RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: STR-R01

“Cramming for FISMA”: How to Launch a NIST 800-53 Moderate System in 180 Days

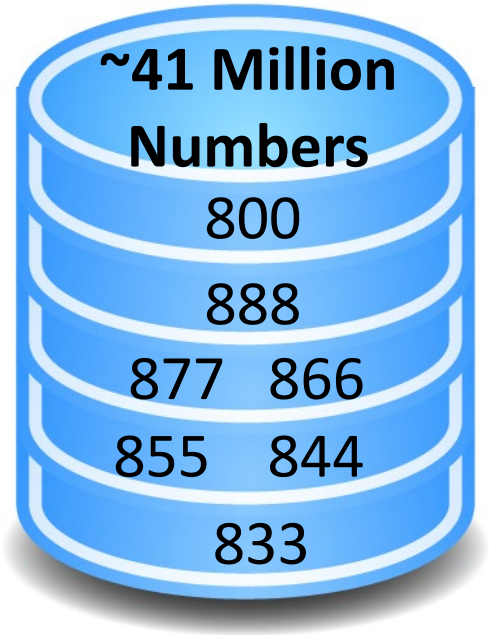
Johannes Wiklund

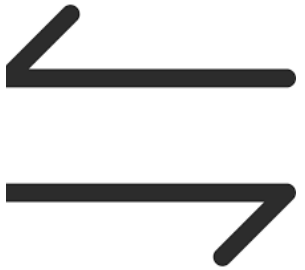
Vice President, IT & Cyber Security
Somos, Inc
Add me on LinkedIn: www.linkedin.com/in/wiklund
Follow me on Twitter: @WiklundUS

Back Story

- Somos is a leading provider of trusted, numbering and registry services – most well-known as the Toll-Free Number Neutral Administrator
- Over the past four years, Somos, in partnership with the FCC, has worked to modernize Toll-Free administration
- Largest Initiative – Achieved June 2019: Launch a high-performance, API driven Toll-Free Number Registry

