WORKSHEET:
How to Assess a Cyber Security Provider

When you choose a cyber security service provider you are trusting a partner company to take over roles that are vital to the safe operation of your IT systems. Due to the importance of this issue and its technical complexity, this is not an easy decision.

To help track your assessment of a provider, we have prepared a worksheet that allows you to document your needs in cyber security and compare three providers in several important areas.

Self Assessment

- [ ] Y [ ] N Your cyber security needs
- [ ] Y [ ] N IT asset inventory and accounting
- [ ] Y [ ] N Create IT Risk Assessment
- [ ] Y [ ] N Regular patching and software updates
- [ ] Y [ ] N Development of a data security policy
- [ ] Y [ ] N User training
- [ ] Y [ ] N Penetration testing
- [ ] Y [ ] N Other:

PROVIDER ASSESSMENT

Area of Evaluation	Provider 1	Provider 2	Provider 3
Provider's team successfully communicates complex technical issues			
Understands our business goals and plans			
Has worked with our technology before			
Offers custom solutions			
Integrates existing solutions			
Offers Security Incident and Event Monitoring (SIEM)			
Monitors network intrusion			
Provides network behavior analytics			
Monitors endpoints			
Provides reports			
Provides real-time dashboards			

Area of Evaluation	Provider 1	Provider 2	Provider 3
Can effectively explain the meaning of data collected through monitoring tools			
Conducts penetration testing			
Conducts phishing tests			
Provides social engineering test scenarios			
Is flexible based on your growth targets			
Can respond immediately to changes in the security landscape			
Offers prerecorded training			
Offers live customized training			
Provides instructional design services			
Integrates with our Learning Management System (LMS)			
Offers per-user pricing			
Offers per-device pricing			
Carries relevant certifications			
Can support our compliance needs			
Has scalable technology and support			
Other:			