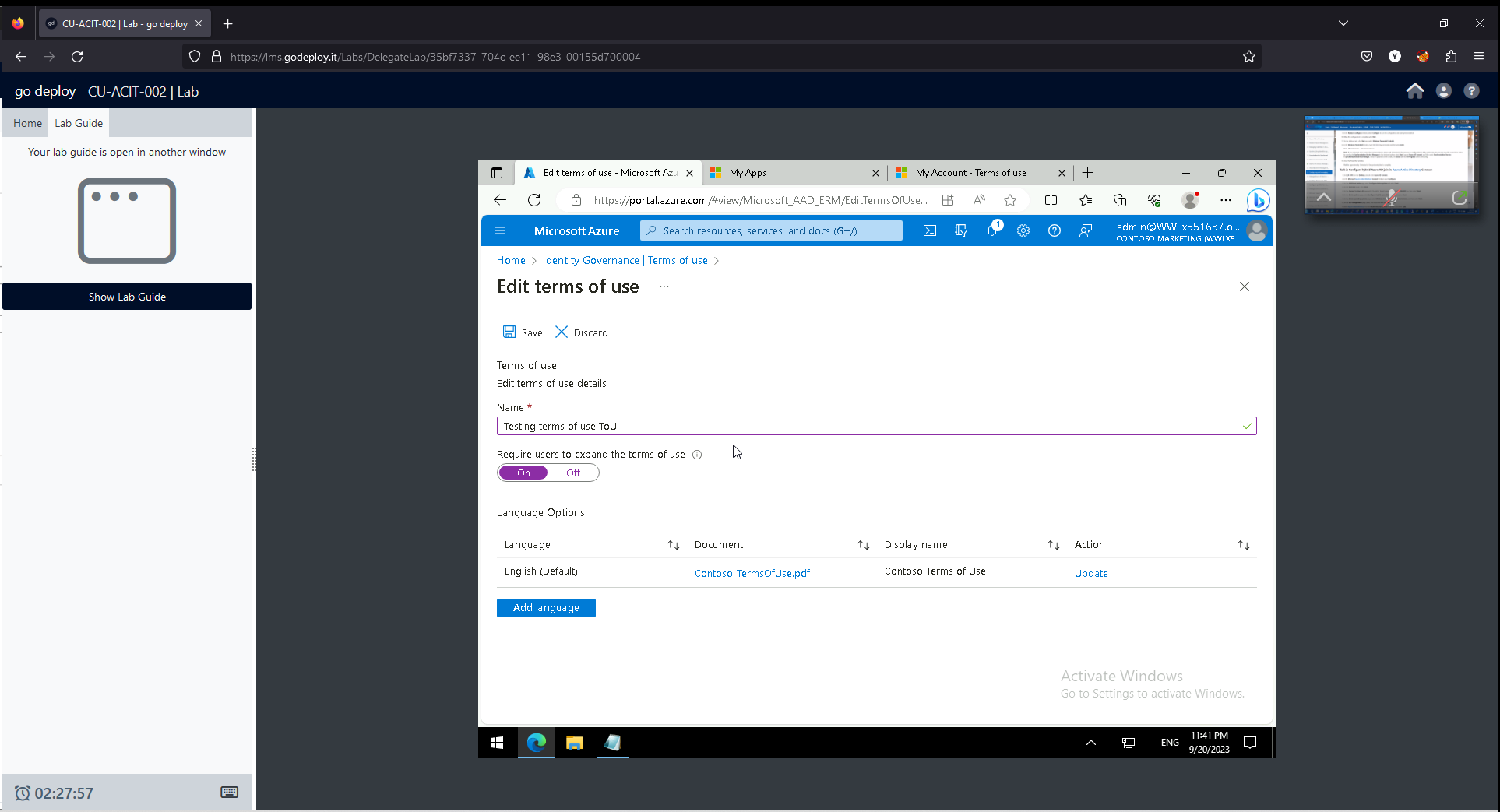


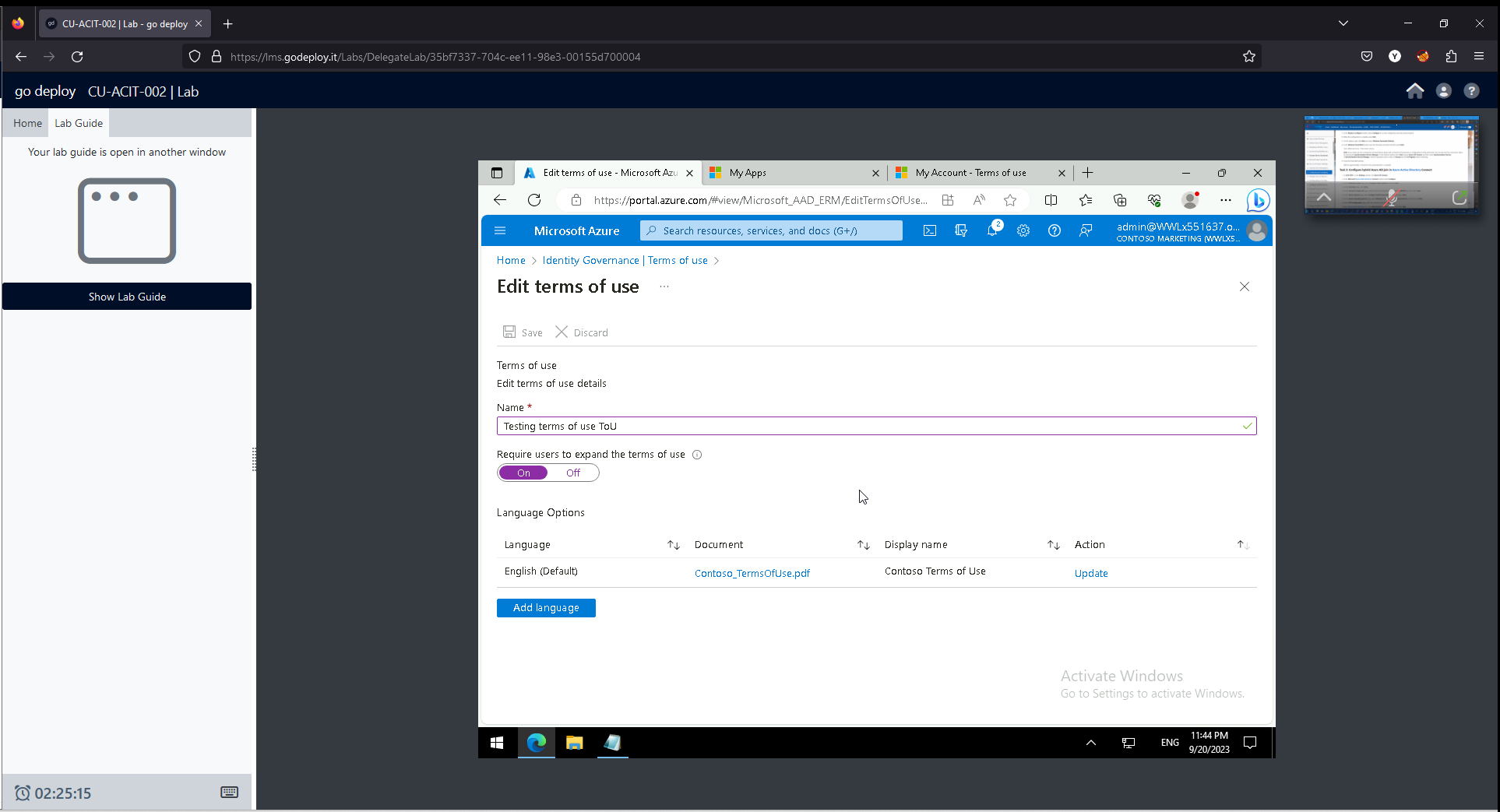


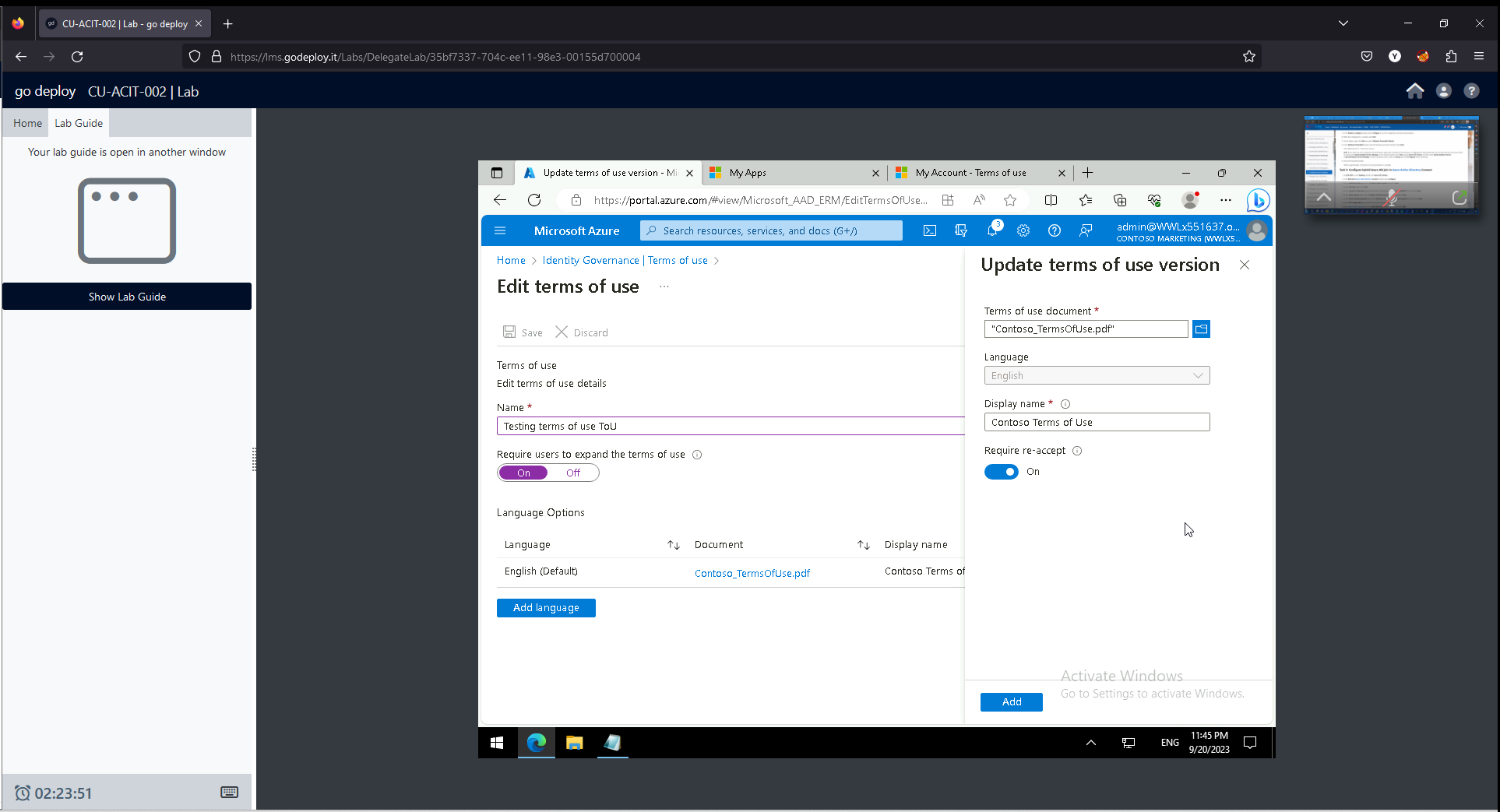












The "Add terms of use and acceptance reporting" feature within Azure Active Directory (Azure AD) allows organizations to enforce terms of use policies for accessing applications and resources, and it provides reporting capabilities to track user acceptance of these terms. Here's an executive summary highlighting how this feature supports compliance with the security strategy:

Executive Summary:

As part of our security strategy, it is paramount to ensure that all users within our organization adhere to our policies and terms of use when accessing applications and resources. The "Add terms of use and acceptance reporting" feature within Azure Active Directory (Azure AD) provides a robust framework to enforce these policies and monitor user compliance effectively.

