My great-grandmother's secret sauce: Your guide to CMMC, HITRUST, NIST and everything in between

Matt Morton

Senior Strategic Consultant

Vantage Technology Consulting Group

VANTAGE
Technology Consulting Group

What is a recipe?

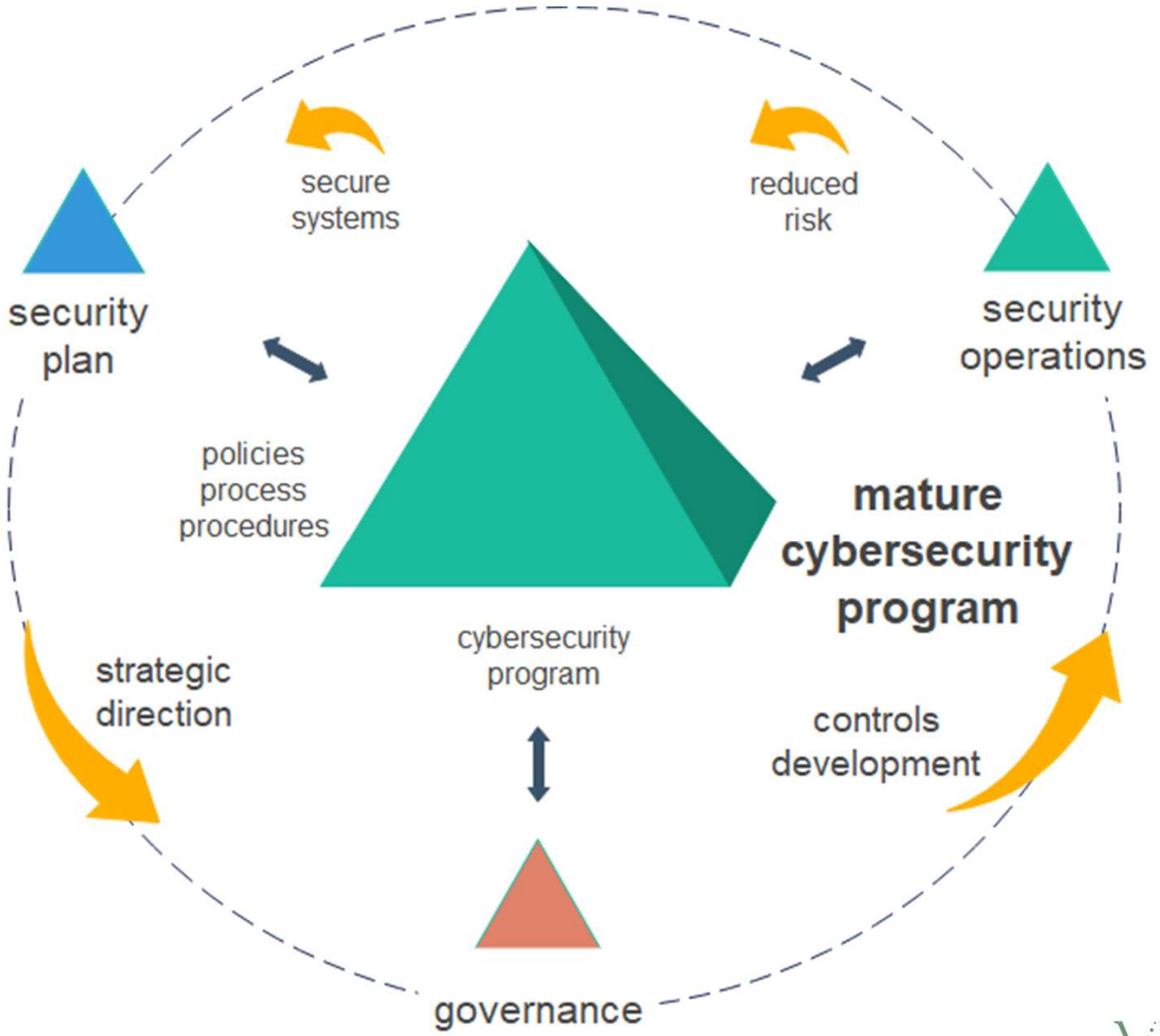
- Ingredients List
- Ingredient amounts
- Preparation Instructions

VANTAGE
Technology Consulting Group

Why are we doing this?

