CHECKLIST

SYSTEM

- [ ] Can an attacker crash the system?
- [ ] Does the system track how many failed login attempts a user has experienced?
- [ ] What is the predominant operating system, if any?
- [ ] Does migrate a monolithic system to microservices decreases the technical debt?
- [ ] Is your main financial planning system and its supporting infrastructure vulnerable to manipulation?
- [ ] Who is behind the clickety clack of the keyboard breaking into your system?
- [ ] Are your systems correctly configured to prevent hackers from getting in?
- [ ] Do you make a backup of your system before applying patches?
- [ ] Should you differentiate between internal & external systems?
- [ ] Will you, the vendor, need to remotely log on to the system for administration or maintenance?
- [ ] What are the operating systems on the machines that you manage?
- [ ] Are your systems really protected?
- [ ] Which systems would cause the most significant disruption if compromised?
- [ ] What systems have the info that you need?
- [ ] What is the nature of the system/population being assessed?
- [ ] Do you keep a log file of any system changes and updates?
- [ ] Does the system permit electronic approvals?
- [ ] What is the configuration, health, or operating system status?
- [ ] Can an attacker completely take over and manipulate the system?
- [ ] Does migrating a monolithic system to microservices decrease the technical debt?
- [ ] What systems and networks are allowed to be tested?
- [ ] Does your system have the ability to do throttling/rate limiting by IP to a specific ISP?

CHECKLIST

- [ ] What it systems do you have in your enterprise?
- [ ] NOTES: