Virtual CISO –
Security Program Maturity Assessment

eSentire will review and assess the effectiveness of Client's internal security program against the "Core 15" assessment areas of eSentire's "Cybersecurity Reference Model", other cybersecurity standard(s) or regulatory requirements as may be mutual agreed to by Client and eSentire in writing. The "Core 15" areas of the eSentire Cybersecurity Reference Model include:

- IT Security Strategy & Governance
- Human Resources
- Security Architecture
- IT/Security Risk Management
- Monitoring & Operations
- Incident Response
- Information Management
- Asset Management
- Vulnerability & Patch Management
- Third Party Risk Management
- Compliance & Audit
- Secure Network Design
- Authorization & Access Controls
- Malicious Code Prevention
- Secure Builds

The Security Program Maturity Assessment will also include meetings with appropriate Client designates and subject matter experts, eSentire evaluating risk areas and defining overall risk levels of Client's internal security program, as well as eSentire evaluating and reporting to Client on the quality of Client's processes, routines, and controls. eSentire will provide to Client a baseline assessment of Client's internal security program against eSentire's "Cybersecurity Reference Model", including an executive summary and details findings report in Microsoft Word and Excel formats.