PUBLIC CONTRACTING INSTITUTE

IT Systems Overview: Meeting Federal Security & Compliance Regulations

PUBLIC CONTRACTING INSTITUTE

Today's Presenter – CORTAC Group

Ace Swerling
(CORTAC)

+1 305. 24 1213
ace.swerling@cortacgroup.com

Ace Swerling has over 30 years of security experience and has helped many of the largest organizations in the world to expand and protect their business by taking a balanced approach. Starting at a large US Defense contractor, he learned that security is critical to defending the country, complying with regulations, and resisting attack. Security is equally critical to facilitating collaboration and ensuring economical results. He is dedicated to security and collaboration as business enablers by identifying business needs, defining processes, mapping to technical requirements, selecting vendors, and implementing quality solutions while managing risk and ensuring compliance.

Ace specializes in IT strategy & security architecture, governance, risk, and compliance (GRC), product ownership supporting requirements definition, product selection, and implementation, identity and access management, hybrid cloud adoption, integration, and management, email, collaboration, document classification & handling, and customer and supply chain portals.

What CMMC Will Do

1. **Uniform and auditable metric to measure strength / maturity / resiliency of a contractor's cybersecurity program or capabilities**
2. **Eliminate partial credit (POA&Ms) / Must fully comply**
3. **Recognize different levels of protection for more sensitive data**
4. **Integrate requirements with Government's CUI program for identifying and marking data**
5. **Provide prime contractors with objective basis for assessing subcontractor cyber maturity**

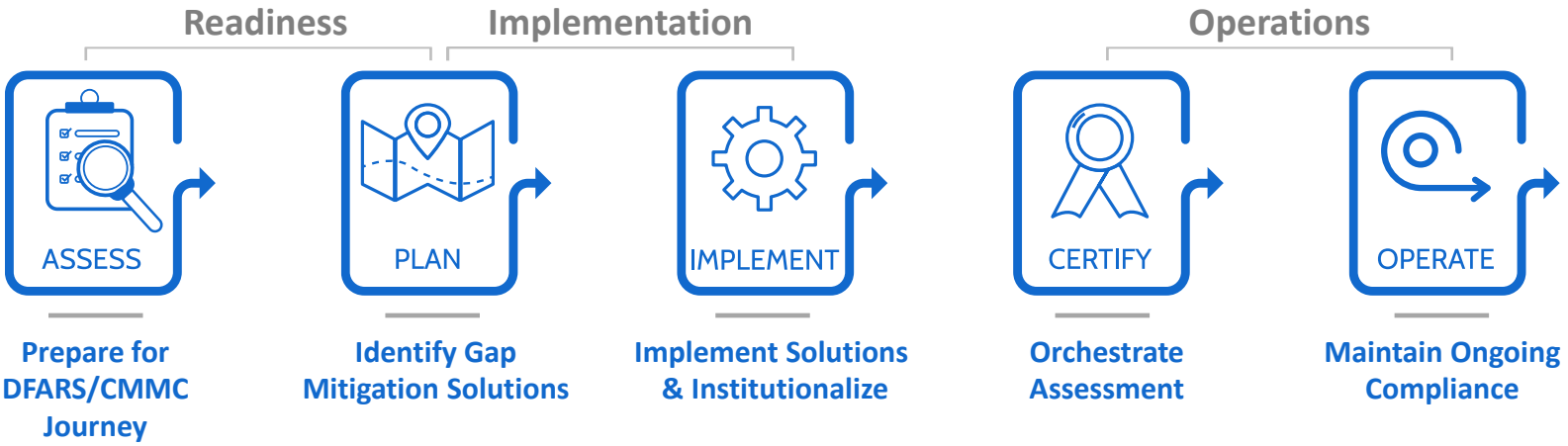
What CMMC Will Not Do

1. **Moot compliance with DFARS 252.204-7012**
2. **Eliminate need to identify, mark, control the distribution of CUI / CDI through the supply chain**
3. **Eliminate the need for imposition of other cybersecurity controls that DoD could choose to apply**
4. **Eliminate the need to make continuous improvements and updates to cybersecurity programs, even after an organization is certified**
5. **Eliminate all subcontractor cybersecurity related risks**

