BUREAU OF THE
Fiscal Service
U.S. DEPARTMENT OF THE TREASURY

SECURITY BEYOND A “SYSTEM”

Fiscal Service’s Approach to External Services

Jim McLaughlin, CISSP
Manager, Security Policy & Risk Management

Ralph Jones
Security Analyst

Federal Computer Security Program Managers’ Forum August 17, 2016

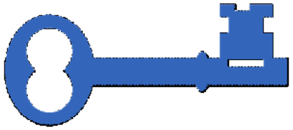
Overview

- Some operations that are handled by external service providers are NOT “Systems”

- These services still need appropriate security to ensure ongoing operational resiliency

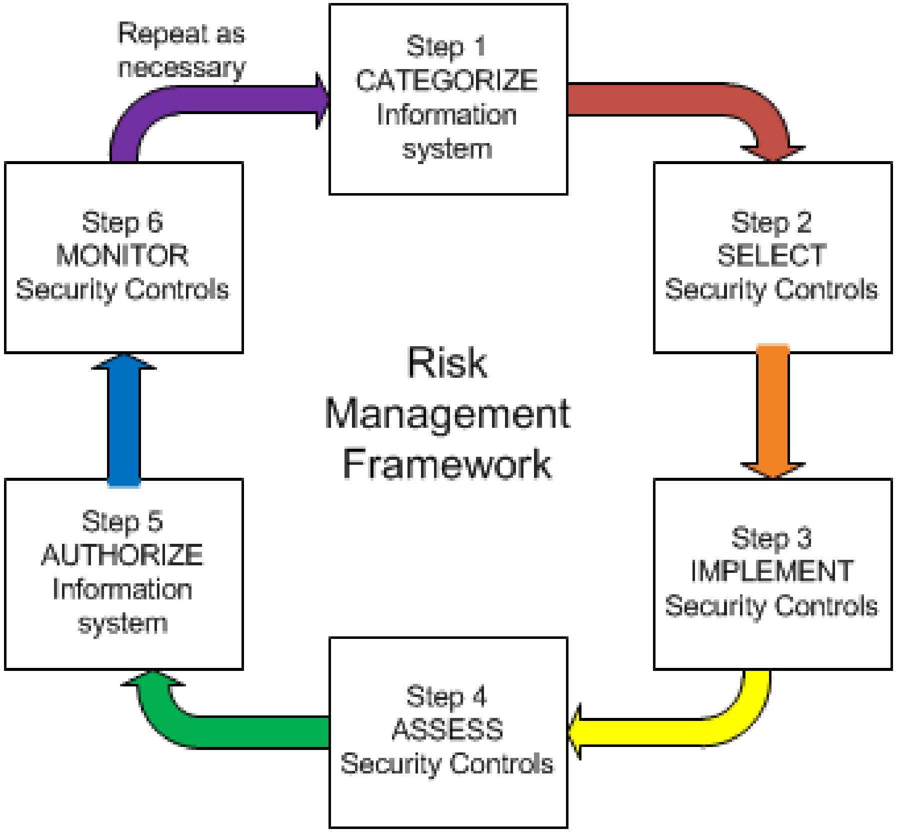
- Fiscal Service (FS) developed an “External Services” process to address security requirements for Services

Key points



- A Service is NOT a System
- Look BEFORE you leap
- Verify BEFORE you trust (or use)
  - Never trust and then verify

Remember the RMF



Repeat as necessary
Step 1 CATEGORIZE Information system
Step 2 SELECT Security Controls
Step 3 IMPLEMENT Security Controls
Step 4 ASSESS Security Controls
Step 5 AUTHORIZE Information system
Step 6 MONITOR Security Controls
Risk Management Framework

At Treasury, it is all about the money

$

Clarify

- Everything business units are doing that touches sensitive information not likely inside a “System” boundary
- With more pressure to reduce costs, more business functions are being outsourced
- Services can get into organizations under the radar bypassing Security unless Security is closely aligned with Procurement and Budget governance processes

A Service is NOT a System

Plain English simple definition :