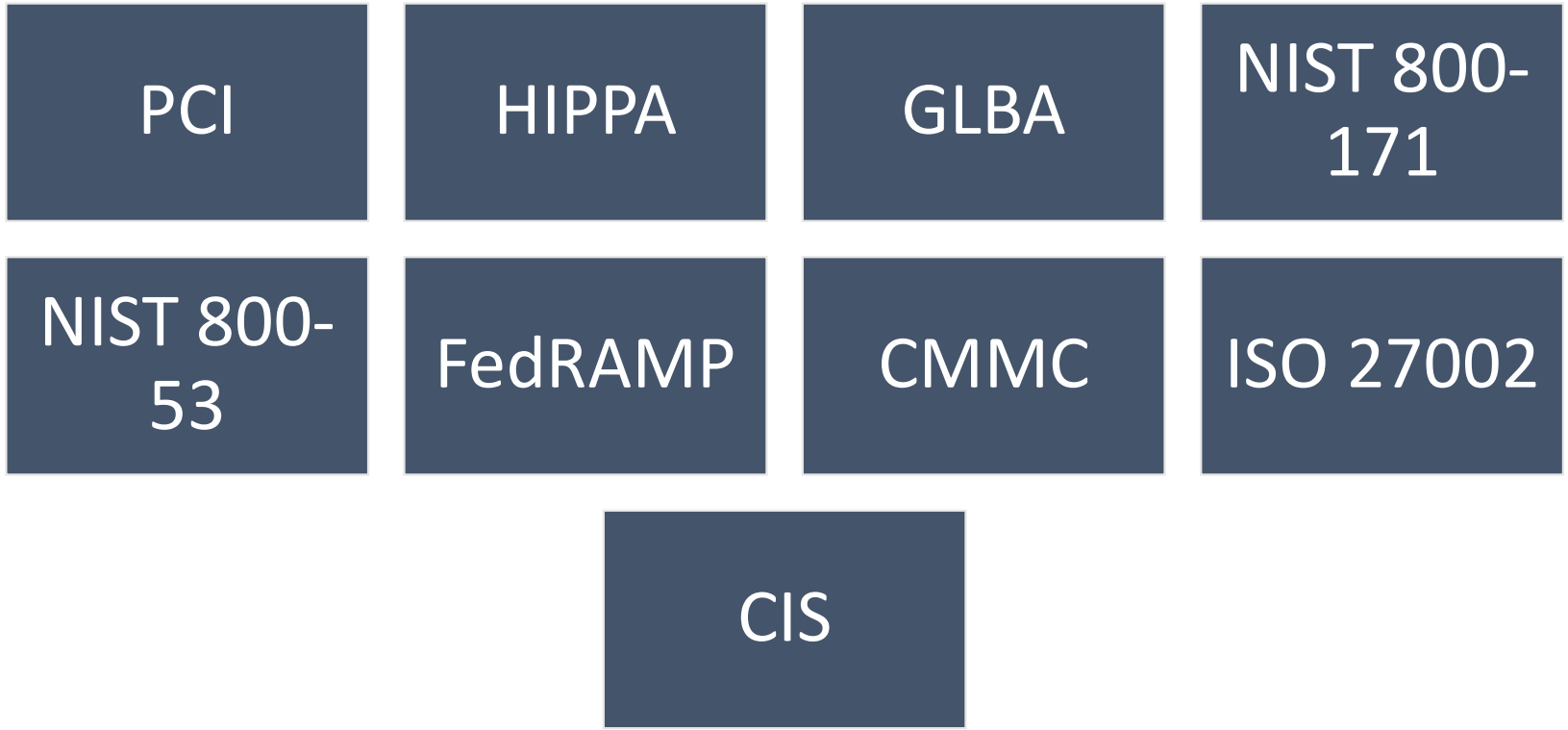
- Breaches
- Risk
- Cybercrime
- Intellectual Property Theft

