THE RISK-BASED AUDIT PROCESS

Transform cybersecurity compliance requirements (SOC 2, ISO 27000, HITRUST, PCI DSS) into a meaningful, risk-based audit strategy.

1 Start with Key Business Risks

Identify critical data, systems, and business impacts in case of failure.

2 Map Compliance to Risks

Determine what risks each compliance control is attempting to address.

RISK-BASED AUDIT

3 Evaluate Control Effectiveness

Assess if controls are truly reducing their associated risks.

4 Translate to Executive Language

Communicate risk trends and priorities for executive decision-making.

Continuous Improvement Cycle

- **Efficiency** by focusing efforts on real threats
- **Strategic value** by connecting cybersecurity to business risks
- **Improved security outcomes** that executives will support.

INFOSEC SPECIALISTS

CYBERSECURITY. SIMPLIFIED.