US Census Bureau
Office of Information Security

Security Control Overlays: A Dynamic Approach to Risk Management

May 8, 2019

About the Speakers

Tameika Turner

Ms. Turner was promoted to the position of IT Specialist in the Certification and Accreditation Branch in 2011. She was instrumental in the Census Bureau's transition from the 3-year Certification & Accreditation (C&A) cycle to the Risk Management Framework (RMF) through: the development of IT system risk profiles driven by a quantitative risk scoring methodology, the establishment of enterprise common controls, and the deployment of a Governance, Risk, and Compliance repository. She also leads and coordinates data calls for auditors and other external entities. In her new role as the Risk Management Program Branch Chief, Ms. Turner oversees security policy & procedure development, leads the coordination of data calls from external auditors, and continues to support the Assessment & Authorization (A&A) activities leading up to the 2020 Decennial Census.

Ms. Turner graduated from Bowie State University with a BA in Business Administration and is working toward a master's degree in Information Assurance. She was awarded the Department of Commerce Gold Medal Award in 2014 and has obtained the ISC^2 Certified Authorization Professional (CAP) certification.

Kunmi Akingbade

Mr. Akingbade is a Senior Manager at Deloitte in the Cyber practice. He specializes in the following areas: helping federal agencies establish a comprehensive risk management program by developing security strategies & policies, managing the deployment/integration of Governance, Risk, and Compliance (GRC) tools, preparing/executing security audit readiness activities, and conducting security assessments.

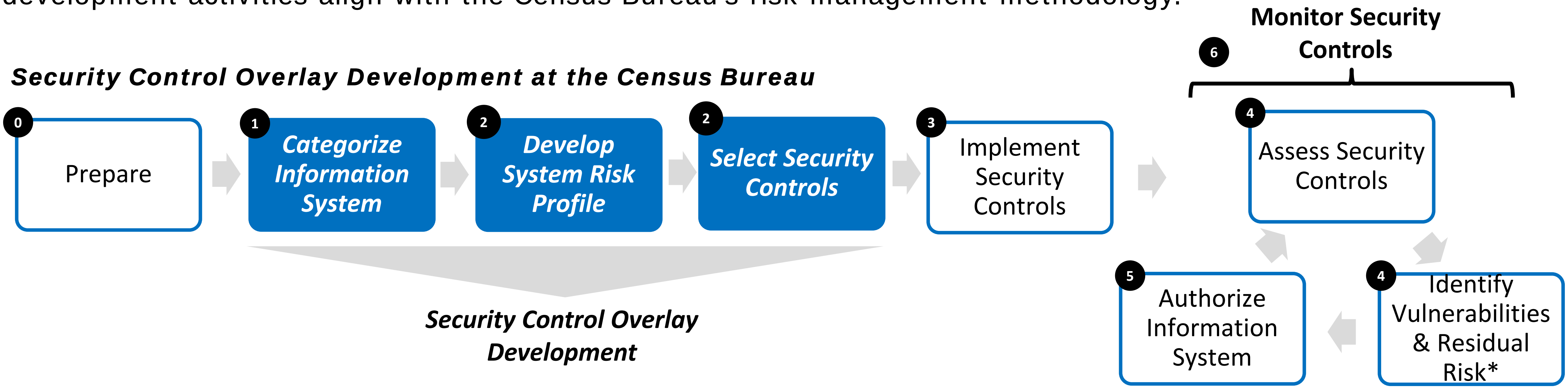
Mr. Akingbade currently holds the following industry certifications: Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), and Certified Information Privacy Professional (CIPP/G). He graduated from the University of Maryland, College Park with a degree in Information Systems and Operations Management, and a certificate in entrepreneurship. He continued his education at the University of Maryland, University College obtaining dual Master's degrees in Cybersecurity and Business Administration.

Agenda

- Security Control Overlay Establishment at the Census Bureau
- Security Control Overlays in Action
  - Common Controls Providers
  - IRS Publication 1075
  - Cloud-Based Systems and Services
- Organizational Benefits of Security Control Overlays

Security Control Overlay Establishment at the Census Bureau

Risk Management & Security Control Overlays: The graphic below illustrates how security control overlay development activities align with the Census Bureau's risk management methodology.



Security Control Overlay Development at the Census Bureau

0 Prepare

1 *Categorize Information System*

2 *Develop System Risk Profile*

2 *Select Security Controls*

3 Implement Security Controls

6 **Monitor Security Controls**

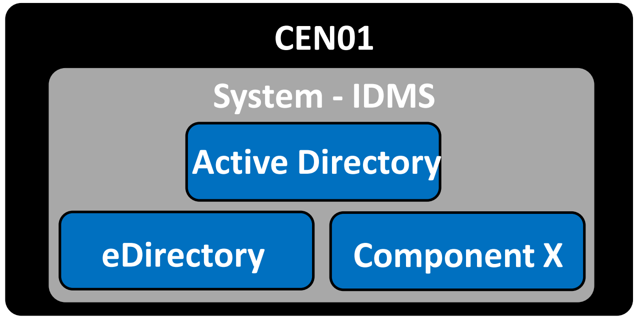
4 Assess Security Controls

4 Identify Vulnerabilities & Residual Risk*

5 Authorize Information System

Security Control Overlay Development

To understand the Census Bureau's security control overlay processes, it is important to see how the organization breaks down and documents its information technologies.



CEN01

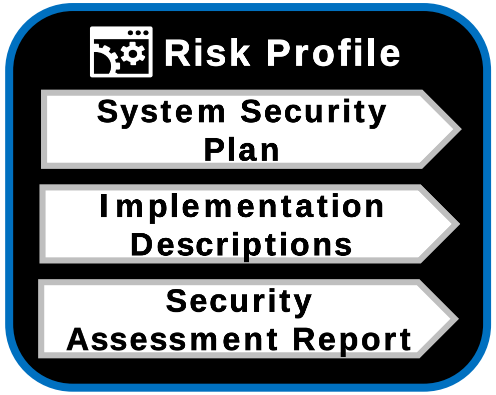
System - IDMS

Active Directory

eDirectory

Component X

- **CEN:** Categorization of information systems based on various business/mission factors.
- **System:** Categorization based on similar technological requirements and operating environments.
- **Component:** Individual technologies that comprise a system.



Risk Profile

System Security Plan

Implementation Descriptions

Security Assessment Report

The Census Bureau captures its **security information** for information systems in Risk Profiles. Risk Profiles are comprised of:

- System Security Plan
- Implementation Descriptions
- Security Assessment Report

**Risk based on the number and criticality of vulnerability scan findings and the results of manual control assessments*

Census Bureau Security Control Overlays: Overlays help an organization apply controls to information systems in a dynamic and scalable manner commensurate with business and security requirements.

What Is a Control Overlay?

- Overlays are a **specification of security or privacy controls** employed during the tailoring process.
- Overlays may be more / less stringent that the original control parameters, and are intended to **refine** security control baselines.

How Can They Help Organizations?

✓ Increase the **visibility of key risks** for information systems and their data.

✓ Reduce **time** and **LoE** during the authorization process.

✓ Apply security controls **consistently** across information systems despite different technical/business needs.

Important Considerations:

- Method is **scalable** and **transferable** based on organizational needs and complexity (e.g., system-level vs. component-level).
- Method is **tool-agnostic** and can be applied to any Governance, Risk, and Compliance tool or program (e.g., CSAM, eMASS).
- Implementation was **iterative** and occurred in **phases** over a prolonged period of time.
- ISSO works in coordination with SO and Security Engineer to **verify** controls are correctly scoped/tailored.

Using Questionnaires to Drive Overlay Development: The Census Bureau leverages two (2) automated questionnaires to narrow the scope of applicable security controls for an information system, and generate an control overlay.

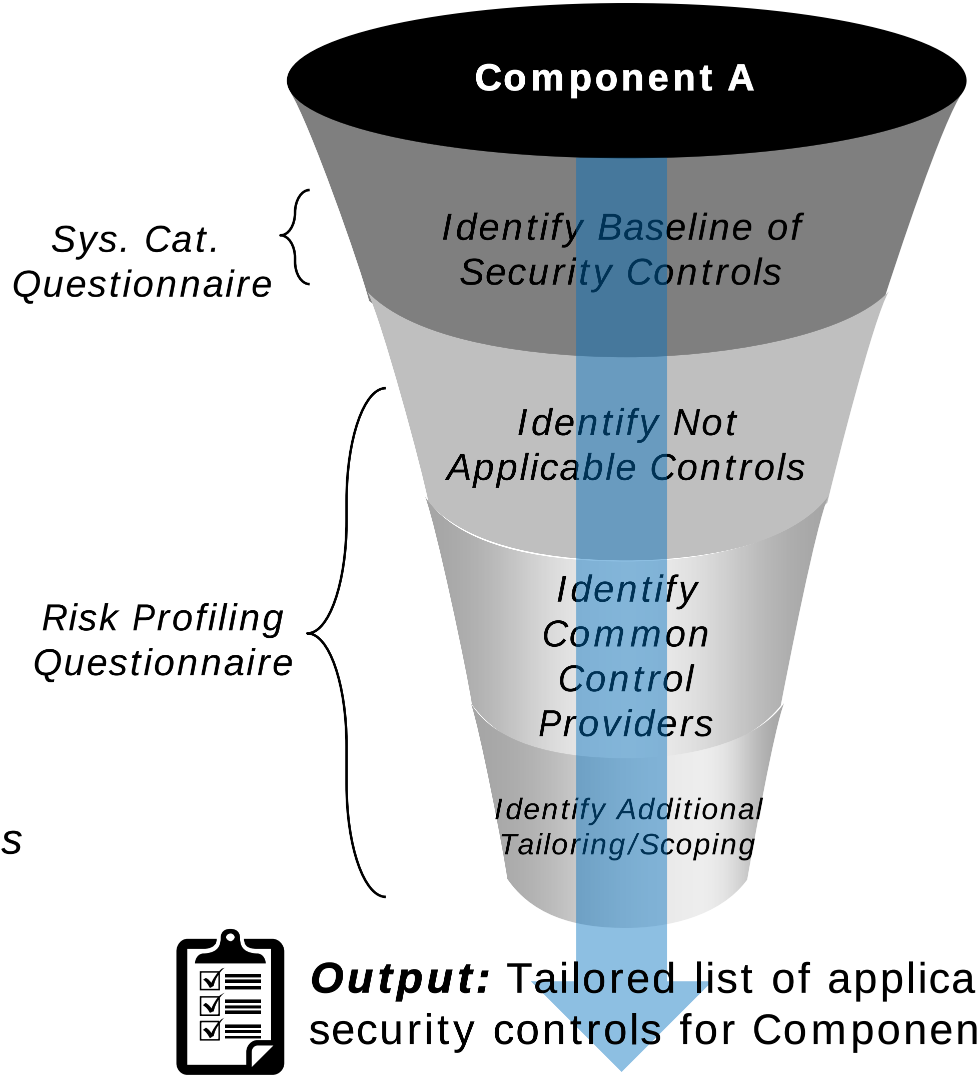
During Steps 1 and 2 of the Census Bureau's Risk Management Framework Methodology, ISSOs and Security Engineers complete the questionnaires below for each component. Questionnaires are currently completed in the Census Bureau's centralized risk repository, the Risk Management Program System (RMPS), but will be transitioned to RSA Archer.

1. System Categorization Questionnaire

2. Risk Profiling Questionnaire

The following slide will provide an overview of the mechanics of each questionnaire.

Automated Security Control Selection


Component A
Sys. Cat. Questionnaire
Identify Baseline of Security Controls
Risk Profiling Questionnaire
Identify Not Applicable Controls
Identify Common Control Providers
Identify Additional Tailoring/Scoping

Output: Tailored list of applicable security controls for Component A

A Closer Look at Automated Questionnaires: The questionnaires below help the Census Bureau align security controls with business, technical and organizational factors, and assign ownership of security controls.