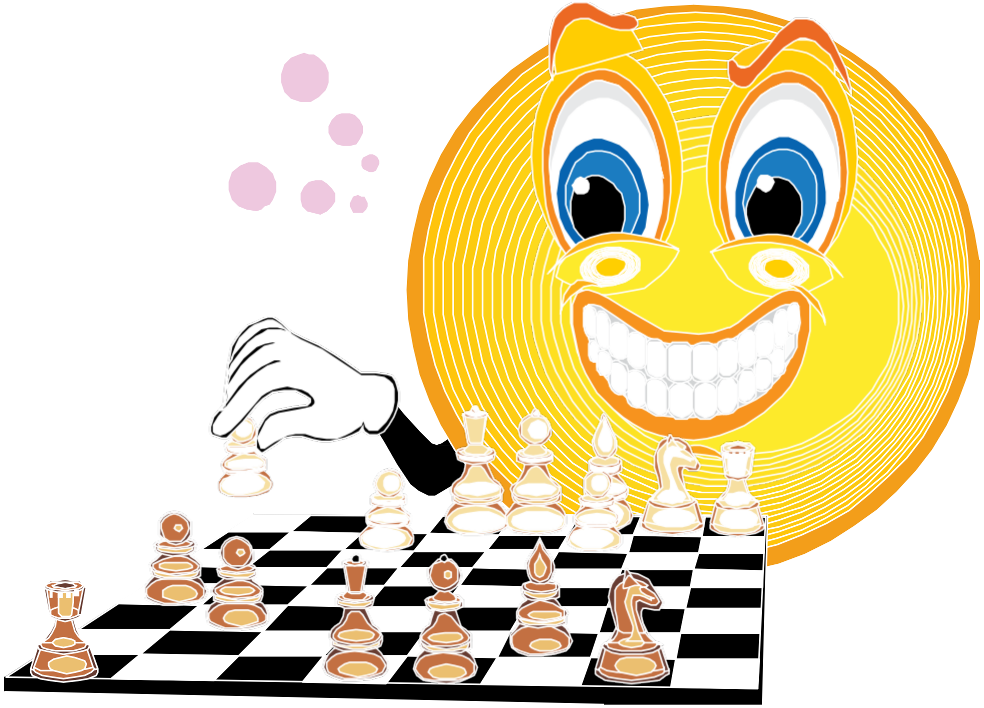
- Something owned & operated by somebody else
- Others are using it
- Readily available for acquisition
- Not customized for FS
- Not on the FISMA inventory

Services are

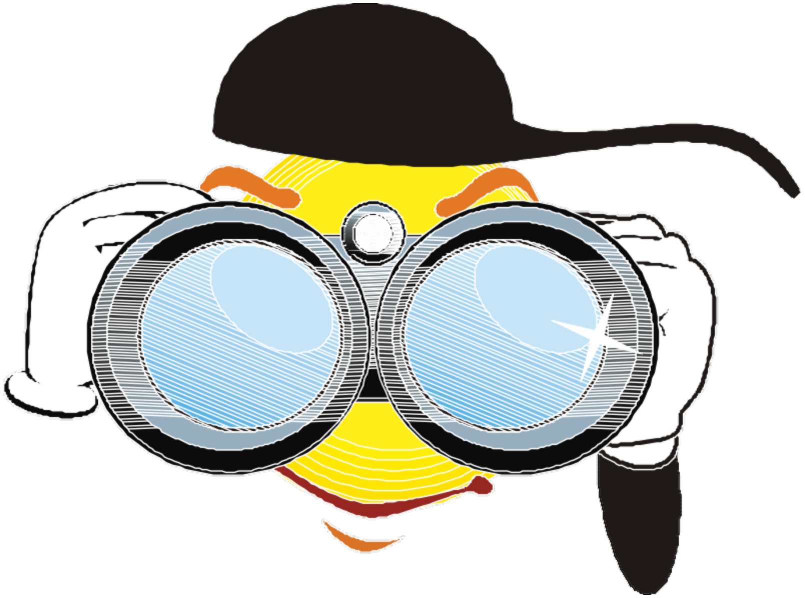
- An existing application or information processing service already used by the private sector and/or government that is operated by an external organization (private company, government organization, nonprofit organization, Federal Reserve, or financial institution)
- Readily available for acquisition and require no significant customization
- By definition, not FISMA systems

