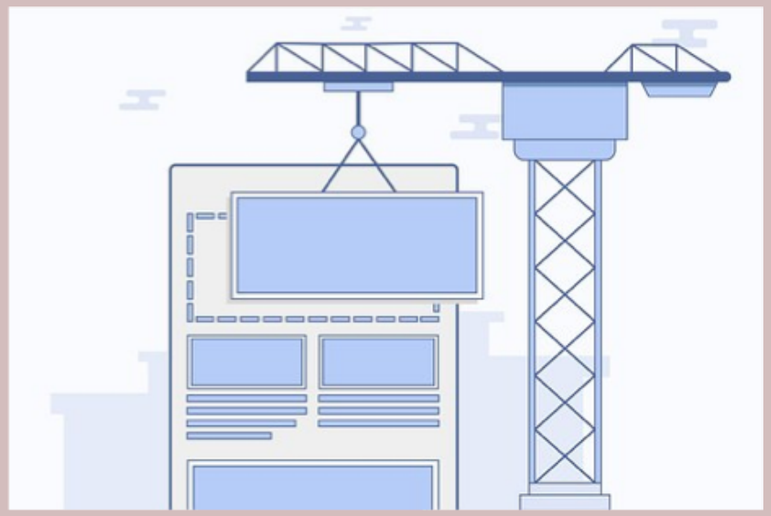
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Standard Frameworks

Security Architecture & Tool Sets

Standard Frameworks

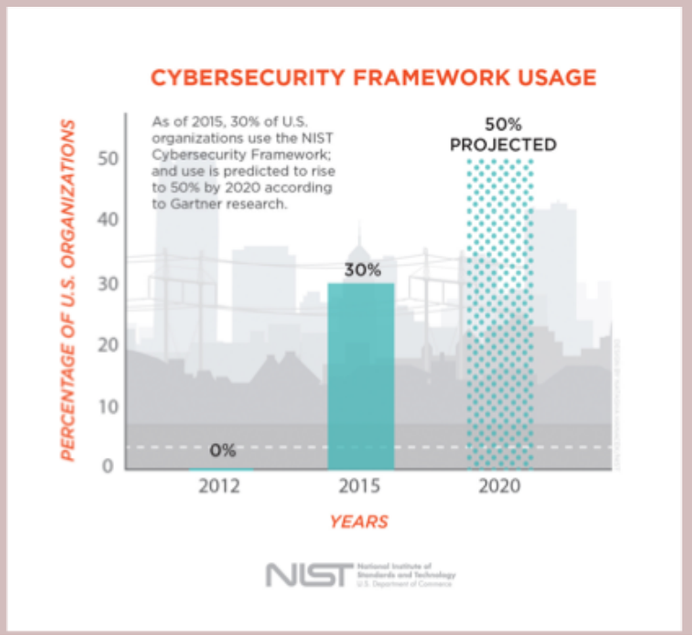
- Creating your own cybersecurity program is daunting task
- Standard frameworks exist to help
- Provide a standardized approach



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

NIST Cybersecurity Framework

- Designed to meet one or more objective
  1. Describe current posture
  2. Describe desired state
  3. Identify and prioritize areas for improvement
  4. Assess progress toward desired state
  5. Communicate risk among internal and external stakeholders



NIST Cybersecurity Framework

- Framework Core is a set of five security functions that apply to all industries
- Framework Implementation Tiers measure how the organization is positioned to meet cybersecurity objectives
- Framework Profiles describe how the organization might approach the functions covered by Framework Core

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

ISO 27001

- Used to be the most commonly used information security standard
- Declining in usage outside of regulated companies that require ISO compliance
- To become ISO 27001 certified, an external accessor validates organizational compliance