Aspects



VANTAGE
Technology Consulting Group

Multiple Standards



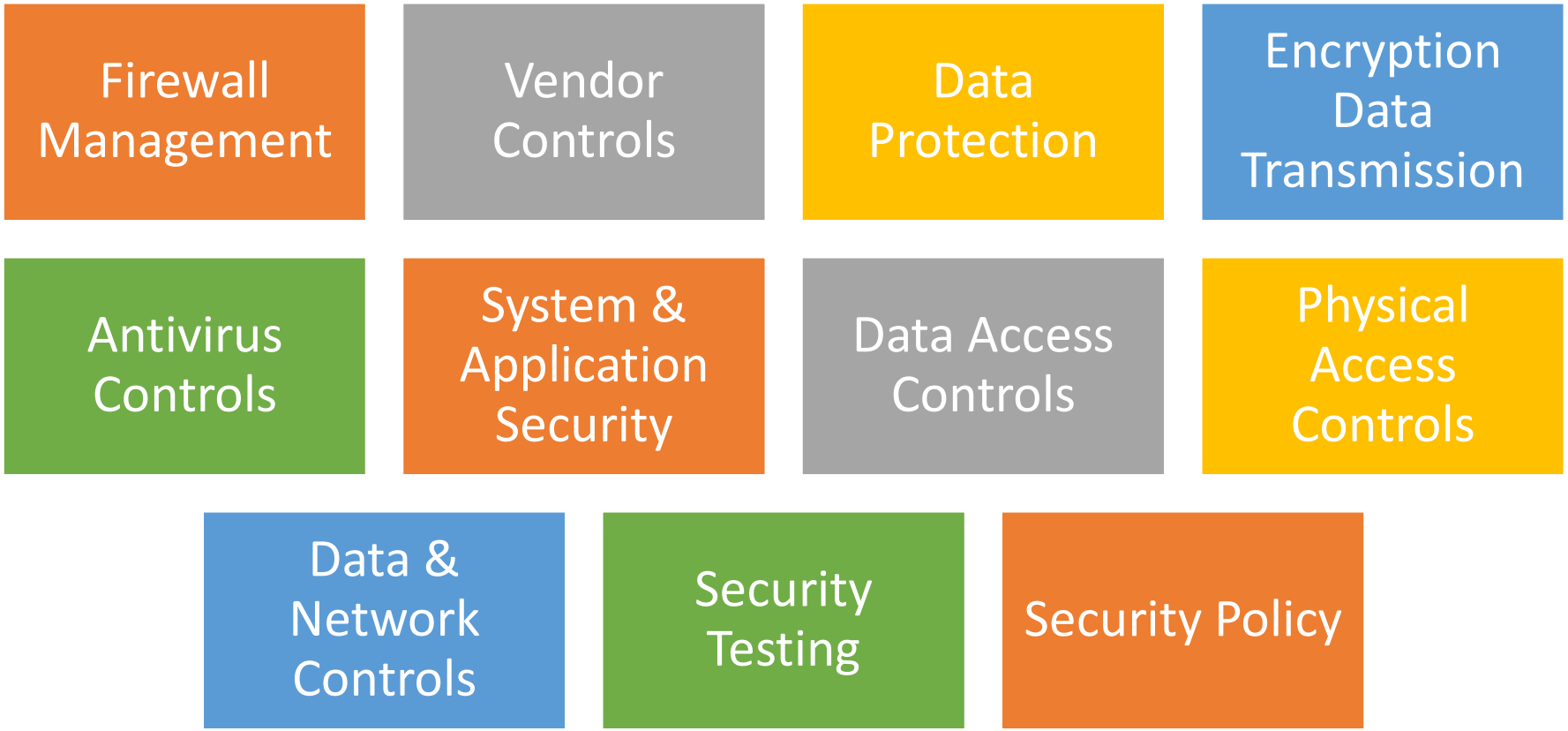
VANTAGE
Technology Consulting Group

PCI DSS

- PCI Compliance

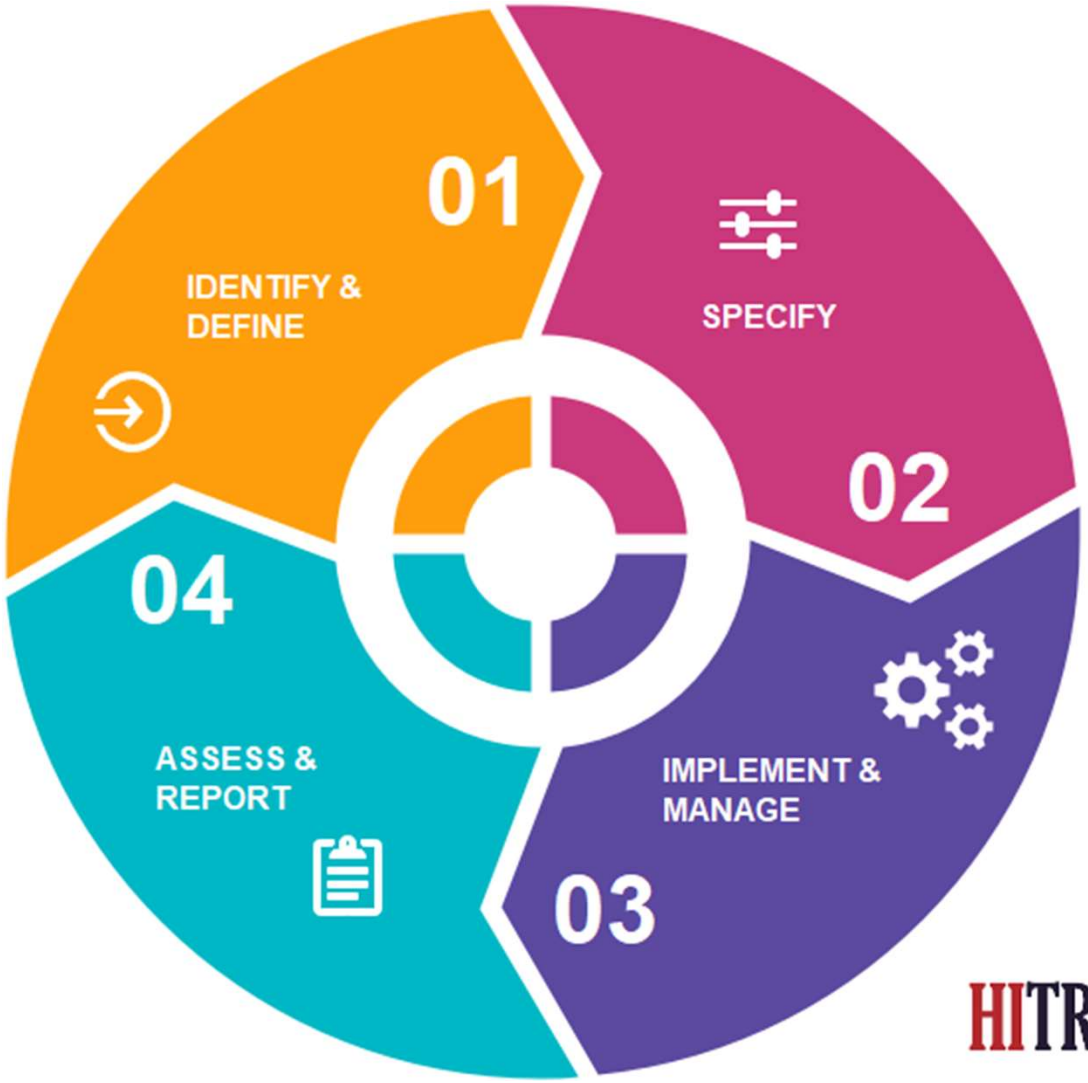
VANTAGE
Technology Consulting Group

PCI DSS



VANTAGE
Technology Consulting Group

HITRUST



VANTAGE
Technology Consulting Group

HITRUST

VANTAGE
Technology Consulting Group

FedRAMP

- Government cyber security risk management program for the purchase and use of cloud products and services used by U.S. federal agencies.
- Requires
  - Completion of FedRAMP documentation
  - FedRAMP SSP
- Controls comply with FIPS 199
- Commercial cloud offerings by FedRAMP Third Party Assessment Organization (3PAO) – see CMMC
- Development of a Plan of Action and Milestones (POA&M)
- Obtain Joint Authorization Board (JAB) Provisional ATO (P-ATO) or Agency ATO
- Implementation of a Continuous Monitoring (ConMon) program including monthly vulnerability scans.
- Typically is NIST 800-53 moderate

GLBA

- Graham Leach Bliley Act
- Section 501 of the GLBA, “Protection of Nonpublic Personal Information,” requires financial institutions to establish appropriate standards related to the administrative, technical, and physical safeguards of customer records and information.
- Ensure the security and confidentiality of customer data
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such data
- Protect against unauthorized access to, or use of, such data that would result in substantial harm or inconvenience to any customer
- FFEIC
- Encryption strength sufficient to protect the information from disclosure until such time as disclosure poses no material risk
- Effective key management practices
- Robust reliability
- Appropriate protection of the encrypted communication’s endpoints

NIST 800-171

Federal Government relies heavily on contractors and external service providers to carry out missions.

Data is flowing between federal and non-federal systems.

Frequently shared with State and local governments.

Was created to address several shortcomings in current standards in protecting CUI

Outlines the controls necessary from the federal governments perspective to control the data that is entrusted to its partners.

Required to do business with federal systems.

VANTAGE
Technology Consulting Group

What is NIST 800-171?

