JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

A Short History of the NIST RMF

Gary Stoneburner
Gary.Stoneburner@jhuapl.edu

Brief History of NIST Risk Management Framework (RMF)

- And then there was congress:

  Federal Information Security Management Act (FISMA) 2002

    NIST “shall …[provide guidance for] minimum information security requirements … no later than 36 months”

Brief Chronological History of the “RMF”

SP 800-30 Risk Management (2002)

Risk through IT, not to IT

SP 800-30 Rev 1 Risk Assess (2012)

Determine risk (part of original 800-30)

SP 800-53 Security Controls (2005)

RM is (RMF) and is part of control selection process

SP 800-37 Rev 1 Applying the RMF (2010)

RMF has its own home

SP 800-39 Risk Management (2011)

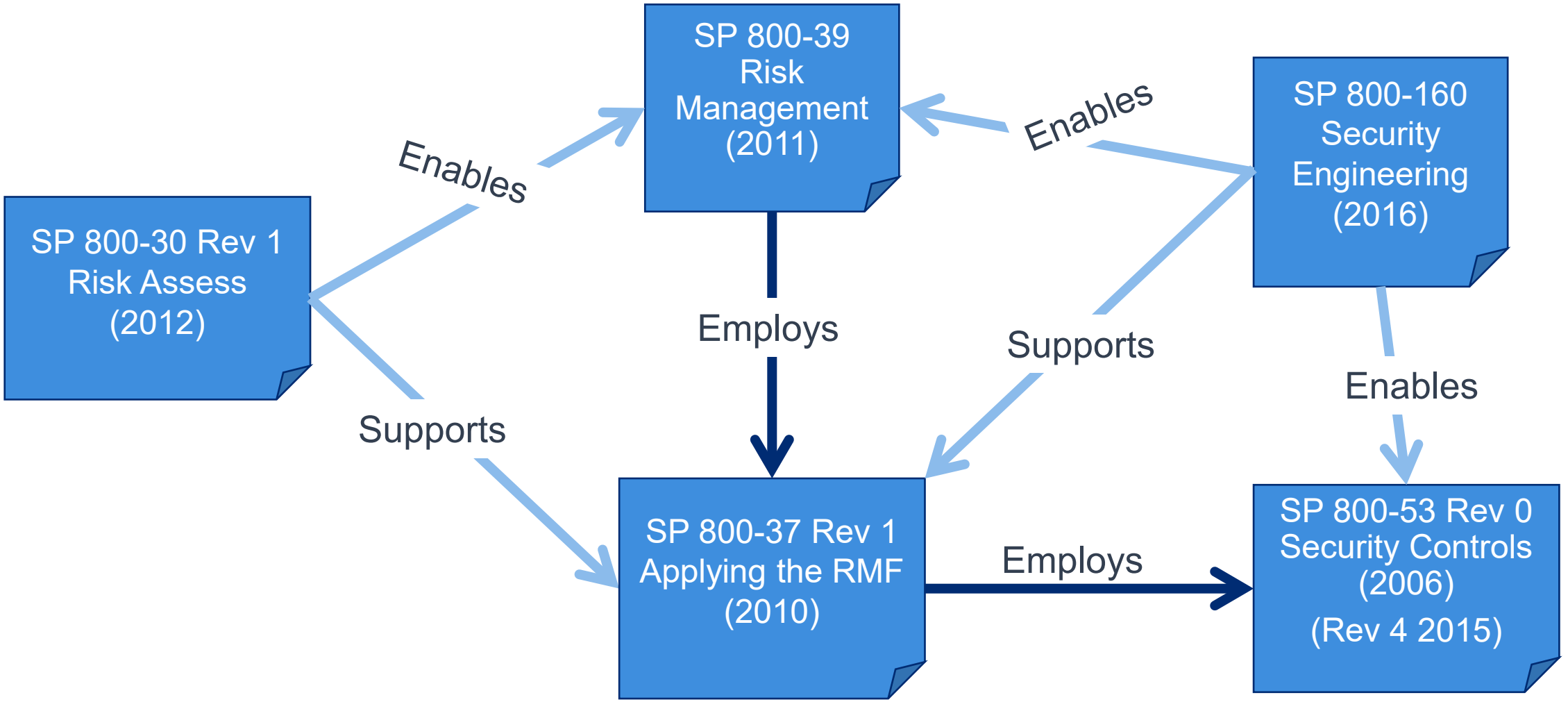
RMF now system level of 3 level RM

SP 800-160 Security Engineering (2016)

Engineering for security

RMF - Risk Management Framework
RM – Risk Management

“RMF” – Inter-Relationship of NIST Guidance



RMF – NIST Controls, What they really are

AU-4 Audit Storage Capacity The organization:

Allocates audit record storage capacity in accordance with [_____].

AU-5 Response to Audit Processing Failures The information system:

a. Alerts [_____] in the event of an audit processing failure; and

b. Takes the following additional actions: [_____].

- NIST controls are purposefully ***incomplete***
  - Blanks, multiple choice, and
  - NIST explicitly states may need to change text to "*fully define the intent*"

The controls are ***template*** text intended for use in expressing ***derived*** requirements

Reality Check – NIST Control Baselines

- **NOT** levels of security capability (even if you were told how to complete the purposefully incomplete NIST controls)
- Starting point **alternative to a blank page**
- "***starting point*** *in determining the security controls*" to be *tailored* –
  - scoped ("*eliminate unnecessary*"),
  - compensated ("*alternatives*"),
  - supplemented (add controls to *sufficiently mitigate risks to organizations, individuals, and the Nation*) and
  - Completed (blanks, multiple choice, and changes to control text)

Need - Capability engineering to achieve mission need (Not a set of controls)

From SP 800-160 (NIST's System Security Engineering (SSE) guidance

1. "… ***security objectives*** *are foundational in that they establish and scope what it means to be adequately secure*"
2. *"Protection needs are determined based on the security objectives, life cycle concepts, and stakeholder concerns [and] subsequently transformed into* ***stakeholder security requirements****"*
3. *"… transforms the stakeholder security requirements into the* ***system requirements*** *that reflect a technical security view of the system"*
4. *"… generate system* ***architecture*** *alternatives, to select one or more alternative(s) that frame stakeholder concerns and meet system requirements, and to express this in a set of consistent views."*

Security Controls about here

Bottom line - Engineering required

"… *today's systems have dimensions and an inherent complexity that* ***require a disciplined and structured engineering approach*** *to achieve any expectation that the inherent complexity can be effectively managed*"

Quotes from SP 800-160 [emphasis added]

Engineering: Expertise and experience to capture complex system requirements without expectation of pre-defined, answers-in-policy