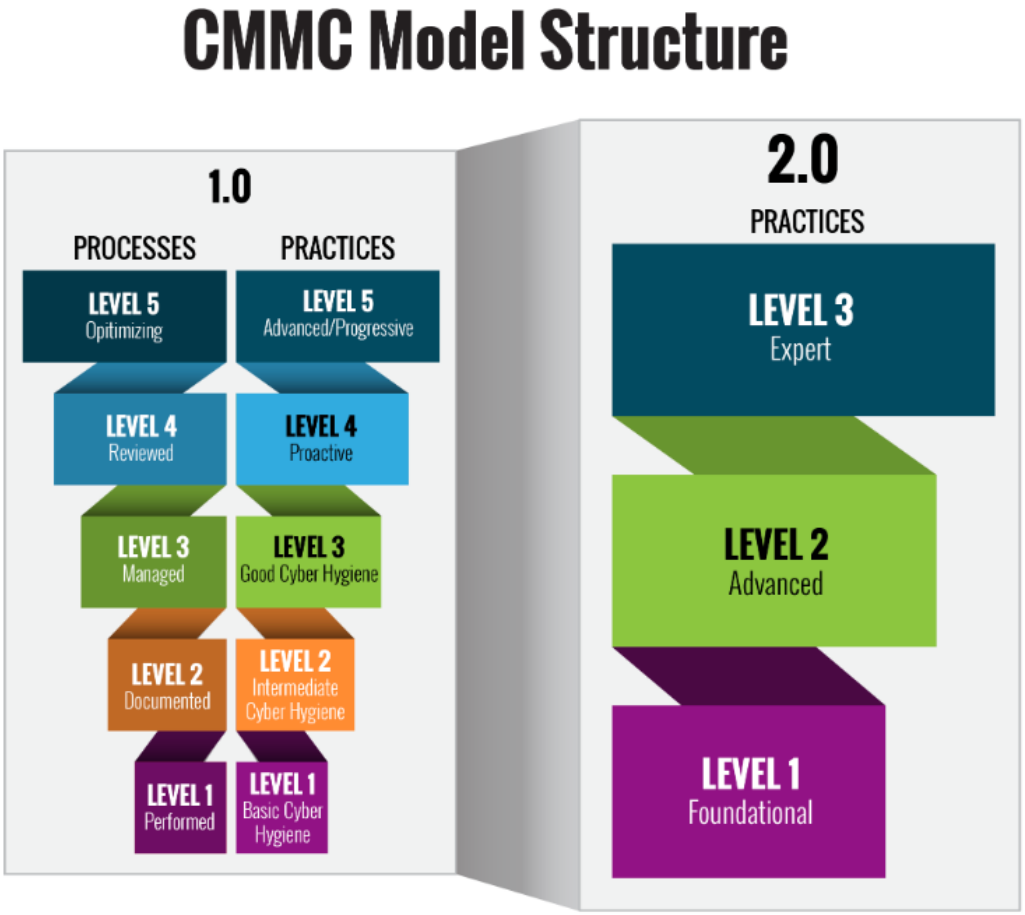
What Is Known About Certification

- Purpose: Demonstrate a threshold level of cyber maturity at the level required in a contract or by a prime contractor
- Certifications are more about compliance than security
  - Make sure the plan is documented and followed. Everything that's being done must be documented.
- CMMC assessments are rigorous
  - If you're not a 100% confident you're prepared, then you aren't
    - Every practice requirement must be addressed
    - Every process requirement must ultimately be satisfied
  - Primary reasons OSCs fail
    - CUI improperly identified; CUI boundary improperly defined
    - Documentation inadequate or insufficient

CMMC JOURNEY



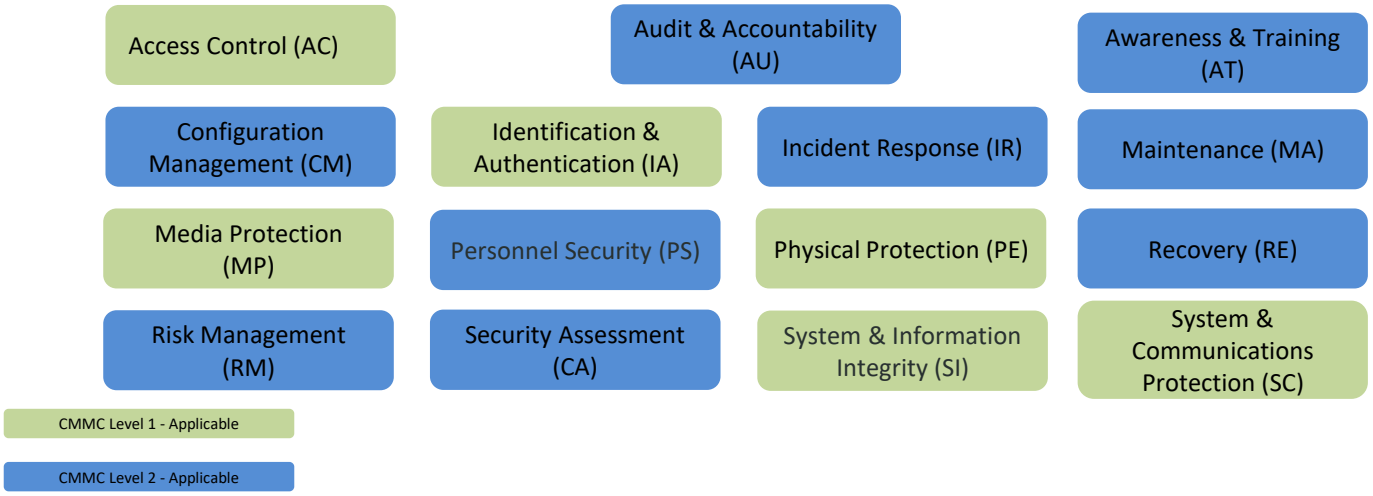
CMMC Model Overview



Source: Cybersecurity Maturity Model Certification (CMMC), version 2.0, November 2021

Note that the "CMMC Delta 20" controls have been removed. The CMMC 2.0 standards are NIST SP 800-171 v2 and SP 800-172a

CMMC Domains by Level



LEVEL 1: BASIC CYBER HYGIENE

- This level is intended to be equivalent to the requirements in FAR 48 CFR § 52.204-21 for safeguarding of Federal Contract Information (FCI) in covered contractor information systems.
- 15 Practices (technical activities) covering:
  - Limit access
  - Identify users
  - Sanitize media
  - Limit physical access
  - Protect networks
  - Find and fix system flaws
  - Stop malware
- At this level, it is sufficient to demonstrate that you "perform" the practices. There is no measurement of process maturity required. You may have limited or inconsistent processes.