7 Toll-Free Area Codes



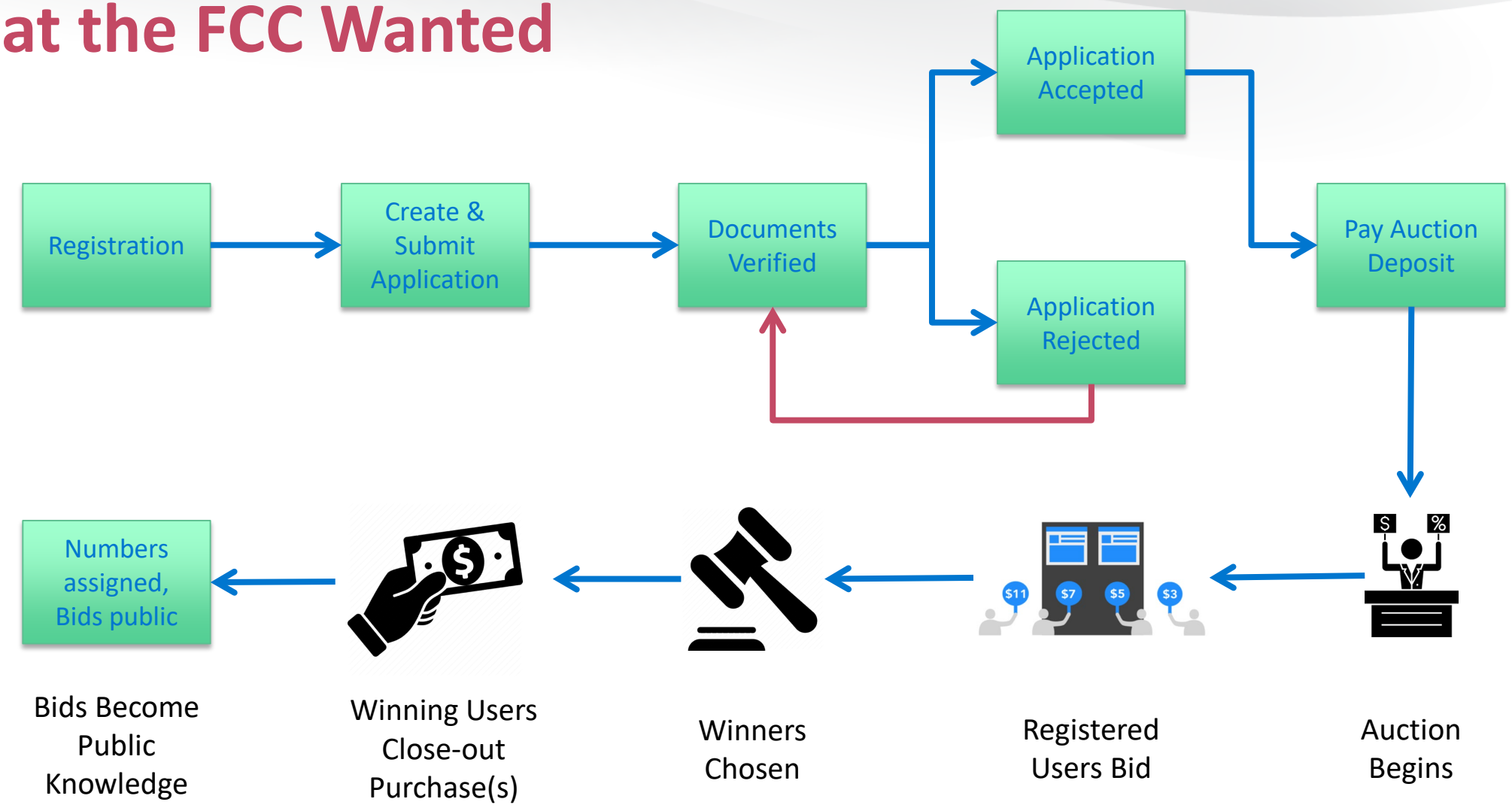


~1.3 Trillion Transactions
(as of Q4 2019)

Back Story

- To further modernize Toll-Free Number assignment, the FCC announced the use of an auction to distribute sought after Toll-Free Numbers in the 833-area code
- In support of the 833 Auction, Somos was tasked with providing a web-based platform that would host the auction
- The project required an aggressive schedule – 180 days – and strict requirements including FISMA compliance

What the FCC Wanted



System had to be FISMA Compliant

SOMOS®

What is FISMA Compliance?