Key Benefits:

1. **Policy Enforcement**: By incorporating terms of use agreements into the authentication process, Azure AD ensures that users must acknowledge and accept these terms before accessing applications and resources. This helps mitigate risks associated with unauthorized access and ensures that users are aware of their responsibilities regarding data protection and security.
2. **Customization**: The feature allows organizations to create tailored terms of use agreements that align with their specific security and compliance requirements. This flexibility enables us to address unique regulatory mandates or internal policies effectively.
3. **User Awareness**: Enforcing terms of use during authentication serves as a constant reminder to users about their obligations regarding security practices and data handling. This increased awareness can lead to a culture of security consciousness throughout the organization, ultimately reducing the likelihood of security incidents due to user negligence.
4. **Auditing and Reporting**: The feature includes comprehensive reporting capabilities that provide insights into user acceptance of terms of use agreements. This auditing functionality allows us to track and monitor compliance trends over time, identify potential areas of non-compliance, and take corrective actions promptly.
5. **Compliance Alignment**: By integrating terms of use enforcement and acceptance reporting into our security strategy, we demonstrate a commitment to regulatory compliance and risk management. This alignment strengthens our overall security posture and helps us meet the requirements of industry standards and data protection regulations.

In summary, the "Add terms of use and acceptance reporting" feature within Azure AD is a critical component of our security strategy, enabling us to enforce policy compliance, enhance user awareness, and demonstrate adherence to regulatory requirements effectively. By leveraging this feature, we can mitigate security risks, foster a culture of compliance, and bolster our organization's overall security posture.

**Task 7:**

Collaborate with the IT team to establish a feedback process that alerts the cyber security team to potential new risks, aiding in proactive risk management. Research the latest proactive risk management methods and recommend at least two methods.

Ref: <https://reciprocity.com/resources/what-is-proactive-risk-management/>

Here are two methods that proactive risk management.

* An emergency action protocol (EAP) is one example of a proactive risk management tactic. The EAP includes relevant policies and procedures for responding to an adverse event; it also details who is responsible for what in the event of such an incident. The goal is to remain prepared for adverse events and assure fast action if they occur.
* Employee training is another example of proactive risk management. Through walkthroughs, drills, and other practical actions, the organization can better prepare its workforce to recognize potential hazards and act appropriately to minimize damage.
* A third example are robust cybersecurity controls to prevent cyberattacks and data breaches. For instance, vulnerability management software enables security teams to find and fix security gaps before threat actors can exploit those gaps and harm the company.

**Section 3: Review and Revise Implemented Risk Management Strategies**

**Scenario Details:** After a few months of implementing the risk management strategies, you have been tasked with reviewing their effectiveness:

**Task 8:**

Identify benchmarks to measure the effectiveness of the strategies. Review metrics and reports available within Identity Secure Score, and provide the IT Team with metrics/reports that can be used to measure the effectiveness of the strategies that were implemented.

Measuring the effectiveness of strategies implemented within Identity Secure Score requires a comprehensive approach. Here are some benchmarks and metrics that can be used to evaluate the effectiveness:

1. **Reduction in Security Incidents**: Measure the decrease in security incidents related to identity theft, unauthorized access, phishing attacks, etc. Compare the number of incidents before and after implementing the strategies.
2. **Increase in Identity Secure Score**: Continuously monitor the Identity Secure Score provided by the platform. An increase in the score indicates improvements in identity security posture.
3. **User Authentication Metrics**:
   * Authentication Success Rate: Measure the percentage of successful authentications over a given period.
   * Authentication Failure Rate: Measure the percentage of failed authentication attempts. A decrease in this rate indicates improved security.
   * Time to Authenticate: Measure the time taken for users to complete the authentication process. Decreased time may indicate smoother authentication processes.
4. **Usage of Multi-Factor Authentication (MFA)**: Track the adoption rate of MFA among users. A higher adoption rate suggests better security practices.
5. **Privileged Access Management (PAM) Metrics**:
   * Percentage of Privileged Accounts: Track the proportion of privileged accounts compared to total accounts.
   * Compliance with Least Privilege Principle: Measure how well the organization adheres to granting minimal privileges necessary for users to perform their jobs.
6. **Phishing Resistance Metrics**:
   * Phishing Click Rate: Measure the percentage of users who click on phishing emails. A decrease in this rate indicates improved awareness.
   * Phishing Reporting Rate: Measure the percentage of reported phishing emails. An increase in reporting suggests improved vigilance among users.
7. **Compliance Metrics**:
   * Compliance with Security Policies: Monitor adherence to internal security policies related to identity management.
   * Regulatory Compliance: Ensure compliance with relevant regulations (e.g., GDPR, HIPAA) regarding identity protection.
8. **Time to Detect and Resolve Security Incidents**: Measure the time taken to detect and respond to identity-related security incidents. Decreasing this time helps in mitigating potential damages.
9. **Training and Awareness Metrics**:
   * Training Completion Rate: Measure the percentage of employees who have completed identity security training.
   * Post-Training Assessment Scores: Assess employees' understanding of identity security practices post-training.
10. **Cost of Identity-related Incidents**: Calculate the financial impact of identity-related security incidents, including mitigation costs, lost productivity, and reputational damage.