CMMC Level 1: FCI vs CUI and Compliance

Any organization that possesses Federal Contract Information (FCI) as defined in FAR 52.204-21 must comply with CMMC Level 1.

What FCI <u>is</u>:

Not intended for public release

Provided by the government under a contract to develop or deliver a product or service to the government

Generated for the government under a contract to develop or deliver a product or service to the government

What FCI <u>isn't</u>:

Not including information provided by the government to the public such as a public website

Simple transactional information, such as necessary to process payments

CUI ≠ Level 1

If you handle CUI, Level 1 will not be enough

CUI is information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls

Source: https://www.acquisition.gov/content/52204-21-basic-safeguarding-covered-contractor-information-systems

LEVEL 2: GOOD CYBER HYGEINE

- This level is intended to be equivalent to the requirements NIST SP 800-171 Rev 2 specified under DFARS 252.204-7012 for safeguarding of Controlled Unclassified Information (CUI) and Covered Defense Information (CDI) in contractor information systems.
- 110 Practices (technical activities) adding:
  - Separation of duties
  - Control mobile devices
  - Encryption (FIPS-validated)
  - Centralized audit log management
  - Software blacklisting or whitelisting
- 340 evaluation criteria
- At this level, you must demonstrate that you establish and maintain plans for each of the capability domains and allocate adequate resources to meet the plans.

L2 Practices Removed From CMMC 1.0

These are a good idea, but not required.

Practice Number	Practice Description
AM.3.036	Define procedures for the handling of CUI data.
AU.2.044	Review audit logs.
AU.3.048	Collect audit information (e.g., logs) into one or more central repositories.
IR.2.093	Detect and report events.
IR.2.094	Analyze and triage events to support event resolution and incident declaration.
IR.2.096	Develop and implement responses to declared incidents according to pre-defined procedures.
IR.2.097	Perform root cause analysis on incidents to determine underlying causes.
RE.2.137	Regularly perform and test data back-ups.
RE.3.139	Regularly perform complete, comprehensive, and resilient data back-ups as organizationally-defined.
RM.3.144	Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.
RM.3.146	Develop and implement risk mitigation plans.
RM.3.147	Manage non-vendor-supported products (e.g., end-of-life) separately and restrict as necessary to reduce risk.
CA.3.162	Employ a security assessment of enterprise software that has been developed internally, for internal-use, and that has been organizationally defined as an area of risk.
SA.3.169	Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.
SC.2.179	Use encrypted sessions for the management of network devices.
SC.3.192	Implement Domain Name System (DNS) filtering services.
SC.3.193	Implement a policy restricting the publication of CUI on externally owned, publicly accessible websites (e.g., forums, LinkedIn, Facebook, Twitter).
SI.3.218	Employ spam protection mechanisms at information system access entry and exit points.
SI.3.219	Implement email forgery protections.
SI.3.220	Utilize sandboxing to detect or block potentially malicious email.

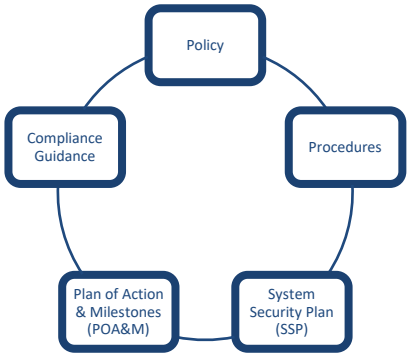
LEVEL 3: EXPERT CYBER HYGIENE

- Adds controls as defined in NIST SP 800-172a:
- NIST SP 800-172a includes 35 practices with 182 evaluation criteria
  - Total = 502 evaluation criteria
  - = (320 from 800-171) + (182 from 80-172a)

- "Level 3 will be based on a subset of NIST SP 800-172 and more detailed information will be released at a later date"
  - Source: Cybersecurity Maturity Model Certification - Model Overview (osd.mil)

Common Gaps

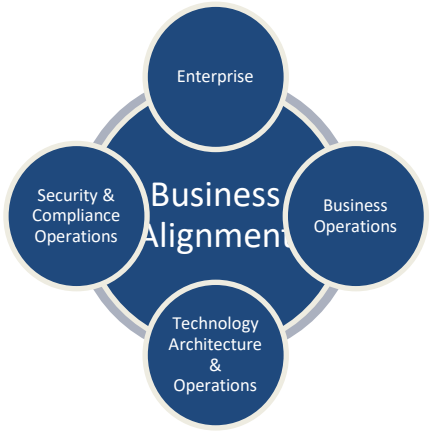
DOCUMENTATION



Description

One key aspect of CMMC is its focus on documentation. Often contractors may focus on technical controls to the detriment of robust compliance policies and evidence of implementation of controls.