FIPS 200

FIPS 199

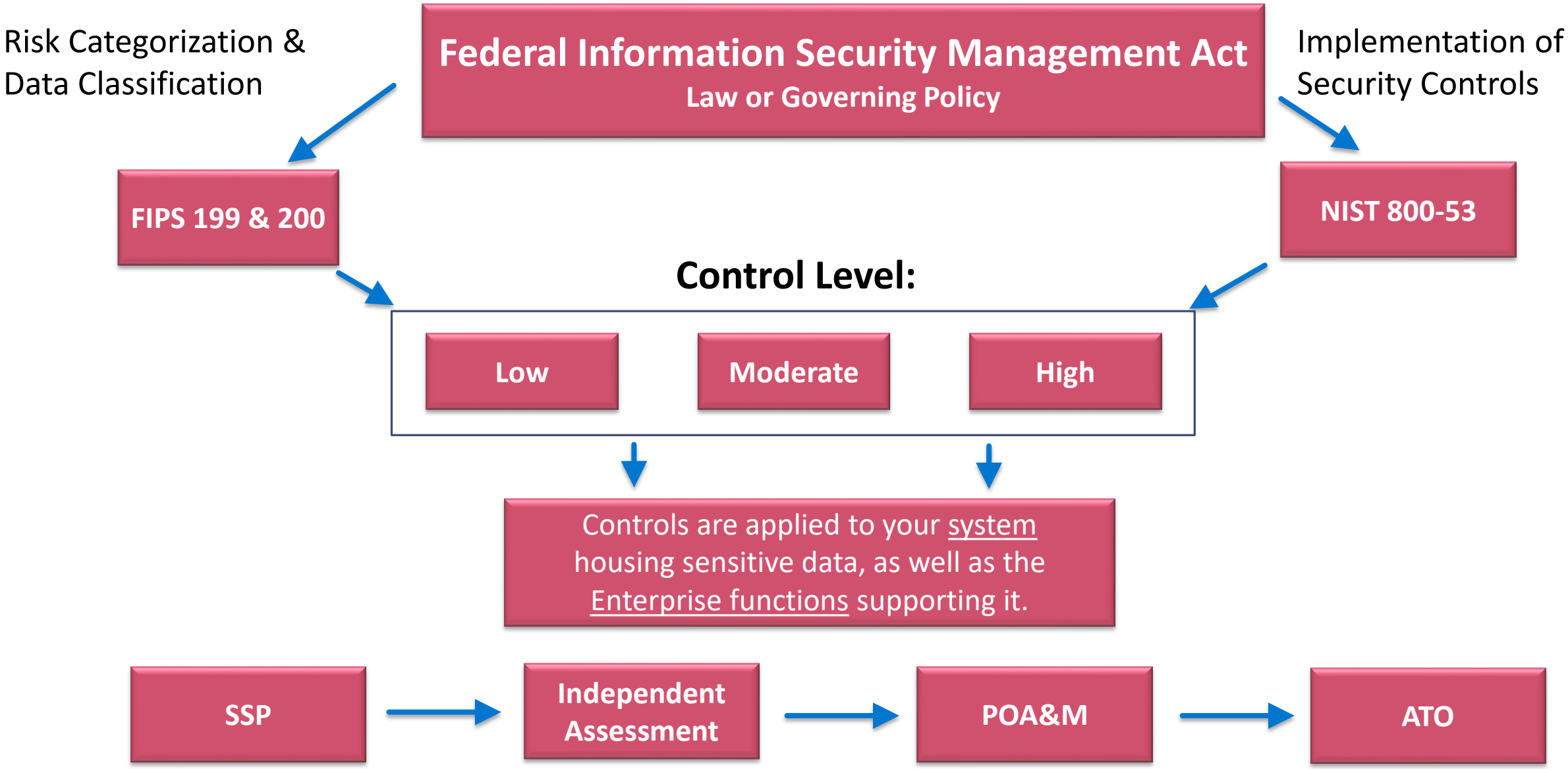
ATO

NIST 800-53

FedRAMP

POA&M

How we navigated the FISMA Process

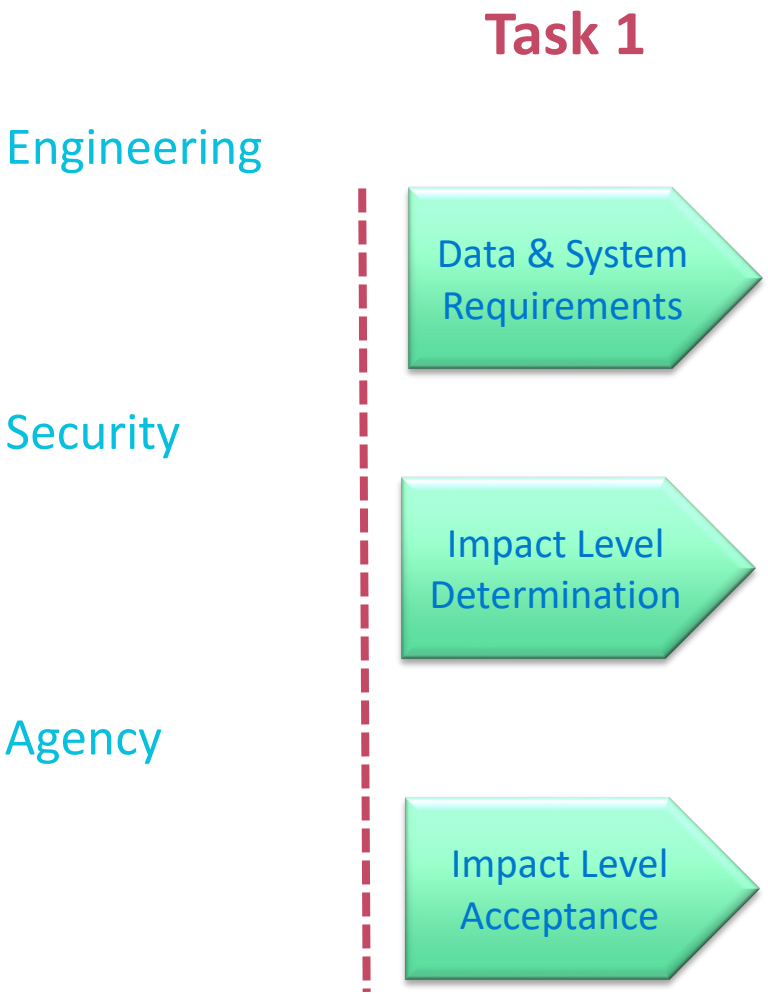


FISMA Compliance – Our Approach

RSAConference2020

AND NOW FOR THE DETAILS….
PLUS Actionable advice for each step

Task 1: Impact Level Determination



Task 1: Impact Level Determination

- Do Data Scoping Up Front!
- The sensitivity of the **Data** is the main driver for the classification of the system (Low, Moderate and High)
- Impacts the number of controls you have to implement

Task 1: Impact Level Determination Guidelines

- FIPS 199 and 200 are the guiding documents for impact determination
- System impact is based on a high watermark for:

Confidentiality **Integrity** **Availability**

Number of controls tested, by system impact level

Low	Moderate	High
124	261	343

Task 1: Impact Level Determination

Using FIPS-199/FIPS-200 as guidance, we determined that since the system will conduct an asset sale it should be assessed at the MODERATE level