1. The System Categorization Questionnaire determines the security control baseline:

NIST 800-60 data types which automatically determine the FIPS-199 Security Categorization (Low, Moderate, High)

2. The Risk Profiling Questionnaire further narrows applicable controls by asking questions related to:

- Business Processes (e.g. data sensitivity, business use, scope of users, etc.)
- Technical factors (e.g. system architecture, network location, accounts, etc.)
- Full or hybrid Common Control Provider usage by the component
- Applicability of the control based on technical specifications

Understanding the Impact

This approach enables the Census Bureau to select security controls **consistently**, and in a **repeatable** manner by removing the manual step of selecting controls, which is often highly subjective. It also enables us to assign **security responsibility** for shared services, and automatically eliminates controls that are **not applicable** to a given technology.

Security Control Overlays in Action

Common Control Providers: The establishment of a robust Common Control Program is a key tenant of the Census Bureau's Risk Management Program.

The Census Bureau established the following categories of common control providers to help assign security responsibility and manage risk:

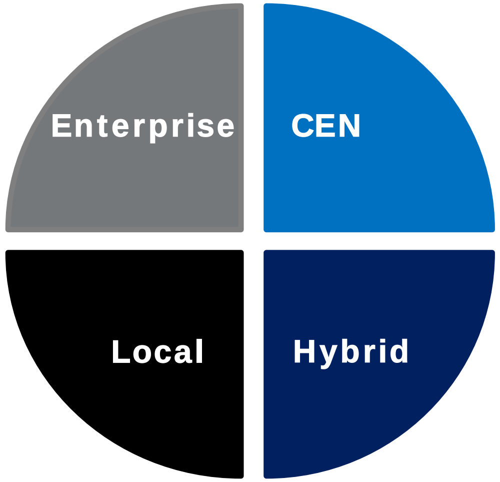
Enterprise:
A component, system, or documented process that provides an **enterprise service.**

CEN:
Non-technical, **operational** requirements that apply to components managed by a Directorate.

Local:
A component, system, or a documented process that serves a **subset of components** that reside within a particular Directorate.

Hybrid:
An enterprise, CEN-level, or local CCP that **shares responsibility** for a control with a component.

Security controls can be tailored to the following types of common control providers:



Establishing Overlays for Common Control Providers

The Risk Profiling Questionnaire helps identify controls satisfied by CCP, either fully or partially.

Example:

Risk Profiling Questionnaire

☐ *Will this component leverage account management services from the enterprise?*

By answering "Yes" to this question, controls associated with the Enterprise Account Management CCP are automatically removed from the **component applicable** control set. Controls satisfied by a CPP are categorized as **inherited risk**.

This approach enables the Census Bureau to:

- Align security **responsibilities** with organizational Centers of Excellence (COEs)
- Reduce **duplication** of technologies, processes, and policies in a cost-effective and security-centric manner
- Increase **efficiency** of authorization activities and continuous monitoring, as controls provided by CCPs are only assessed once.

IRS Publication 1075: At the Census Bureau, information systems that process, store, or transmit Title 26 data must comply with IRS Publication 1075 requirements.

IRS

Publication 1075

Tax Information Security Guidelines
For Federal, State and Local Agencies

Safeguards for Protecting Federal Tax Returns
and Return Information

IRS Publication 1075 provides guidance to ensure the policies, controls, and safeguards employed by the recipient agencies **adequately protect the confidentiality of FTI.**

A Closer Look: Title 26 Overlay

The Title 26 overlay was designed to enforce the generally more stringent IRS requirements to information systems as appropriate.

Risk Profiling Questionnaire

What is the highest data sensitivity within this component?

- FOUO
- T13
- **T26**

By answering "T26" to this question on the Risk Profiling Questionnaire, the **Title 26 overlay is automatically applied to the information system.**

Key Takeaway: **Dynamic Control Parameters**

The Title 26 overlay does not just add security controls to an information system's baseline. It also automatically ***modifies*** organization-defined assignments to be commensurate with IRS Publication 1075 requirements.