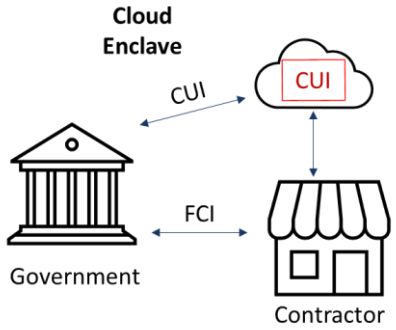
SECURITY & COMPLIANCE PROGRAM



Description

As contractors are permitted to implement NIST SP 800-171 through use of POA&Ms, significant gaps may exist relative to CMMC Level 3 requirements and above. Thus, contractors need to ensure that they devote sufficient resources to upgrade their controls where needed.

TECHNICAL SOLUTIONS



Description

Contractors that use or are seeking to migrate to cloud solutions will need to ensure that those solutions and the way in which they are implemented do not create compliance risks.

Requirements for Certification

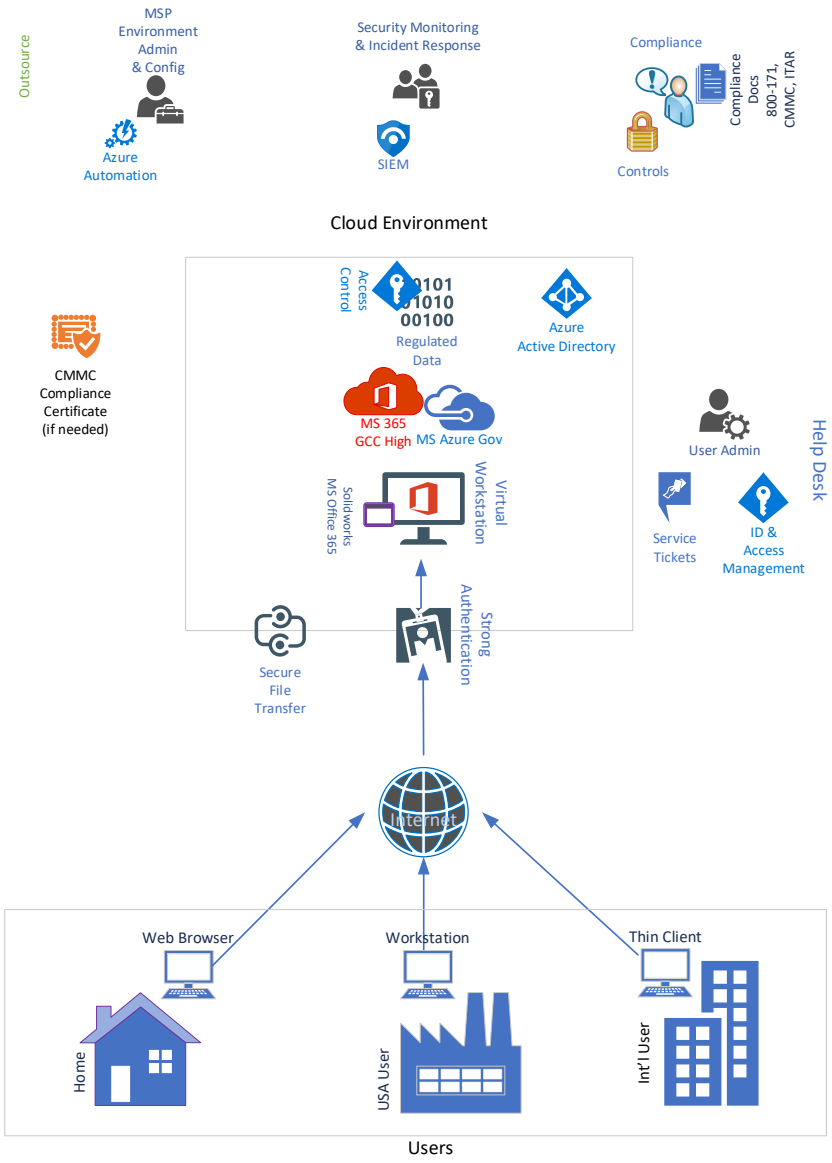
- Must ensure that documentation is clear
- Institutionalization is a requirement
- Technical compliance should be aligned with effective security
- Ensure security program & compliance have parity with IT function. More to come…