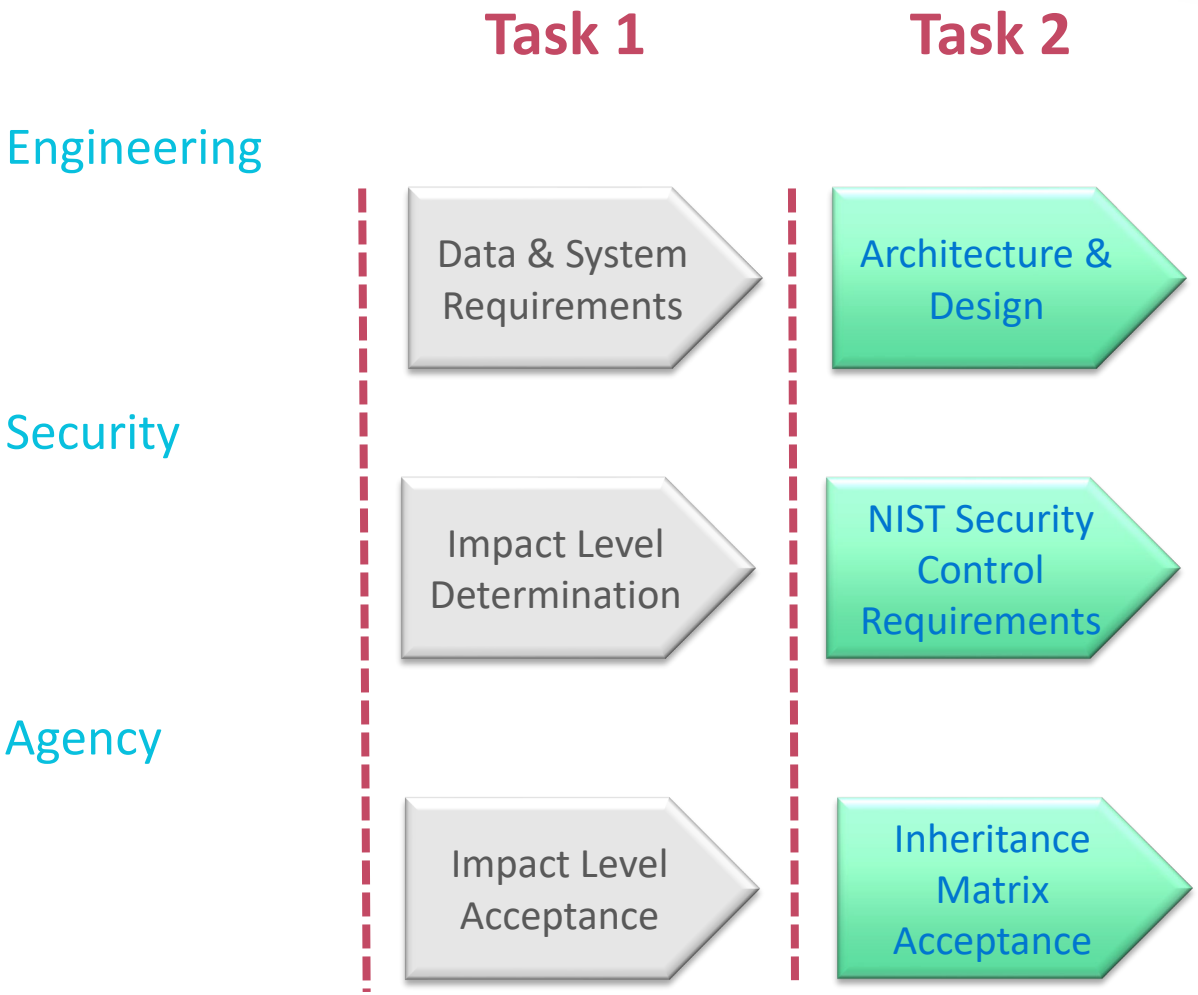
C.2.5.3 Federal Asset Sales Information Type

Federal Asset Sales encompasses the activities associated with the acquisition, oversight, tracking, and sale of non-internal assets managed by the Federal Government with a commercial value and sold to the private sector. The recommended security categorization for the Federal asset sales information type is as follows:

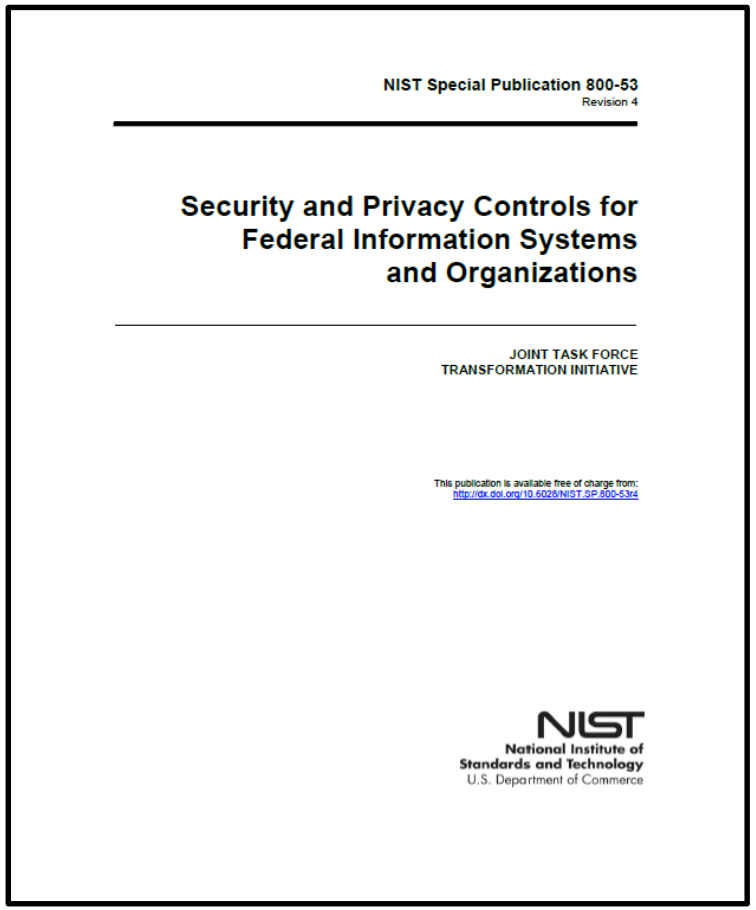
Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

Get your Agency's buy-in on the Classification!

Task 2: NIST Security Control Requirements



Task 2: NIST 800-53 Control Requirement Overview


NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

- Security and Privacy Controls for Federal Information Systems
- Fixed baseline of requirements for each impact level
- Requirements can be met in several ways:
  - Corporate Policy
  - Infrastructure
  - Software

Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Task 2: NIST Security Control Requirement Detail

- The controls are organized in Control Families.
  - Base controls are always required, including for low compliance level
  - Moderate and High compliance require control enhancements

AC-2 ACCOUNT MANAGEMENT

Family: AC - ACCESS CONTROL

Class:

Priority: P1 - Implement P1 security controls first.

Baseline Allocation:

Low	Moderate	High
AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)

Source: https://nvd.nist.gov/800-53/Rev4/control/AC-2

Task 2: Align Corporate Security Policy with NIST

- Your organization probably has a Security Policy
- It needs to be beefed up!
- Numerous supporting standards can be developed
- These need to apply Corporate Wide unless they are down-scoped to System Specific

Task 2: Infrastructure Impacts – The Case for Cloud

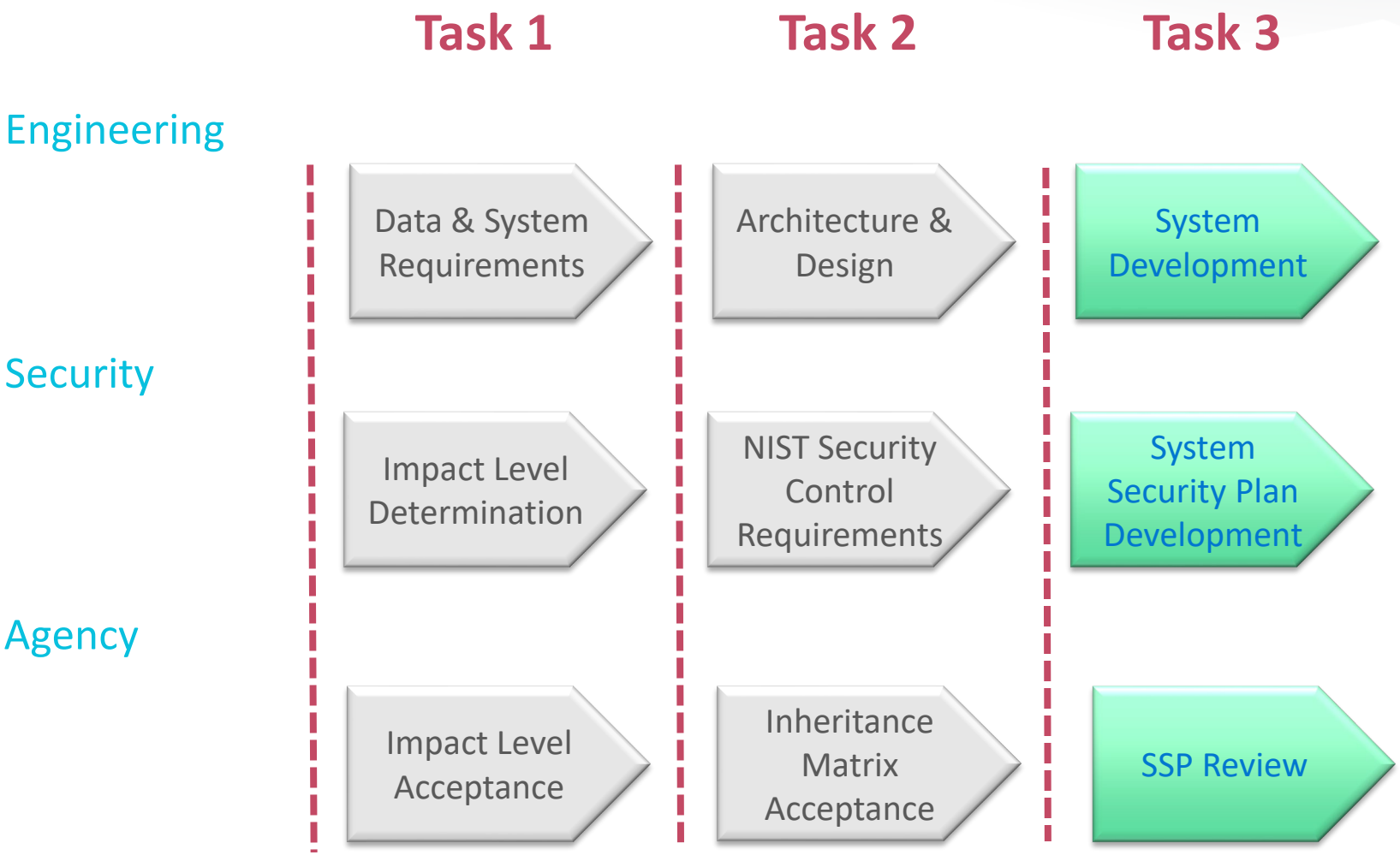
- Many of the NIST 800-53 requirements apply to the infrastructure used to host the application
- If you choose to use Public Cloud hosting, many of these controls are *inherited* from the FedRAMP certification of the Cloud Provider
- **PRO TIP: Check out the FedRAMP inheritance matrix from your cloud provider.** In our case almost 40% of the controls were either fully inherited from or shared with the Cloud Provider.

