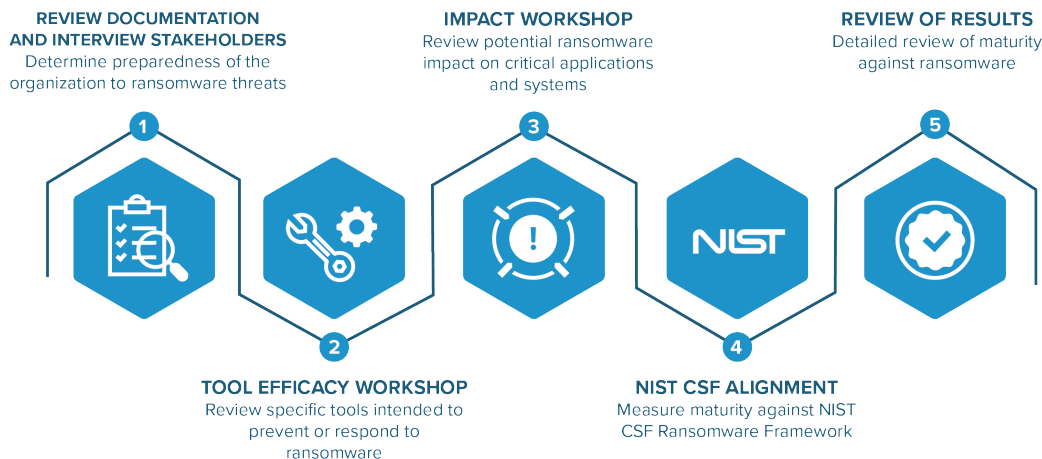# Ransomware Assessment

The K logix Ransomware Assessment, through documentation review and various interviews/workshops, collaboratively looks at attack surfaces from the perspective of ransomware exposure.

## RANSOMWARE ASSESSMENT OVERVIEW

- Review relevant documentation and interview customer stakeholders. The focus of interviews is the preparedness of the organization to ransomware threats.
- Two workshops are included in all Ransomware Assessments:
    - The first is a workshop to review specific tools intended to prevent or respond to ransomware, wherein K logix will examine the efficacy of the tools as informed by the client.
    - The second workshop is an impact workshop focused on critical applications and systems and the impact that a successful ransomware attack would have on them.
- Aligning the interviews, workshops, and measuring the maturity against the NIST CSF Ransomware Framework, provides clients with a detailed look at their maturity against ransomware.



**REVIEW DOCUMENTATION AND INTERVIEW STAKEHOLDERS**
Determine preparedness of the organization to ransomware threats

**IMPACT WORKSHOP**
Review potential ransomware impact on critical applications and systems

**REVIEW OF RESULTS**
Detailed review of maturity against ransomware

**TOOL EFFICACY WORKSHOP**
Review specific tools intended to prevent or respond to ransomware

**NIST CSF ALIGNMENT**
Measure maturity against NIST CSF Ransomware Framework

## BENEFITS

- Measurement against the NIST CSF Ransomware Framework
- Expert led review of current anti-ransomware tools
- Discussion of the business impact of ransomware