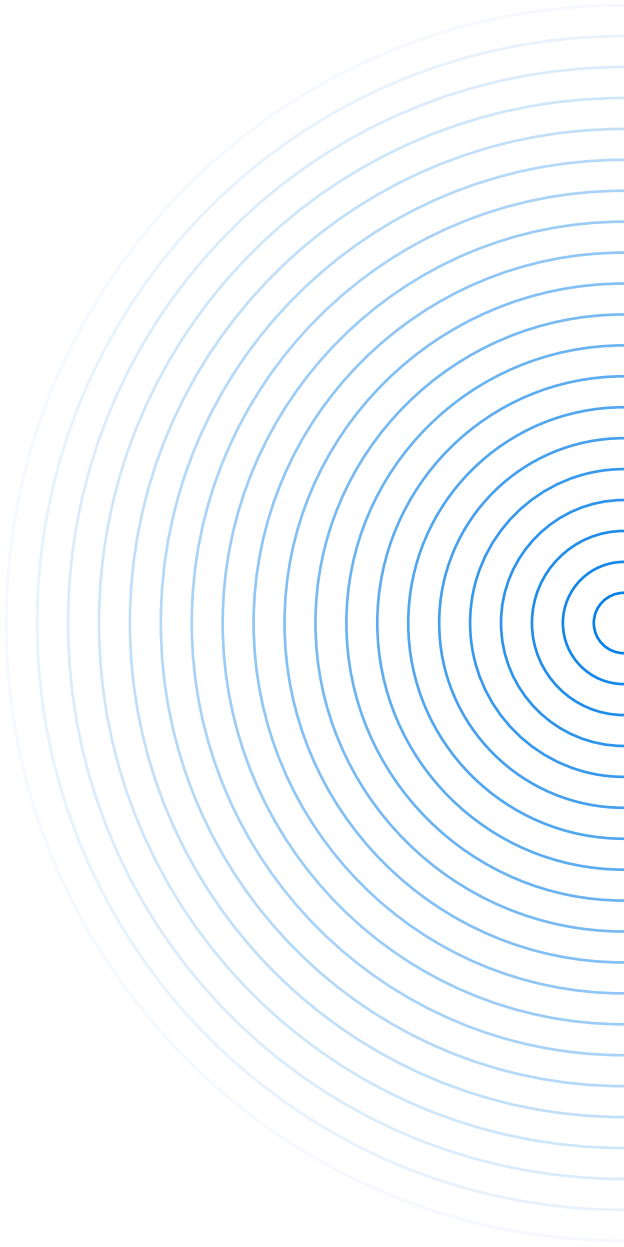
NIST 800-171 Compliance Checklist

1. Identify and Categorize Your CUI

- [ ] Implement an internal review to identify the CUI your organization handles
- [ ] Categorize CUI based on the 20 categories outlined in the CUI registry including:
  - [ ] Critical infrastructure
  - [ ] Defense
  - [ ] Export control
  - [ ] Financial
  - [ ] Immigration
  - [ ] Intelligence
  - [ ] International agreements
  - [ ] Law enforcement
  - [ ] Legal
  - [ ] Natural and cultural resources
  - [ ] North Atlantic Treaty Organization (NATO)
  - [ ] Nuclear
  - [ ] Patent
  - [ ] Privacy
  - [ ] Procurement and acquisition
  - [ ] Proprietary business information
  - [ ] Provisional
  - [ ] Statistical
  - [ ] Tax
  - [ ] Transportation



DRATA

2. Perform a Gap Analysis

- [ ] Perform a gap analysis to determine what requirements you're meeting and what controls you need to implement to achieve compliance
- [ ] Evaluate existing security controls to assess your current processes and procedures against the requirements set forth in NIST 800-171

3. Implement and Test Security Controls

- [ ] Develop and implement any controls that aren't currently in place to satisfy NIST 800-171
    - [ ] This includes developing policies, procedures, and processes related to the 14 requirement families
    - [ ] Baseline controls and specific details on each requirement can be found in the 800-171 publication
    - [ ] Once you implement the controls, begin testing them to ensure they're able to withstand potential threats

4. Document Your System Security Plan

- [ ] Appoint an internal team of senior IT professionals and any other relevant stakeholders within your organization to build out your SSP
- [ ] List all company personnel with responsibilities related to your system, such as system administrators and IT specialists.
- [ ] Collect documentation for your SSP, including security policies, system records, previous audit results, and system architecture documents
- [ ] Complete the SSP template using the template provided by NIST
- [ ] Create a plan of action and milestones (POAM)
    - [ ] If you uncover areas of non-compliance while creating your SSP, include them in your plan of action along with key milestones and a compliance deadline

- [ ] After completing the steps outlined in your POAM, update your SSP with plan modifications
    - [ ] Be sure to update version numbers in your SSP to keep track of ongoing modifications as infrastructure and technology continue to evolve

5. Conduct Ongoing Risk Assessments

- [ ] Continuously monitor your operations, assets, and individuals related to handling and protecting CUI
    - [ ] Ensure risk assessments consider threats, vulnerabilities and the likelihood and impact on your organization
- [ ] Conduct ongoing vulnerability scans of your system and system components

6. Develop an Incident Response Plan

- [ ] Establish an incident response plan that includes procedures for preparation, detection, analysis, containment recovery and user response activities
- [ ] Track and document system security incidents
- [ ] Regularly test your incident response plan to assess its ongoing effectiveness

7. Commit to Ongoing Employee Education

- [ ] Ensure managers, system administrators, and users of the company systems are trained on potential security risks and applicable policies, standards, and procedures related to the security of those systems
- [ ] Train personnel to carry out their security-related responsibilities