

## Expected ARCC

## Expected ARCC by Vulnerability

## Expected ARCC by Threat

HOME Instructions

Single Studies

Capability Ratings  
Bar ListRisk Valuations  
Bar ListVulnerability Valuations  
Bar ListThreat Valuations  
Bar List

Advanced Analytics

Capability Worksheet

NIST  
800-53

Study Comparisons

Capabilities

Risk Valuations

Total Risk

Filter Studies



Risk ID	Expected ARCC
CM-T13	\$4,437,200
CM-T05	\$3,935,900
CM-T25	\$3,926,700
CM-T24	\$3,904,100
CM-T01	\$3,011,600
<b>Total</b>	<b>\$19,215,500</b>

Vuln description	Expected ARCC
PS - Personnel Security	\$22,958,200
<b>CM - Configuration Management</b>	<b>\$19,215,500</b>
PL - Planning	\$9,142,400
CA - Security Assessment and Authorization	\$6,466,200
PM - Program Management	\$6,123,000
AU - Audit and Accountability	\$5,966,800
MA - Maintenance	\$5,771,800
AC - Access Control	\$5,589,900
RA - Risk Assessment(s)	\$5,584,300
SI - System and Information Integrity	\$4,763,800
SC - System and Communications Protection(s)	\$3,384,300
AT - Awareness and Training	\$2,901,900
IA - Identification and Authentication	\$2,482,300
MP - Media Protection	\$2,126,800
SA - System and Services Acquisition(s)	\$1,938,200
PE - Physical and Environmental Protection(s)	\$1,877,700
CP - Contingency Planning	\$727,900
IR - Incident Response	\$264,400
<b>Total</b>	<b>\$105,283,600</b>

Threat Description	Expected ARCC
T13-Attackers exploit and infiltrate through network devices whose security configuration has been weakened over time by granting, for specific short-term business needs, supposedly temporary exceptions that are never removed.	\$4,437,200
T05-Attackers exploit weak default configurations of systems that are more geared to ease of use than security.	\$3,935,900
T25-Attackers access data and networks from inside the company enabled by insufficient physical security, controls and procedures	\$3,926,700
T24-Attackers are able to gain unauthorized access to systems due to gaps in security governance and/or enforcement of security policies	\$3,904,100
T01-Attackers continually scan for new, unprotected systems, including test or experimental systems, and exploit such systems to gain control of them.	\$3,011,600
<b>Total</b>	<b>\$19,215,500</b>