**Task 9:**

The IT Team has provided a report based on the Identity Secure Score for you to evaluate the effectiveness of the implemented strategies. The report includes the following data: Evaluate the data and provide a summary of the effectiveness of the implemented strategies. Include any recommendations to update the risk management strategies going forward.

|  |  |  |
| --- | --- | --- |
|  | **Implementation** | |
|  | **Before** | **After** |
| **Secure Score** | 34.23% | 53.82% |
| **# of risky sign-ins** | 4 | 0 |
| **Users not registered with MFA** | 0.00% | 98.00% |
| **Identity Governance – Access Packages** | 0 | 3 |
| **Access packages – delivery errors** | NA | 1 |

Based on the provided data from the Identity Secure Score report, it's evident that the implemented strategies have had a positive impact on the organization's identity security posture. Here's a summary of the effectiveness of the strategies along with recommendations for updating risk management strategies going forward:

1. **Secure Score Increase**: The significant increase in the Identity Secure Score from 34.23% to 53.82% indicates an overall improvement in the organization's identity security. This suggests that the strategies implemented have been effective in enhancing security measures.
2. **Reduction in Risky Sign-ins**: The decrease in the number of risky sign-ins from 4 to 0 is a positive outcome, indicating improved detection and prevention of potentially harmful authentication attempts. This reduction suggests that security controls are effectively mitigating risks associated with unauthorized access.
3. **Increase in MFA Adoption**: The drastic increase in the percentage of users registered with Multi-Factor Authentication (MFA) from 0% to 98% is a significant improvement. MFA adds an additional layer of security to user accounts, making them less vulnerable to unauthorized access. This indicates successful implementation and user adoption of MFA, enhancing overall security.
4. **Implementation of Identity Governance Access Packages**: The introduction of three Identity Governance Access Packages signifies progress in implementing access controls and governance measures. Access packages help in organizing and managing user permissions effectively, reducing the risk of unauthorized access to sensitive resources.
5. **Decrease in Access Package Delivery Errors**: The reduction in access package delivery errors from NA to 1 suggests improvements in the provisioning and delivery processes. However, the presence of even one error indicates room for optimization in the delivery workflow to ensure accurate and timely assignment of access privileges.

**Recommendations for Updated Risk Management Strategies**:

1. **Continuous Monitoring and Improvement**: Maintain a proactive approach to continuously monitor identity security metrics, identify emerging threats, and implement necessary enhancements to stay ahead of evolving risks.
2. **Enhanced Training and Awareness**: Provide regular training sessions and awareness programs to educate employees about the importance of identity security practices, including the use of MFA and adherence to access control policies.
3. **Automated Remediation**: Implement automated remediation processes to address access package delivery errors promptly and accurately, minimizing manual intervention and reducing the risk of misconfigurations.
4. **Regular Security Assessments**: Conduct periodic security assessments, including penetration testing and vulnerability scanning, to identify and remediate any vulnerabilities or gaps in the identity security infrastructure.
5. **Integration with Threat Intelligence**: Integrate Identity Secure Score with threat intelligence feeds to proactively detect and mitigate identity-related threats based on real-time information and industry best practices.