Reference Architecture for Handling CUI

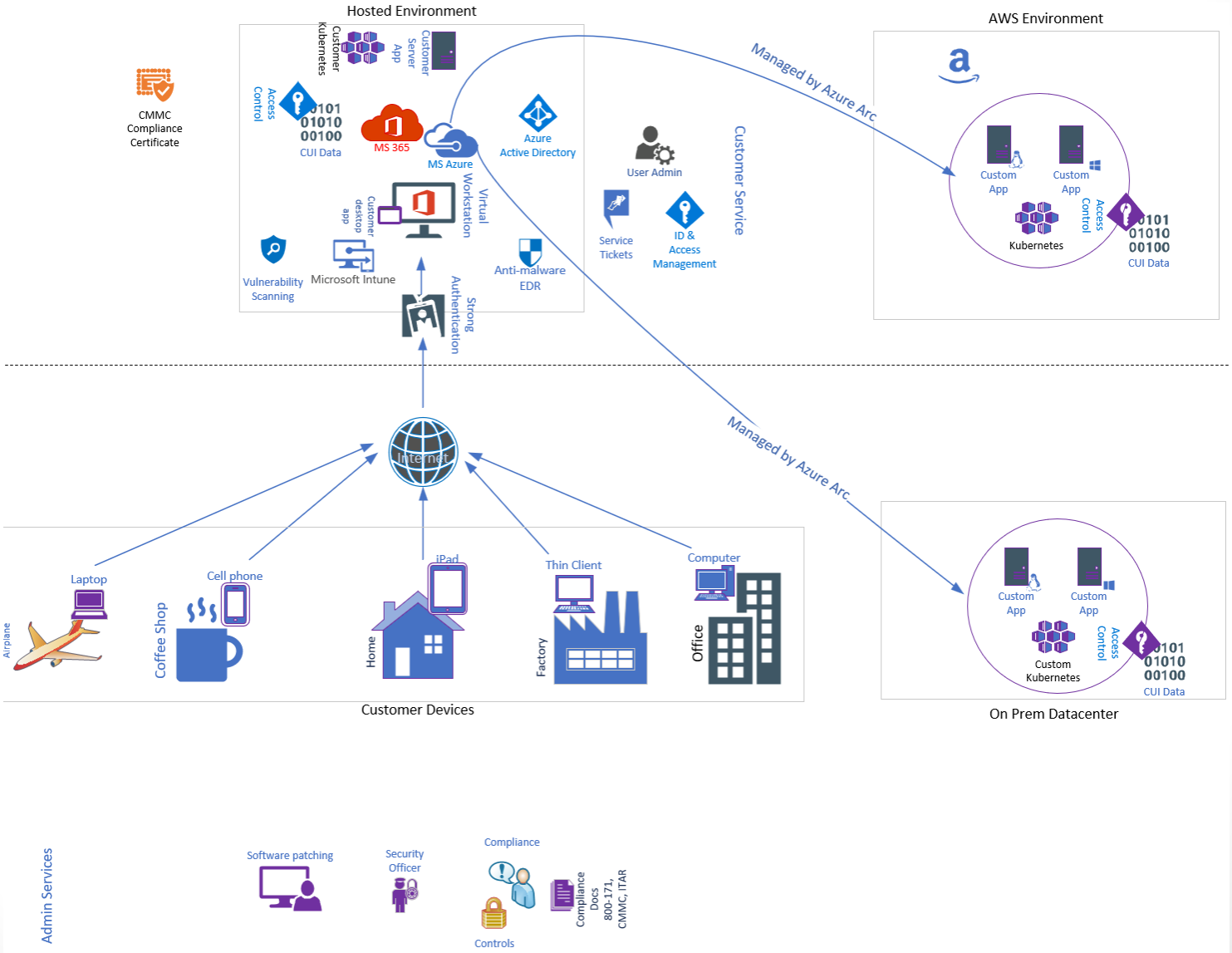
IT Architecture for CMMC Compliance

- Overlaying CMMC controls on existing IT may not be the best way
  - Retrofit vs. re-build
  - End-of-life-systems – isolate and separately manage
  - Operational Technology (OT) is out of scope for now. That will change in the future.
- Cloud adoption
  - Cloud-only vs hybrid designs
  - FedRAMP vs CMMC
  - Not all cloud providers are created equal
    - All claim to be “secure”
    - Many are FedRAMP
    - Shared responsibility models and CMMC alignment vary greatly
- Service Providers
  - Access to data determines need for CMMC

Outsourced Cloud Architecture



Hybrid Cloud Architecture



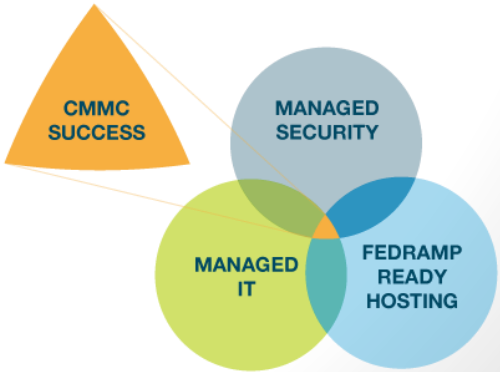
Sample Security Tool Tech Stack

- CMMC-compliant configurations
- FedRAMP cloud computing
- Consider operational support model
- Generally, fewer vendors is better
  - Less complexity
  - Better functionality
  - Lower cost
  - Easier documentation & compliance

Microsoft	OS hardening Mobile device management Encryption Identity and access management Multifactor authentication Data loss prevention	E-mail protection Data security Cloud app security Data replication Compliance monitoring
SentinelOne	Endpoint protection Malware detection and blocking	
elastic	Log management Analysis, alerting, investigation Visualization	
tenable	Software vulnerability management	
N-ABLE	Remote management and monitoring Software install/patch management User support	
FORTINET	Firewall Intrusion prevention Web content filtering	
ConnectWise	Service management	
BitTitan	Data migration	
thycotic	Password vaulting Privileged access management	

Technical Services Overview: What to Look For

- SecOps
  - Blended security and IT operations focused on security effectiveness, stable IT, and compliance
  - Integrated people, process, and technology
  - Operational discipline aligned with CMMC maturity requirements
- Cloud services (FedRAMP Moderate compliant)
  - General productivity and collaboration
  - ERP and other application hosting
- Support
  - End-user devices (laptop, phone), networks, servers, cloud computing
  - Help Desk
- Cybersecurity Maturity Model Certification (CMMC) Level 2, DFARS 252.204-7012 and NIST SP 800-171 compliant security program
  - All required practices and processes
  - Documentation
  - Audit support