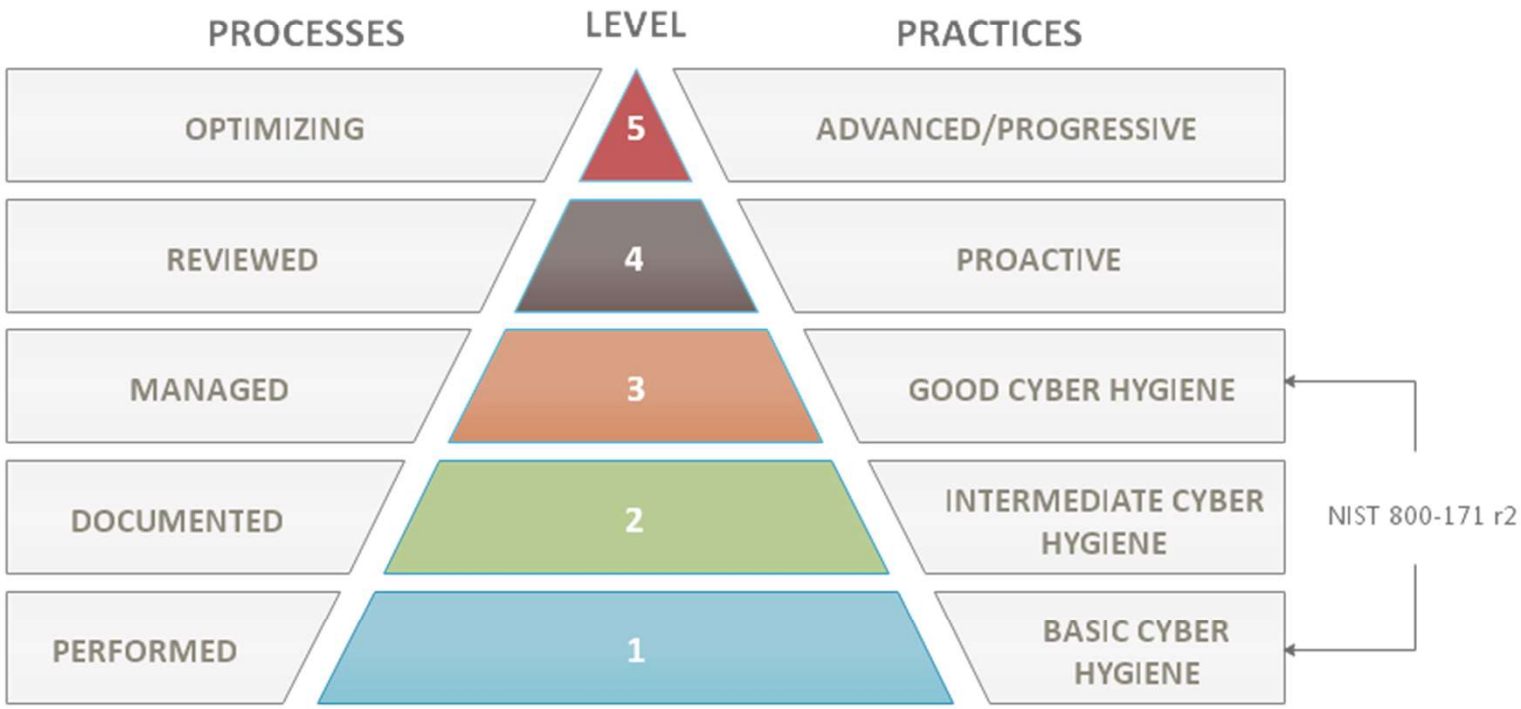
- In place to protect “Controlled Unclassified Information” (CUI)
- Derived NIST SP 800-53 security controls
- Standardizes “derived” requirements
- 14 Security requirement families
- “Makes NIST 800-53 easier”
- Based upon NIST Cybersecurity Framework
- Contractors must be compliant by December 31, 2017
- Self Verified
- DFARS 252.204-7012
  - nine (9) months (from the date of contract award or modification incorporating the new clause(s)) to satisfy the requirement for “multifactor authentication for local and network access” found in Section 3.5.3

CMMC

- CMMC stands for “Cybersecurity Maturity Model Certification”
- Provides increased assurance that a DIB company can adequately protect sensitive unclassified information, accounting for information flow down to subcontractors in a multi-tier supply chain.
- CMMC Level 3 includes the 110 security requirements specified in NIST SP 800-171. The CMMC Model also incorporates additional practices and processes from other standards, references, and/or sources such as NIST SP 800-53, Aerospace Industries Association (AIA) National Aerospace Standard (NAS) 9933 “Critical Security Controls for Effective Capability in Cyber Defense”, and Computer Emergency Response Team (CERT) Resilience Management Model (RMM).

https://www.acq.osd.mil/cmmc/

CMMC



VANTAGE
Technology Consulting Group

CIS Controls™

Version 7: a prioritized set of actions to protect your organization and data from known cyber attack vectors.