Cloud-Based Systems and Services: As the federal government, transitions its technologies from data centers to multiple cloud environments, organizations must be able to integrate FedRAMP packages into their security programs.

How Do We Integrate Cloud Packages?

- Customize cloud package baseline based on the Census Bureau's organizationally defined baseline.
- Apply a questionnaire to identify unique technical characteristics and business needs of the cloud-based system/service.
- Tailor Customer Responsible Controls (CRCs) to common control providers.

How Can They Help Organizations?

- ✓ Create repeatability and reusability across different types of cloud environments.
- ✓ Establishing a repeatable, consistent process for integrating cloud packages into the risk management program.

A Closer Look: Adapting Cloud Packages

The Risk Profiling Questionnaire drives the assimilation of cloud packages by triggering a sub-questionnaire to determine control applicability and identify what the cloud package that can leverage from its environment (e.g., infrastructure/middleware)

Example:

Risk Profiling Questionnaire

☐ *Does this component leverage perimeter defense capabilities from the PaaS?*

By answering **"Yes"** to this question, CRCs associated with perimeter defense capabilities are tailored to the **existing PaaS solution** for the cloud environment, and the Program Area is no longer responsible for implementation.

Key Takeaway: Reducing Customer Responsibility

In addition, the questionnaire helps identify additional **common control providers** from the enterprise, further **reducing the customer responsible implementation** for cloud-based systems and services.

Security Control Overlays and Organizational Benefits

Benefits Realized by the Organization: Using automated mechanisms to generate control overlays is a foundational element of the Census Bureau's Risk Management Program and significantly enhances our ability to execute risk management activities.

Increase **objectivity** in the selection and application of security controls.

Reduce reliance on **institutional knowledge** to tailor security controls.

Drive **service-oriented security culture** and promote technological, operational, and managerial reciprocity.

Help realize cost savings by applying security controls and overlays only **as necessary.**

How You Can Get There:

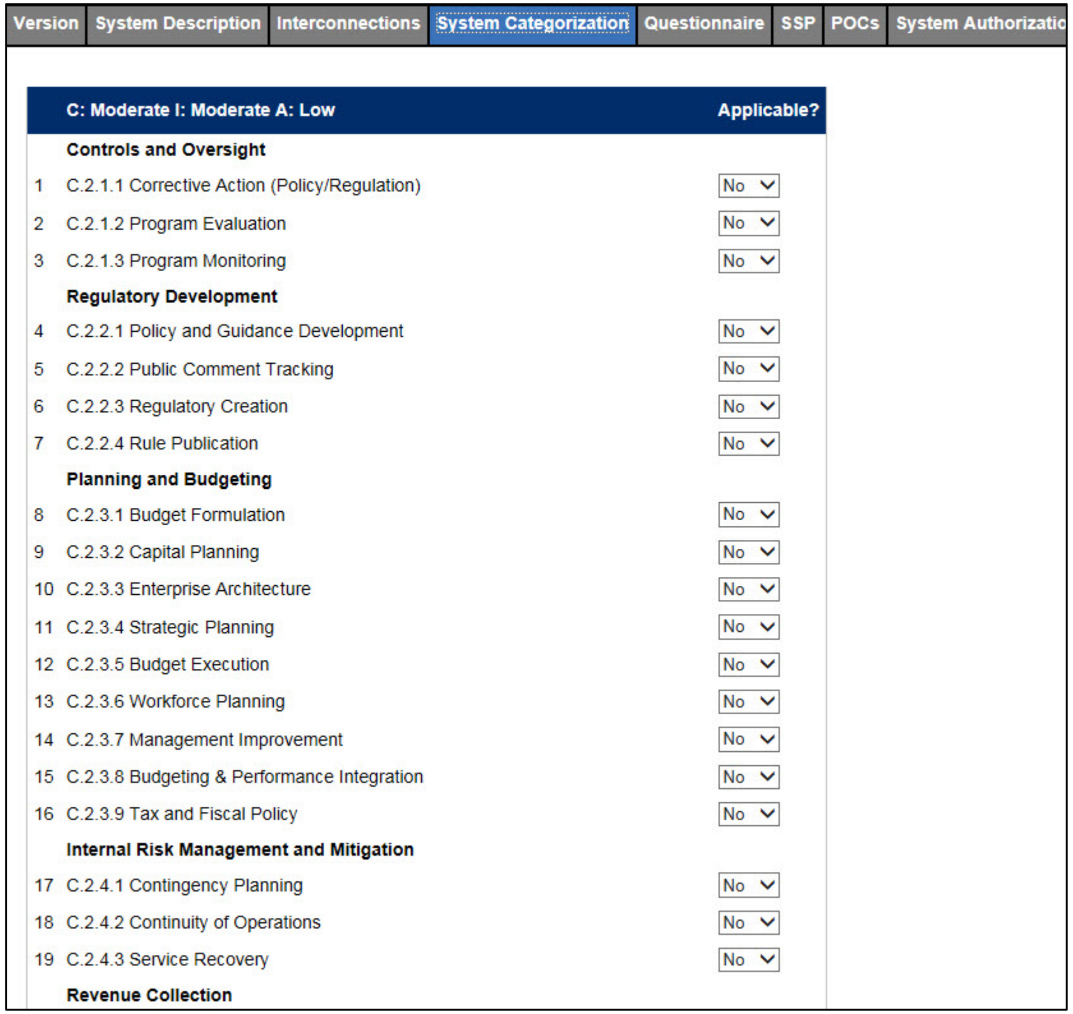
✓ Identify all **information systems, policies/processes, and technologies** in the enterprise.