Utilizing Service Providers

- Overlaying CMMC controls on existing IT may not be the best way
  - Retrofit vs re-build
  - End-of-life-systems – isolate and separately manage
  - Cloud adoption
  - Cloud-only vs hybrid designs
  - FedRAMP vs CMMC
- Not all cloud providers are created equal
  - All claim to be “secure”
  - Many are FedRAMP, all need to be FedRAMP Moderate Equivalent
- Shared responsibility models, CMMC knowledge and certification vary greatly

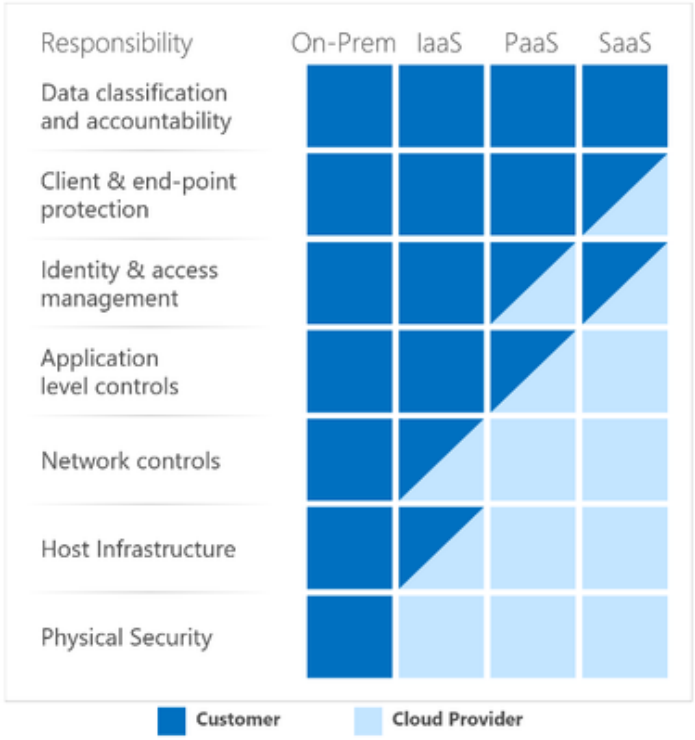
CMMC Shared Responsibility Model

- How much of the compliance burden can be transferred?
  - Third-Party MSPs and MSSPs can act as an extension of staff to guide the security and compliance effort
  - Compliance responsibility *may not be transferred* to a third party. Vendors can help, but the Organization Seeking Compliance is responsible.
- Of 110 required controls, a service provider may cover 86 practices

  Client responsibilities for the remaining practices include:
  - Approval decisions (35 practices)
  - Physical security of on-premises equipment, media, and paper documents (6 practices)
  - Personnel screening (2 practices)
  - Monitoring controls provided by client (1 practice)
- The security program must cover all 110 controls for planning, documentation, monitoring, evidence gathering, and audit support

Cloud Services Can Lower Compliance Burden

- Shared Responsibility Model
  - CSP Responsible: Inherited controls
  - Partially inherited controls
  - Inherited with a customer responsibility
  - Customer Responsible
- CSPs provide responsibility matrix
- Caution: Cloud services aren't a silver bullet



Accelerating CMMC compliance for Microsoft cloud, Richard Wakeman October 2020 Update

Security Programs

Security Program Components

- **Responsibility for cybersecurity compliance**, before, during, and after the CMMC audit.
- **Information Security Officer (ISO)** - “go-to” person for all security compliance items and is responsible to drive the security program from beginning to end.

1X

- **Gap assessment** mapped directly to the applicable compliance requirements (CMMC, FAR, DFARS, etc.)
- Define CMMC **boundaries and data flows** to establish the **scope** of certification.
- **Foundational documents** needed for a mature security program – policies, procedures, security plans, etc.

- **On-going support** to drive periodic recurring security program **continuous monitoring** tasks on a strict schedule, ensuring that all required processes operate effectively.
- **Review** data from system **activity logs, vulnerability scans**, and open **security roadmap** items monthly to tune alerts and prioritize actions.

- Access to **security expertise** for questions, new systems, new risks, etc.

Sample Shared Responsibility

Access to production environment

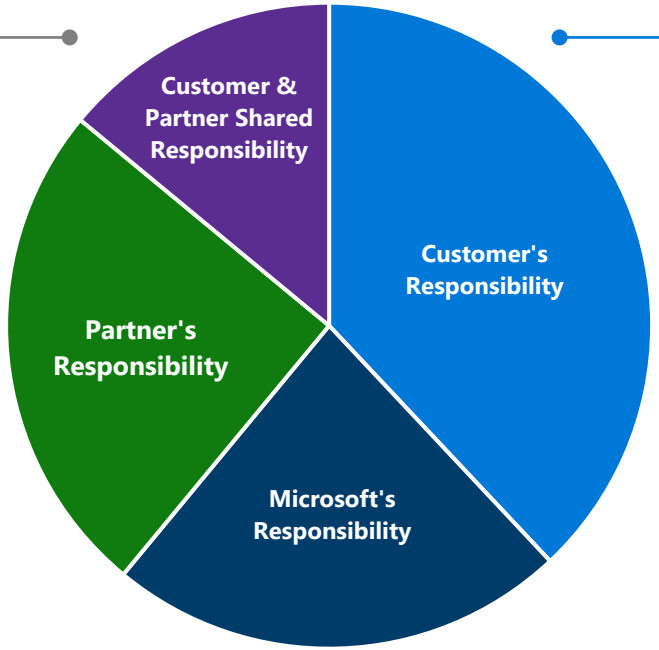
Set up access controls that strictly restrict standing access to customer's data or production environment

Protect data

Encrypt data at rest and in transit based on industrial standards (BitLocker, TLS, etc.)