SOMOS®

Task 2: Software Architecture and Design Impacts

- Many NIST requirements must be designed and built into the system itself
- **PRO TIP**: Designate a Security Champion to be part of the Scrum team
- Role is to ensure Secure by Design principles are followed

Task 3: System Security Plan Development

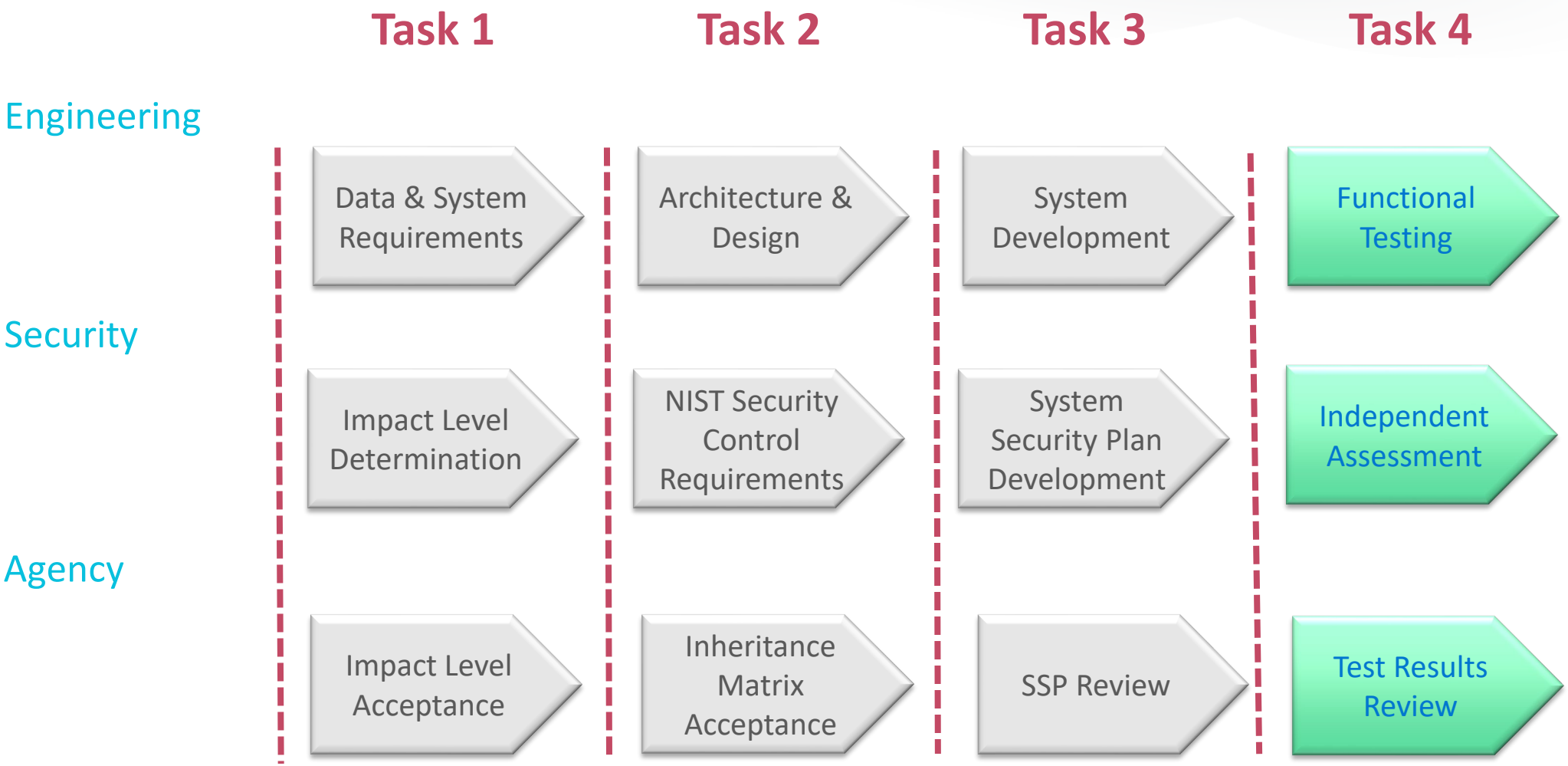


Task 3: System Security Plan Development

- The System Security Plan (SSP) is the key document
- Ours was 440 pages!
- It explained **in detail** how each NIST 800-53 requirement is met, whether it's a corporate, infrastructure or system specific control