✓ Develop a **common control provider program** and establish responsibilities (e.g., Common Control Provider Owner/Stewards).

✓ Centralize security control tailoring/overlay activities through an **automated questionnaire.**

Appendix: System Categorization Questionnaire & Risk Profiling Questionnaire Details

System Categorization Questionnaire Examples: The questions below are samples taken from the System Categorization Questionnaire.



	C: Moderate I: Moderate A: Low	Applicable?
	Controls and Oversight	
1	C.2.1.1 Corrective Action (Policy/Regulation)	No
2	C.2.1.2 Program Evaluation	No
3	C.2.1.3 Program Monitoring	No
	Regulatory Development	
4	C.2.2.1 Policy and Guidance Development	No
5	C.2.2.2 Public Comment Tracking	No
6	C.2.2.3 Regulatory Creation	No
7	C.2.2.4 Rule Publication	No
	Planning and Budgeting	
8	C.2.3.1 Budget Formulation	No
9	C.2.3.2 Capital Planning	No
10	C.2.3.3 Enterprise Architecture	No
11	C.2.3.4 Strategic Planning	No
12	C.2.3.5 Budget Execution	No
13	C.2.3.6 Workforce Planning	No
14	C.2.3.7 Management Improvement	No
15	C.2.3.8 Budgeting & Performance Integration	No
16	C.2.3.9 Tax and Fiscal Policy	No
	Internal Risk Management and Mitigation	
17	C.2.4.1 Contingency Planning	No
18	C.2.4.2 Continuity of Operations	No
19	C.2.4.3 Service Recovery	No
	Revenue Collection	

Risk Profiling Questionnaire Examples: The questions below are samples taken from the Risk Profiling Questionnaire.

Business Process Factors

- Encompass **three major groups** including administration services, support of delivery services, and internal management of resources.
- Includes **vulnerabilities** and **risks** that are applicable to systems that are involved in a **given business process.**

Sample Business Questions	Sample Answers
What is the highest data sensitivity level contained within this component?	FOUO T13 T26
Which of the following usages is best associated with this component?	Collection of Titled Data General Support System Dissemination of Public Info

Technical Factors

- Encompass **four major groups** including operating systems, database management systems, system architecture, and transaction and web processors.
- Includes vulnerabilities and risks that are applicable to systems that utilize a **given technology.**

Sample Technical Questions	Sample Answers
What is the system architecture of the component?	Client/Server Web Application Software Appliance
What is the network location of the component?	Stand-Alone Internal Production Network Publically Accessible