- For example: PayPal is a service

Planning



Look BEFORE you leap



Bad Risk Management

Good Risk Management

Use existing processes

- Security Impact Analysis (SIA)
- Classification Determination Memo (CDM)
- FedRAMP for cloud services
- Incorporate standardized security requirements language into Procurements
- Leverage existing third party assessments

Security Impact Analysis (SIA)

- A form
- A process
- Documents what doing now and what is planned
- Analyzes security impacts of the planned actions
- Assigns risk level to planned actions
- Prescribes work needed to manage risks

Classification Determination Memo (CDM)

- A form
- A process
- Documents what a (thing) is: system vs. service
- Describes what information is being processed

Service review process

Phase 1: Identify

- FIPS 199 categorization level of the information
- Classification and Determination Memo (CDM)
- Security Impact Analysis (SIA)

Phase 2: Assessment and Approval

- Define security requirements based upon CDM and SIA
- Review and document how the service meets those requirements & who responsible for which controls
- Assess the service and determine if risks are acceptable
- Obtain CIO approval that it’s acceptable to use the service

Clarify

ATU instead of ATO

An **external** organization owns and operates a service

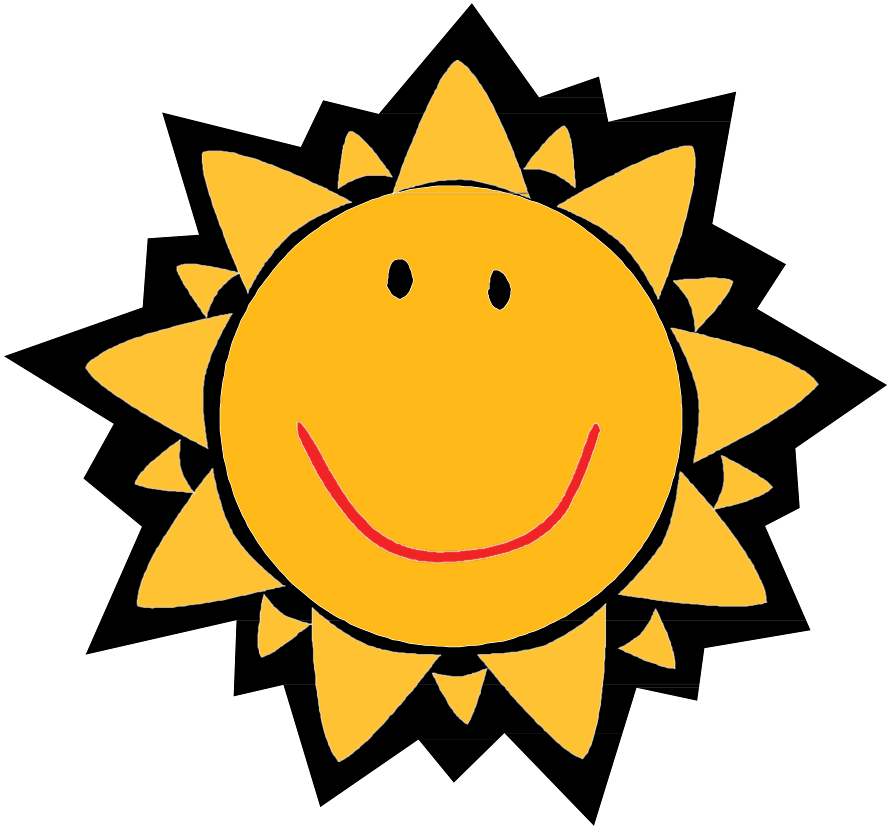
Instead of granting an Authorization to Operate (ATO), a service is approved as

Acceptable to Use (ATU)

$aving$

- Prevent bad procurements
- Avoid need to retrofit security controls
- Ensuring that security is included and working where needed (beyond the “Systems”), helps prevent costly security incidents and operational disruptions

Bright new day



Moving on

Contact Information

Jim McLaughlin, CISSP
Manager, Security Policy & Risk Management
304-480-6149
Jim.McLaughlin@fiscal.treasury.gov

Ralph Jones
Security Analyst
202-874-5057
Ralph.M.Jones@fiscal.treasury.gov