Rolling out two-factor authentication (2FA) involves several critical steps to ensure a smooth and secure deployment. Here is a checklist to ensure your success:

Pre-rollout Preparation:

1. **Assessment and Planning:**
    - Identify which employees do not have a personal or work email address or a mobile number on their employee record. A report can be created using the Employee Census template within Report Builder.
    - Empower your managers with reporting, in order to gather missing email addresses or mobile numbers from their direct reports, by leveraging Report Shipping.
    - Once the missing data has been received, update the appropriate fields on the details tab of the employee record.

2. **Understanding and Educating Your Team on 2FA:**
    - Educating your managers is a proactive way to assist with overcoming objectives for the implementation of 2FA. Share helpful information with your team and your managers on eSS 2FA and its overall impact to Security measures that are necessary to keep the company and your employees' data secure.

Deployment Checklist:

3. **Communications:**
    - Use the Notification Center to notify your employees about eSS 2FA and to send periodic reminders before it is launched.
    - Provide Clear Instructions on what your employees can expect once 2FA is enabled for eSS.
    - Address frequently asked questions (FAQs) regarding the new authentication process.

4. **Monitoring and Support:**
    - Provide support for users who may need assistance with setup.
    - Prepare support resources and personnel to handle inquiries and troubleshooting. Contact your APS Support team for technical items that cannot be resolved by you or your managers.

Post-rollout Evaluation:

5. **Training:**
    - Train support staff and managers on managing 2FA.
    - Educate employees on the importance of 2FA and how to recognize phishing attempts and other Security measures.

6. **Continuous Improvement:**
    - At Onboarding, require new employees to provide a mobile phone number and a personal email address, especially if they will not be provided a work email.
    - Stay updated on Security best practices and potential vulnerabilities.

By following this checklist, you can ensure a comprehensive and secure rollout of two-factor authentication within your organization.