Personnel control

Strict screening for employees, vendors, and contractors, and conduct trainings through onboarding process



Access to production environment

Set up access control policy and SOP, leveraging Customer Lockbox*/ identity management solutions

Protect data

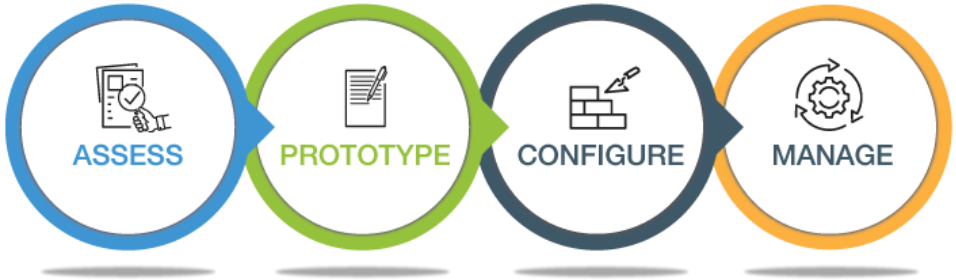
Encrypt data based on org's compliance obligations. E.g. encrypt CUI in transit between users, using its own encryption key, etc.

Personnel control

Allocate and staff sufficient resources to implement and operate an organization-wide privacy program, including awareness-raising and training

Source: Microsoft

CMMC Approach



ASSESS

1. Determine scope, boundary, and CUI data flows for the CMMC environment
2. Evaluate corporate security policies
3. Evaluate IT use cases and current environment
4. Complete Security Control Matrix

PROTOTYPE

1. Select best-fit reference architecture
2. Identify any needed modifications
3. Set up prototype

CONFIGURE

1. Complete system security plan and supporting security program documentation
2. Complete production IT build-out
3. Migrate users and data
4. Train users

MANAGE

1. Continuous monitoring
2. Capacity/performance monitoring
3. Vulnerability/patch mgmt.
4. Change management
5. User support
6. Break-fix
7. Audit readiness/support
8. Security governance

Technical Practices

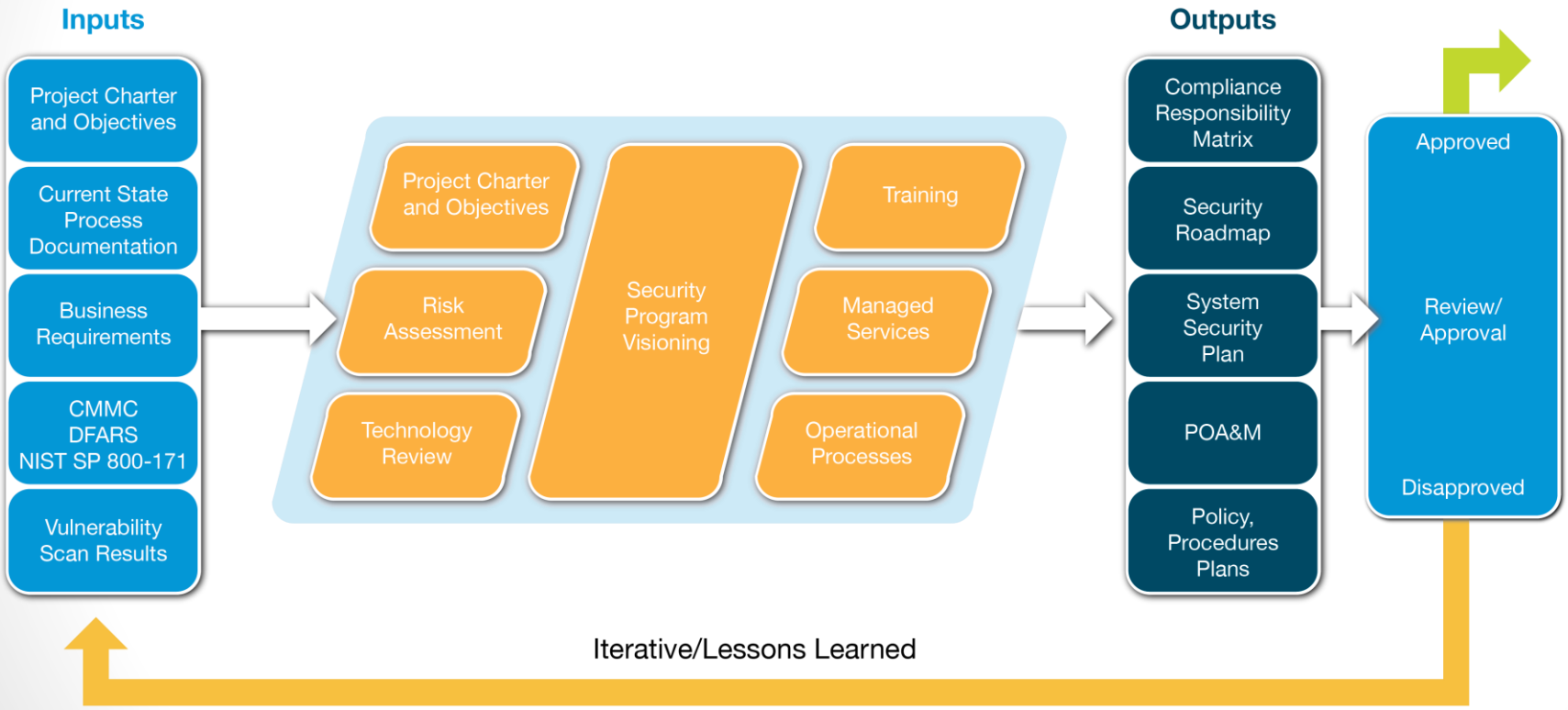
- Managed detection and response (log management)
- Endpoint protection (managed anti-malware)
- Boundary protection (managed firewall)
- Vulnerability scanning
- Network, server, and endpoint management
- Patch management
- Backup and recovery
- Encryption
- Email protection
- Cloud management

