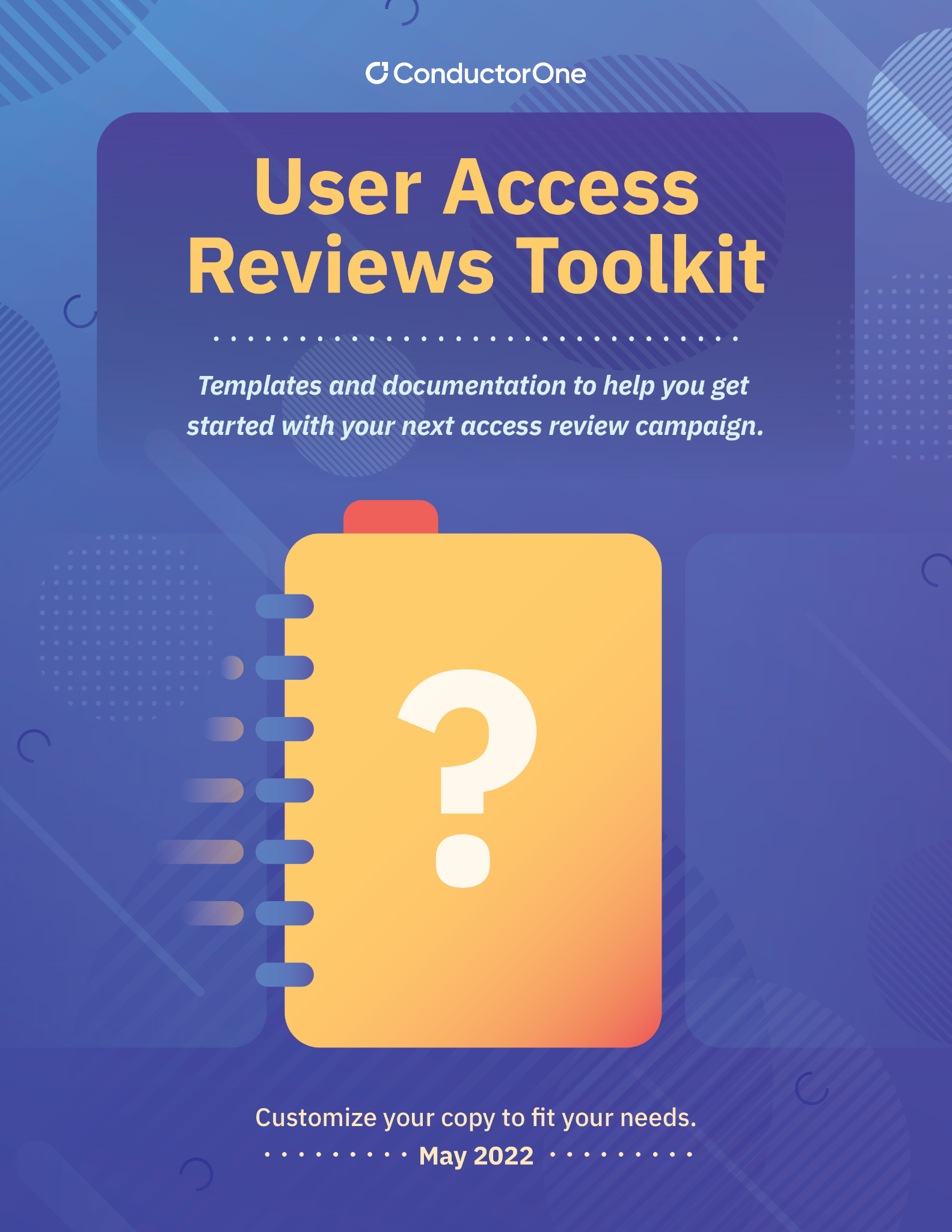
****

**README: ACCESS REVIEW TOOLKIT**

**INTRODUCTION**

The purpose of this toolkit is to provide a set of templates that security and GRC teams can use to conduct periodic user access reviews (UARs). User access reviews are a critical control of a security program that adheres to the principle of least privilege (POLP). They focus on reviewing standing access, roles, and permissions for users across business critical SaaS and IaaS applications to ensure users have appropriate levels of access. The ultimate goal of user access reviews is to revoke or adjust access, ultimately reducing the standing footprint of permissions.

At a high level, user access reviews require:

1 - Identifying in-scope systems and entitlements (levels of access, permissions, etc)

2 - Pulling data from in-scope systems, user directories, and HR systems

3 - Generating a list of granular access certifications at the appropriate levels of access

4 - Federating the access certifications to the appropriate reviewers for decisions on levels of access

5 - Remediating unnecessary or inappropriate access

Depending on the accessibility of these different systems, the ability to extract data from them, the maturity of automation and tooling at your company, you can usually expect user access reviews to take anywhere between 2 - 8 weeks to complete. This will depend largely on the size, scope, and complexity of the system involved, and whether the user access reviews are complete re-reviews vs incremental reviews.

**WHAT’S INCLUDED**

This toolkit contains the following templates and documents to aid in conducting manual user access reviews:

| **Doc** | **Description** | **How to Use** |
| --- | --- | --- |
| ***Notification Templates*** | Illustrative communications for notifying reviews that their input is required and/or is overdue | Copy the appropriate communication template, add and remove language where needed, and send to reviewers |
| ***Application Population Reports*** | A spreadsheet containing population reports from all of your in-scope systems | Populate application population reports for each system that’s in scope, prior to kicking off access reviews. You will also need to ingest HR and/or cloud directory data to map app users. This ensures that you have a complete picture of user status and so that you can identify the corporate identity responsible for the local user account and find the manager for that user, if needed. |
| ***Access Reviews*** | A spreadsheet containing the combined, master list of all access certifications and revocations for a campaign. | Each row of the access certification should be populated based on in-scope entitlements (group memberships, roles, etc). Once certifications are completed, revocations or access changes should be executed and tracked. |

**LEARN MORE**

To learn more about how to automate or create more seamless access reviews, download our [10 Access Reviews Best Practices guide](https://www.conductorone.com/resources/user-access-reviews-best-practices-guide/) or visit us at [www.conductorone.com](http://www.conductorone.com)