15S.24 IT Risk Management and Information Systems Security

Description

Address 80% of high value risks within 30 days. Establish oversight by the Cybersecurity Steering Committee to assure consistent risk acceptance decisions. Visualize vulnerabilities on all IP based systems.

Special Designations: OSI, STI

Commentary (June 2015)

Activity is green. In June, 15 High Value Risks were identified, and were addressed within the 30 day period. In June, multiple FAA entities participated in CYBERGUARD, a cyber security exercise led by DoD. Results from the FAA Cyber Exercise in April and the CYBERGUARD exercise informed revisions to the FAA's Incident Response Process. That revision was briefed to the FAA Cybersecurity Steering Committee, and will be finalized by the end of September.

Commentary (May 2015)

The FAA Cybersecurity Steering Committee reviews incident information monthly for all three operating domains. Action has been taken to correctly associate incidents to the appropriate domain, as well as review architecture of existing technologies for effective visibility. Work continues to solidify the FAA Cyber Incident process based on lessons learned from the FAA Cyber Exercise. No high value risks were identified for May.

Status Table (Quantitative Metric - Meet or Exceed)

Period	Target	Actual	Status
10/2014	3	3	Green
11/2014	3	3	[Green]
12/2014	3	3	Green
01/2015	3	3	Green
02/2015	3	3	[Green]
03/2015	3	3	[Green]
04/2015	3	3	[Green]
05/2015	3	3	[Green]
06/2015	3	3	Green

✓ Indicates that the item is complete.