CIS Controls V7 separates the controls into three distinct categories:

Basic:
Key controls which should be implemented in every organization for essential cyber defense readiness.

Foundational:
Technical best practices provide clear security benefits and are a smart move for any organization to implement.

Organizational:
These controls are more focused on people and processes involved in cybersecurity.

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

CIS Controls™

	FAMILY	ID	FAMILY
	Access Control	MP	Media Protection
	Awareness and Training	PE	Physical and Environmental Protection
	Audit and Accountability	PL	Planning
	Security Assessment and Authorization	PS	Personnel Security
	Configuration Management	RA	Risk Assessment
	Contingency Planning	SA	System and Services Acquisition
	Identification and Authentication	SC	System and Communications Protection
	Incident Response	SI	System and Information Integrity
	Maintenance	PM	Program Management

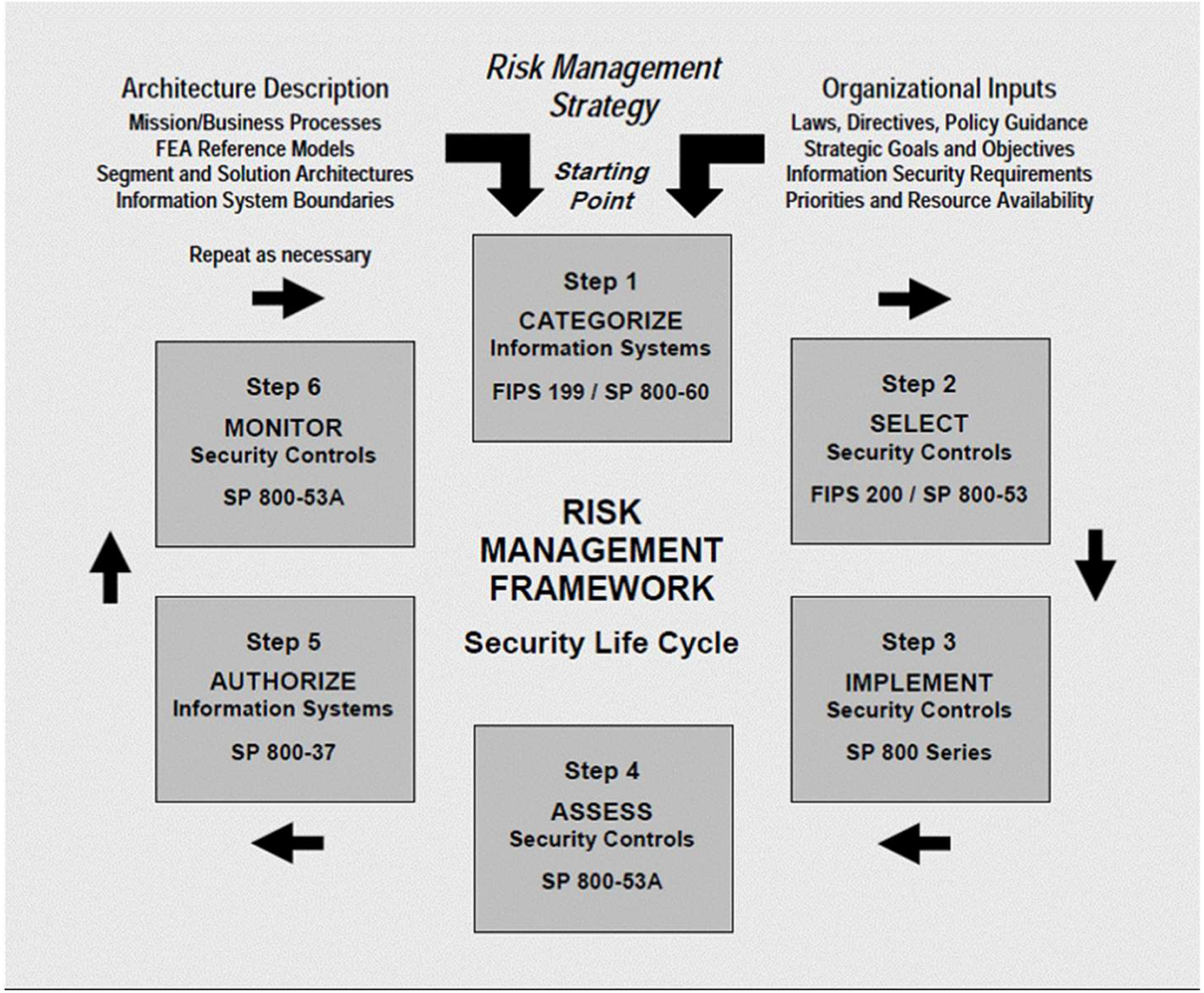
NIST 800-53

- https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Several Frameworks

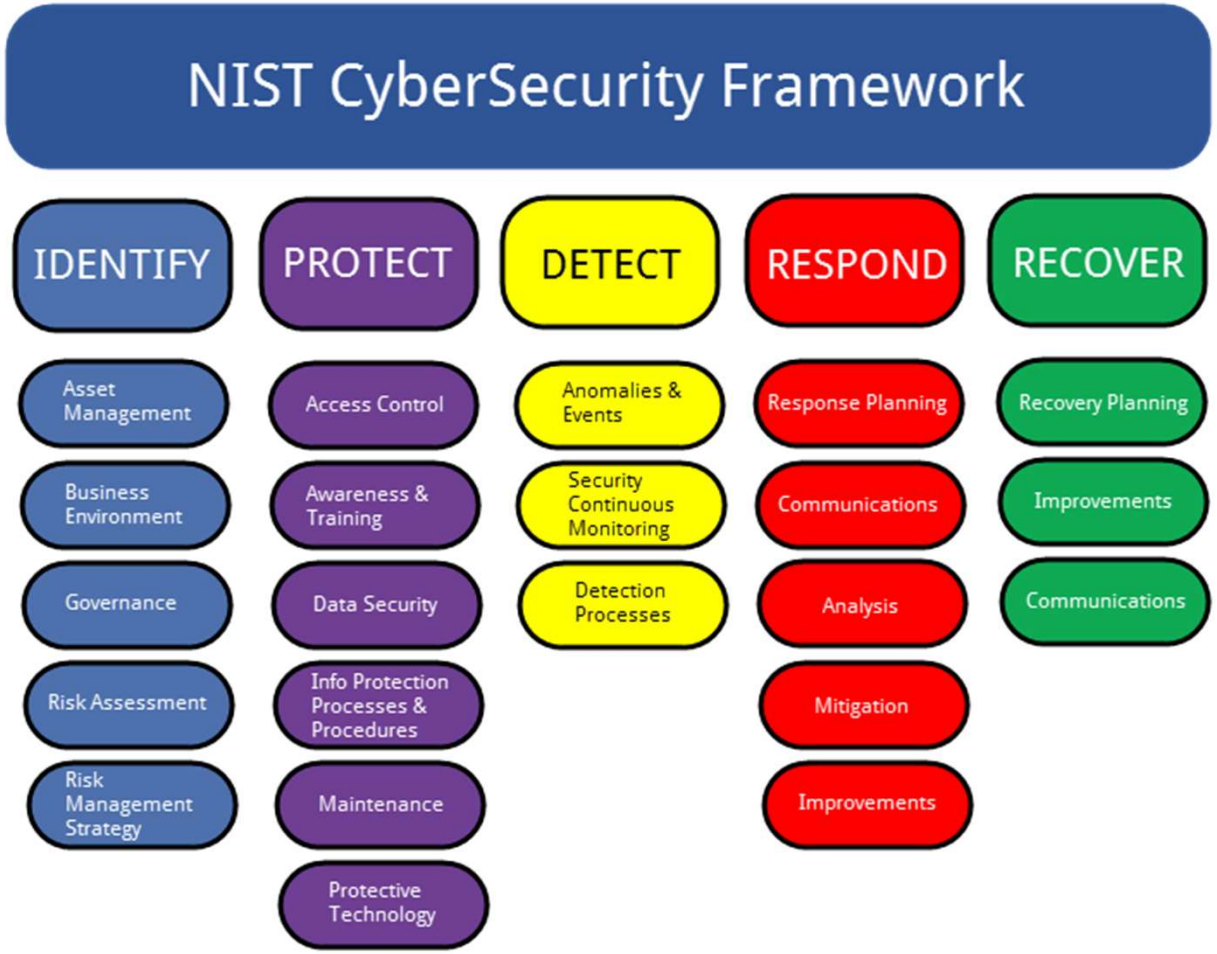
- NIST CSF
- NIST RMF
- ISO 27001

NIST Risk Management Framework



VANTAGE
Technology Consulting Group

NIST CSF



VANTAGE
Technology Consulting Group

NIST Cybersecurity Framework

- Consists of three fundamental components:
  - Framework core: set of information security activities an organization is expected to perform and their desired results
  - Framework tiers: help relate the maturity of security programs and implement corresponding measures and functions
  - Framework profile: used to perform a gap analysis between the current and a desired state of information security/risk management

