CASE STUDY

Government Cyber Security Assessment

STATE DEPARTMENT OF REVENUE

Cyber **security risk assessments** are critical to your organization's effective information security strategy.

It's also important for you to find the right balance between security, compliance, and progress by evaluating the risk and vulnerabilities within your IT infrastructure.

Here's a case study explaining how System Soft Technologies helped with the security at a government agency, successfully improving the State Department of Revenue's cyber security posture and meeting U.S. Internal Revenue Service (IRS) compliance requirements.

Situation

A state-sponsored administrative entity of the Department of Revenue (DOR) requested a third-party cyber security assessment as part of its regulatory compliance required by the IRS. This DOR also identified a need to implement and expand an insider threat program, guarding against trusted insiders who may commit fraud.

This DOR didn't have an insider threat plan in place with approved and implemented policies and procedures. It also didn't have a defined risk management program.

This DOR requested RFPs and then chose System Soft as its trusted, third-party, government cyber security partner in large part because of System Soft's quality of work, deep experience and affordable cost. System Soft's proposal, which outlined its knowledge, experience and resources, were pertinent factors meeting this DOR's goals and driving its decision to partner with System Soft.

Strategy

For this DOR, System Soft developed and executed an information security plan and assessments, which included:

- Handling detailed analysis of system and network vulnerabilities.
- Discovering gaps in IT security governance.
- Assessing patching methods.
- Evaluating current network security capabilities.
- Examining existing security incidents.
- Conducting phone system analysis.
- Administering mainframe testing.
- Reviewing systems controls and current policy and procedures.

System Soft also worked within this DOR's environment as a third-party auditor, creating a report for its CIO, which included:

- Analyzing hundreds of application databases.
- Conducting assessments, gap analysis and audits.
- Providing detailed remediation guidance.

Outcome

During the cyber security assessment, some items were uncovered and required remediation. These were handled by this DOR and its staff. This DOR remediated all issues, improving its overall cyber security posture and meeting IRS compliance requirements.

Because of superior client service, a customized approach and expert project management, System Soft now works as a consultant and trusted advisor to this DOR.

This DOR was so appreciative of System Soft's efforts, it renewed and extended the working agreement by three more years for similar services.

Conclusion

IT departments can strengthen their cyber security posture by partnering with an experienced, trusted, independent third party to perform security assessments.

When seeking an IT risk management partner and a cyber security solution, it's important you turn to one with the most trusted and comprehensive risk assessments available in the IT security industry.

System Soft can help you improve your overall **cyber security** posture and meet required compliance standards.

Contact us to get started on your professional evaluation for risk and compliance.