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

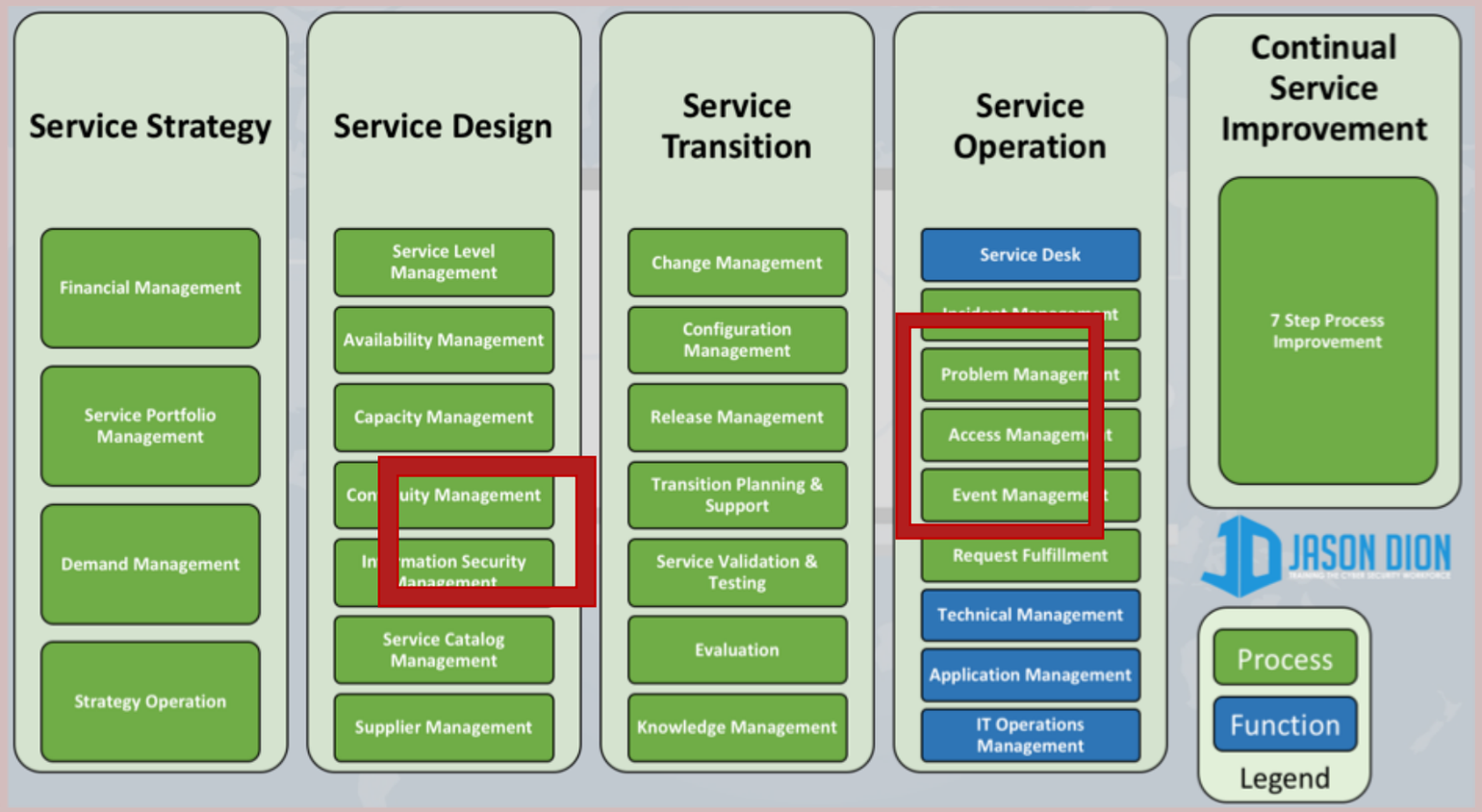
ISO 27001: 14 Categories

- Information Security Policies
- Organization of Information Security
- Human Resource Strategy
- Asset Management
- Access Control
- Cryptography
- Physical and Environment Security
- Communications Security
- System Acquisition
- Information Security Incident Management
- Information Security Aspects of Business Continuity
- Compliance with internal requirements

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Information Technology Infrastructure Library (ITIL)

- Comprehensive approach to ITSM



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

COBIT

- Control Objectives for Information & Related Technologies
- Set of best practices for IT governance developed by ISACA
- Divides IT activities into four domains:
  - Plan and Organize
  - Acquire and Implement
  - Deliver and Support
  - Monitor and Evaluate

COBIT Framework Components

- COBIT framework
- Process descriptions
- Control objectives
- Management guidelines
- Maturity models

COBIT® 5

AN ISACA® FRAMEWORK

JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

The Open Group Architecture Framework (TOGAF)

- Widely adopted approach to EA

- Four domains:
  - Business Architecture
    - Integrates EA with business strategy
  - Application Architecture
    - Contains apps/systems used, interaction between systems, and the relation to the business processes
  - Data Architecture
    - Details approach to storing and managing info assets
  - Technical Architecture
    - Details infrastructure needed to support other domains

Sherwood Applied Business Security Architecture (SABSA)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

- Alternative model for security architecture that maps to architectural layers from different perspectives

- Used in Enterprise Architecture (EA)

View	Architecture Layer
Business	Contextual Security
Architect	Conceptual Security
Designer	Logical Security
Builder	Physical Security
Tradesman	Component Security
Service Manager	Security Service Management