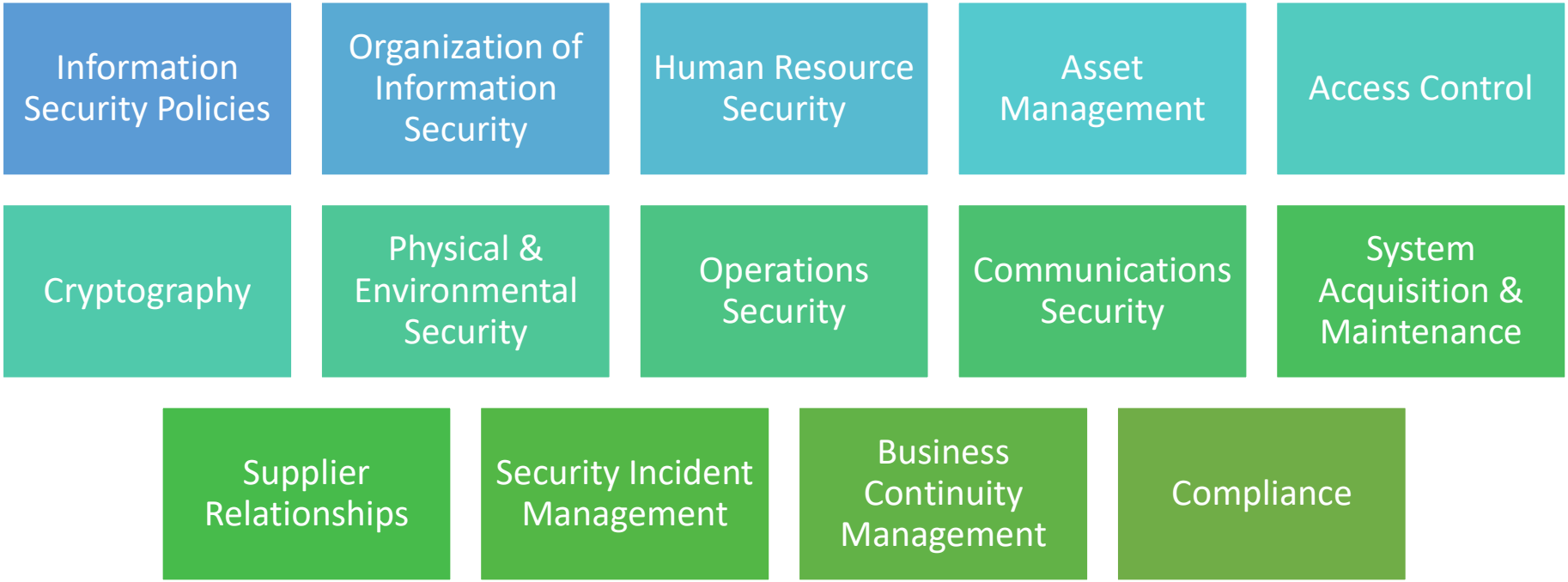
VANTAGE
Technology Consulting Group

NIST Cybersecurity Framework

- Seven-step approach to implementing/improving programs:
  - Prioritize and scope
  - Orient
  - Create current profile
  - Conduct risk assessment
  - Create target profile
  - Determine, analyze, prioritize gaps
  - Implement action plan

VANTAGE
Technology Consulting Group

ISO 27001



VANTAGE
Technology Consulting Group

Recipe for marinara sauce

- Tomatoes (native to hills around Florence)
  - Roma, San Marzano, and Cuore Di Bue
- Sugar - ¼ tsp
- Salt ¼ tsp
- White pepper 1 pinch
- Water (well water from Italian hillside farm) 2 cups
- Cook tomatoes down and remove skins
  - Dry skins and use them later ground up
- 1tbsp olive oil fresh pressed
- 1 clove garlic
- 1 tsp Basil
- ½ tsp Thyme
- ¼ tsp oregano
- Mix ingredients and cook on low for a ½ day

Value Model

- How to get value out of your security investments
  - Ingredients
    - Security Operations
    - Use frameworks to create standards
    - Evaluate by standards
  - Quantity of the ingredients
    - How much compliance?
      - Governance
  - Plan
    - Recipe
      - Instructions on how to measure and combine to get our “sauce”

VANTAGE
Technology Consulting Group

Questions?

VANTAGE
Technology Consulting Group