PRO TIP: Ensure you have sufficient resources. If you don't, be prepared to get help from a consultant!

Task 4: Independent Assessment



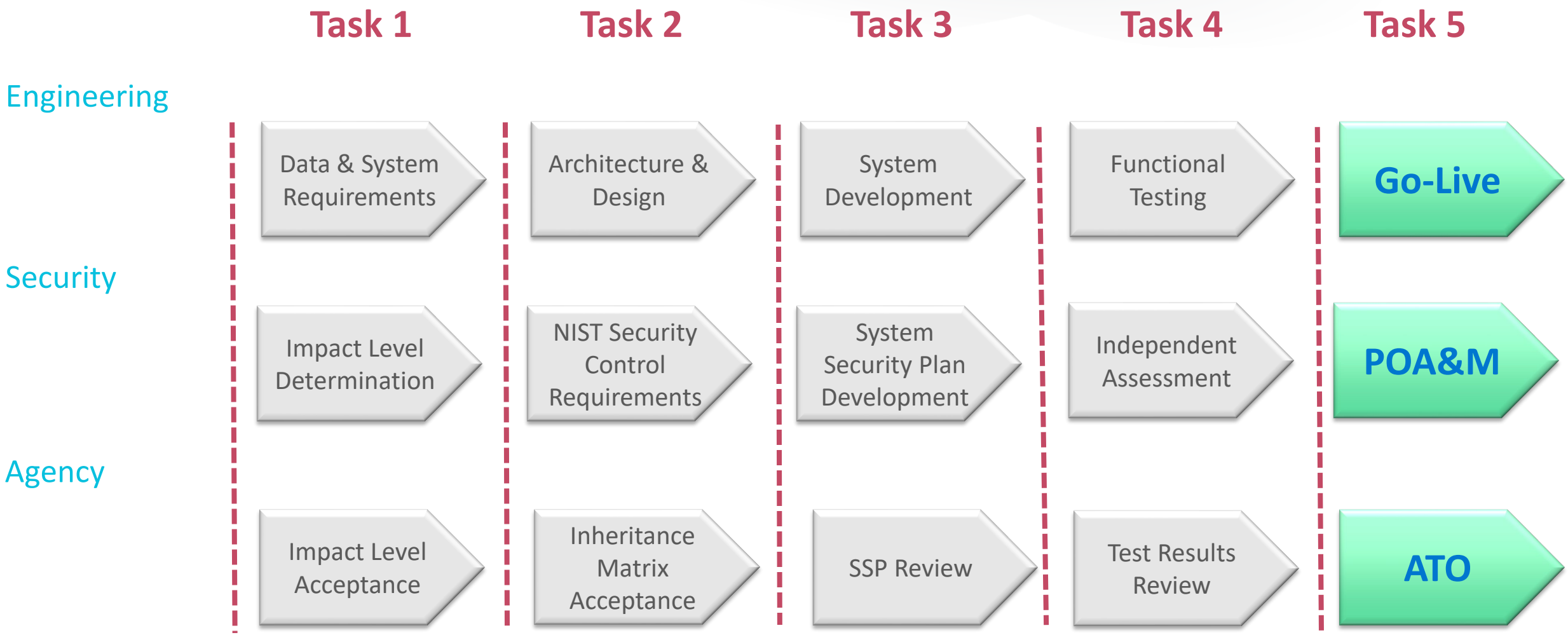
Task 4: Independent Assessment

- An independent assessment is required
- For FedRAMP an authorized 3PAO (Third-Party Assessment Organization) is required. For FISMA, an experienced third-party will suffice.
- The assessor is going to review **every control**
- **Plus** they will perform a Penetration Test