- Practices must produce evidence to show auditors

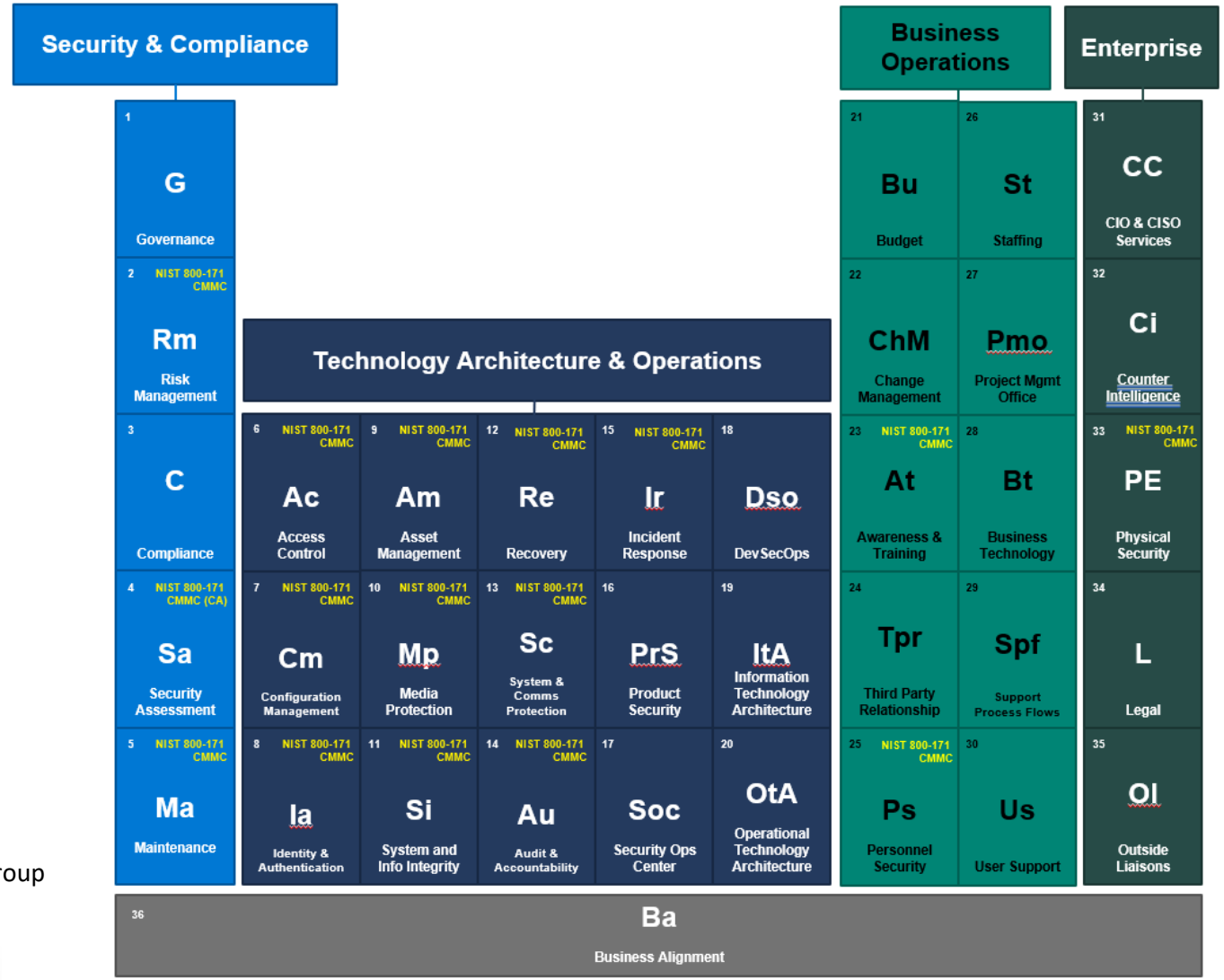
Security Operations & Reporting

- Security control list
- Supporting docs and evidence
- System Security Plan
- Tracking of roadmap projects
- Plan of Actions and Milestones
- Log and vulnerability data
- Continuous monitoring – evidence of effectiveness of controls

Sample Security Program Development



Operational Security Framework



Source: CORTAC Group

Questions