

Title of Nomination	Enterprise Information Security Business Risk Assessment
Project Manger	Theresa Masse
Agencies/Departments	Department of Administrative Services (DAS) Enterprise Information Strategy & Policy Division (EISPD)
NASCIO Category	Information Security and Privacy

The Business Challenge: In the 2005 Legislative Session, Oregon Revised Statute (ORS) 182.122 passed designating the Department of Administrative Services (DAS) as the “single point of accountability” for information security at the State. In support of this mandate, the Enterprise Security Office (ESO) instituted a security strategy wherein DAS would work collaboratively with State agencies to ensure the State’s security posture is at an acceptable level.

The Goal: The goal of the Information Security Business Risk Assessment was to provide a method that would assist agencies in prioritizing the use of resources and providing a secure operational environment for all information.

The Assessment: The *Annual* Enterprise Information Security Business Risk Assessment was launched in 2007 and focused on identifying key business functions and areas of information security concerns. The results of the assessment:

- represent a cross section of state government and are aggregated to produce a statewide report and contribute to the enterprise information security Key Performance Measures.
- highlighted **five theme areas** that the State should focus on including;
 1. Business Continuity Management
 2. Incident Management
 4. Information Owner and Classification
 5. Security Awareness and Training

Significance and Benefits

Standard Methodology: Used to measure improvement in the state’s security posture at the enterprise level.

Commitment to Continuous Improvement: Participating agencies have committed to taking the steps to ensure incremental improvement, and acknowledge this initiative as adding a positive and tangible value to their information security efforts.

Non-Financial Return on Investment: Through active agency involvement and intensified analysis of their security posture, agencies now have:

- a heighten awareness and a proactive method to assist in reducing the cost associated with a security breach, whether it is due to loss of data or application downtime impacting access by users.
- the ability to reduce the threat of fines by actively meeting and monitoring their regulatory compliance requirements.