Task 4: Independent Assessment Results

- The main deliverable is a **Risk Exposure Table**
- This document summarizes where controls were weak, failed, or insufficient evidence was provided
- Your company needs to determine if you can *mitigate or accept* the residual risk
- Any mitigations become part of your Plan of Action & Milestones (POA&M)

Task 5: POA&M and ATO – Authority to Operate



Task 5: POA&M and ATO – Authority to Operate

- Accepting the POA&M paves the way for issuing the ATO
- Agency Partnership is critical: We worked with the FCC CISO and Privacy Counsel
- In our case, they wanted Somos to issue the ATO since it was our system and we should accept the residual risk
- Continuous Monitoring – Follow-ups of the POA&M start now!

RSAConference2020

LESSONS LEARNED
PLUS How to apply them to your own organization

Overcoming Challenges

- Learning the language
  - Vocabulary and guidelines can be understood – you need to spend the time to understand it for yourself
- System Impact Assessment: Ensure you get it right
  - Minimize PII and other sensitive data if possible. Check for approval.
- Authorization Boundary
  - Don’t bite off more than you can chew in your first assessment. For example, we kept laptops used to develop code out of scope.
- Corporate vs. System Specific Controls
  - Be realistic when setting expectations. Don’t set yourself up for failure by setting unrealistic goals.

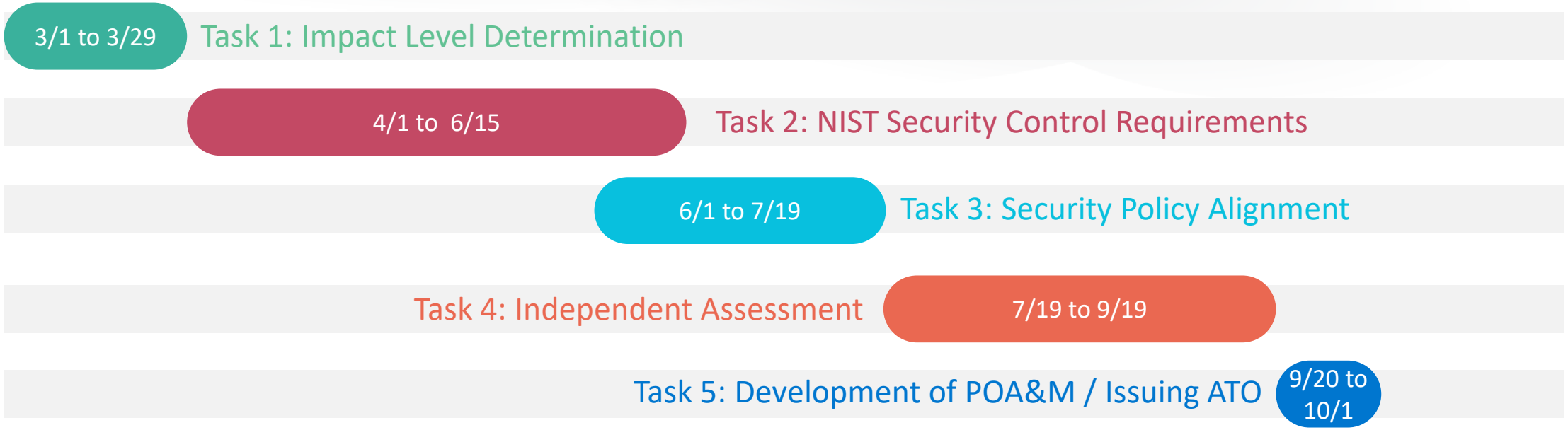
Staffing for Success

- Designate a “Security Champion” who can participate in SCRUM meetings and get other team members up-to-date on FISMA
  - Ideal candidate will have prior experience with FISMA or NIST
- Designate a “Data Collector” during the assessment
  - Assessor will ask for evidence for each control
  - Ensure you have screen shots, change logs and other artifacts

Our Secret Sauce

- Highly engaged Project Sponsor
- Executive Commitment
- Full-time above-and-beyond commitment of staff
- Negotiation skills

How We Did It in 180 days



RSAConference2020

QUESTIONS?