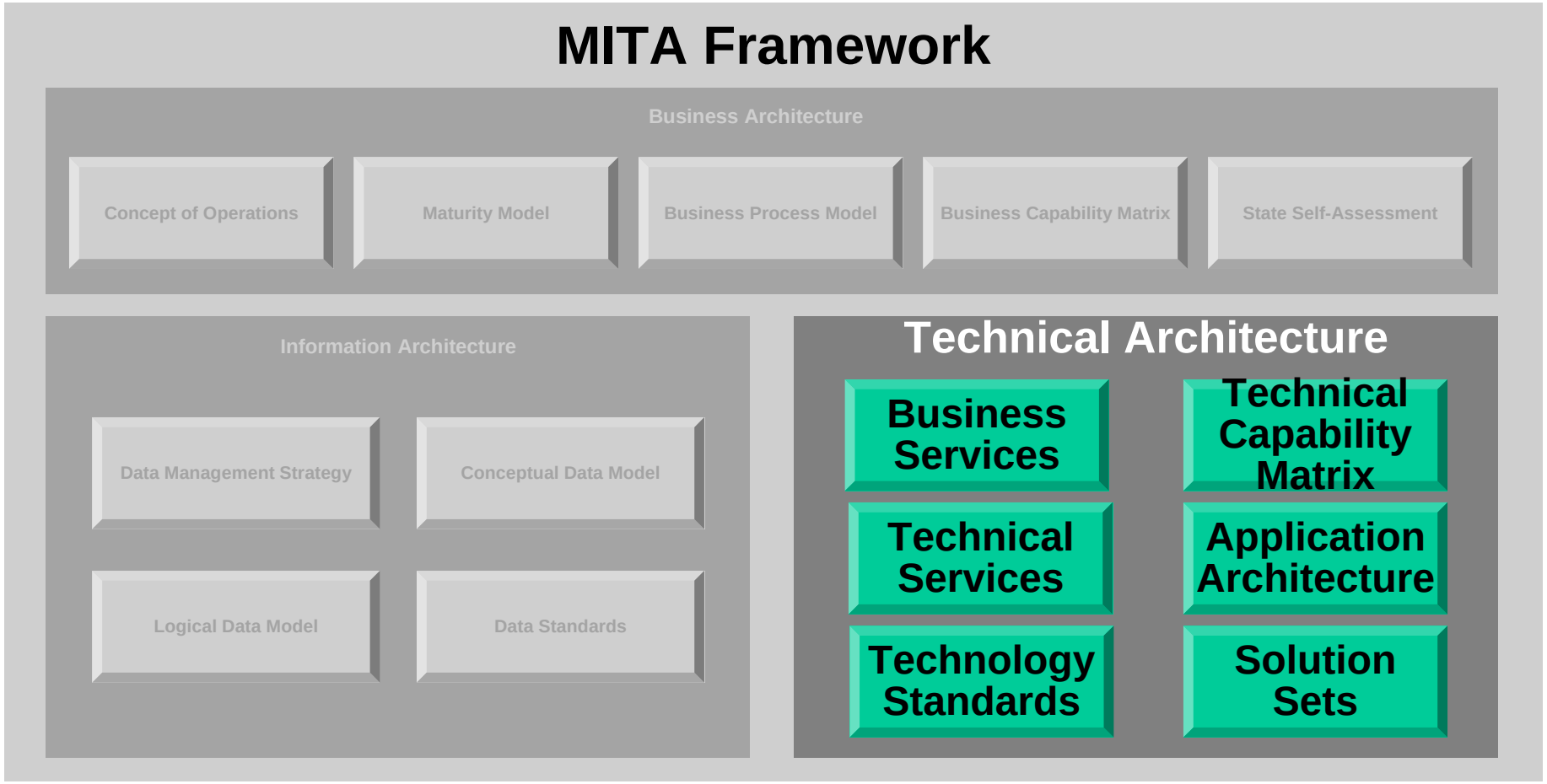
CMS

CENTERS for MEDICARE & MEDICAID SERVICES

MITA Application Architecture

May 8, 2006

Overview of the MITA Framework Components

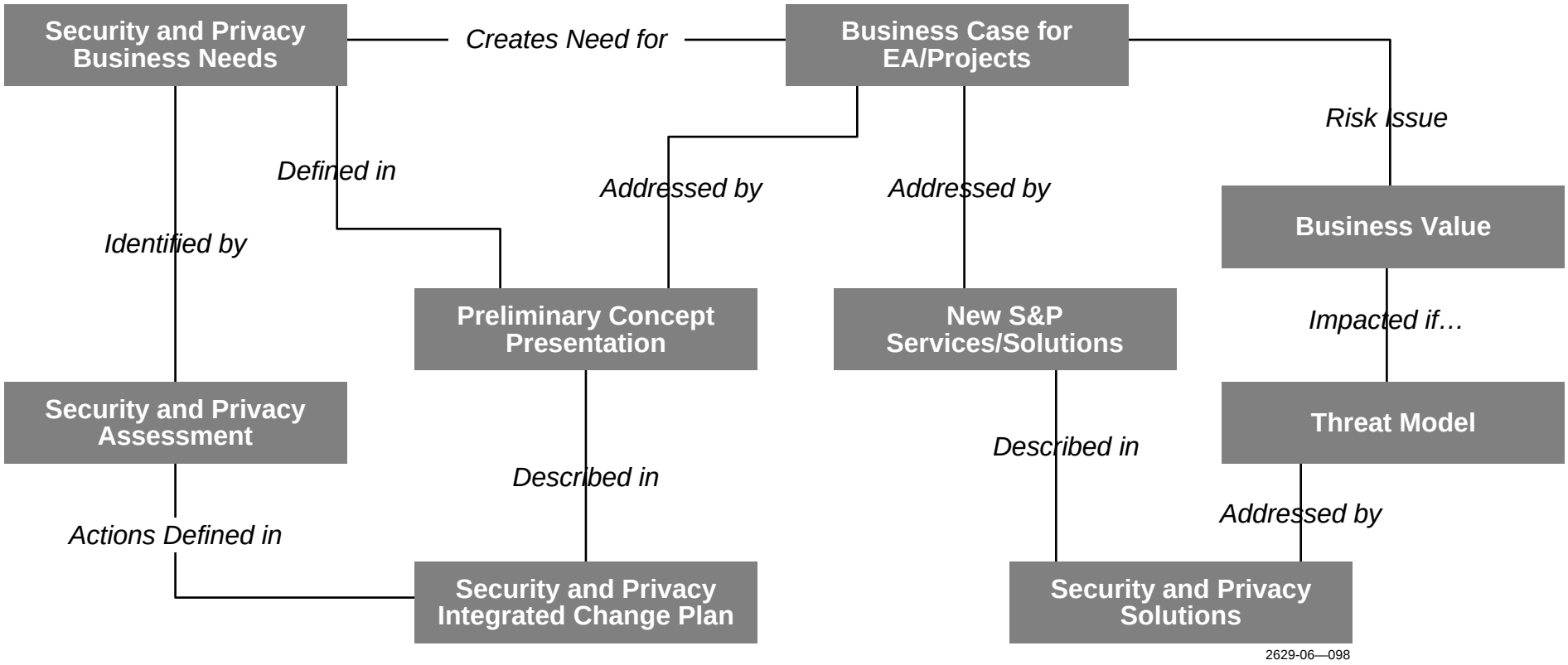


2629-06—013

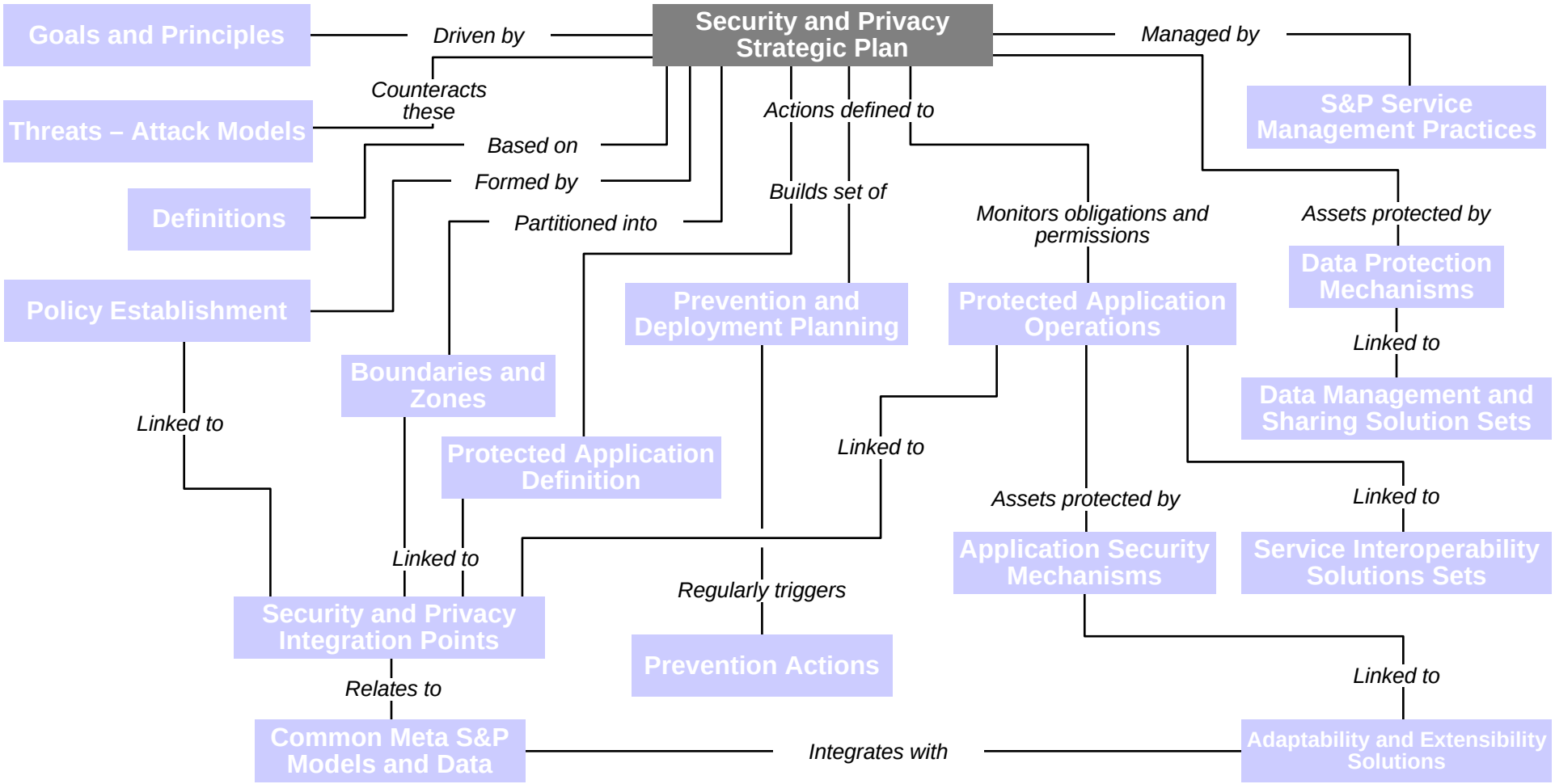
Basic MITA Security & Privacy Principles

Principle	Concepts
Compartmentalize	Reduce the surface area of attack. Ask how you will contain a problem. If an attacker takes over your application, what resources can the attacker access? Can an attacker access network resources? How are you restricting potential damage (e.g., firewalls, least privileged accounts, and least privileged code are examples of compartmentalizing)?
Use least privilege	Run processes using accounts with minimal privileges and access rights and thereby reduce an attacker's capabilities significantly if the attacker manages to compromise security and run code.
Apply defense in depth	Use multiple gatekeepers to keep attackers at bay. Defense in depth means that you do not rely on a single layer of security and assume that one of your layers may be bypassed or compromised. Can you survive if one firewall between different zones is not operational?
Do not trust user input	Your application's user input is the attacker's primary weapon when targeting your application. Assume all input is malicious until proven otherwise and apply an in-depth strategy to validate input, taking particular care to ensure that input is validated whenever a trust boundary in your application is crossed.
Check at the gate	Authenticate and authorize callers early — at the first gate.
Fail securely	If a system component or application fails, do not leave sensitive data accessible. Return friendly error messages to users that do not expose internal system details. Do not include details that might help an attacker exploit vulnerabilities in your application.
Secure the weakest link	Is there a vulnerability at the network layer that an attacker can exploit? What about other points?
Create secure defaults	Is the default account set up with least privilege? Is the default account disabled by default and then explicitly enabled when required? Does the configuration use a password in plain text? When an error occurs, does sensitive information leak back to the client in a way that the client can use against the system?
Reduce your attack surface	If you do not use it, disable it. Reduce the surface area of attack by disabling or removing unused services, protocols, and functionality. Does your server need all those services and ports? Does your application need all these features?

Aligning S&P and Enterprise Architecture

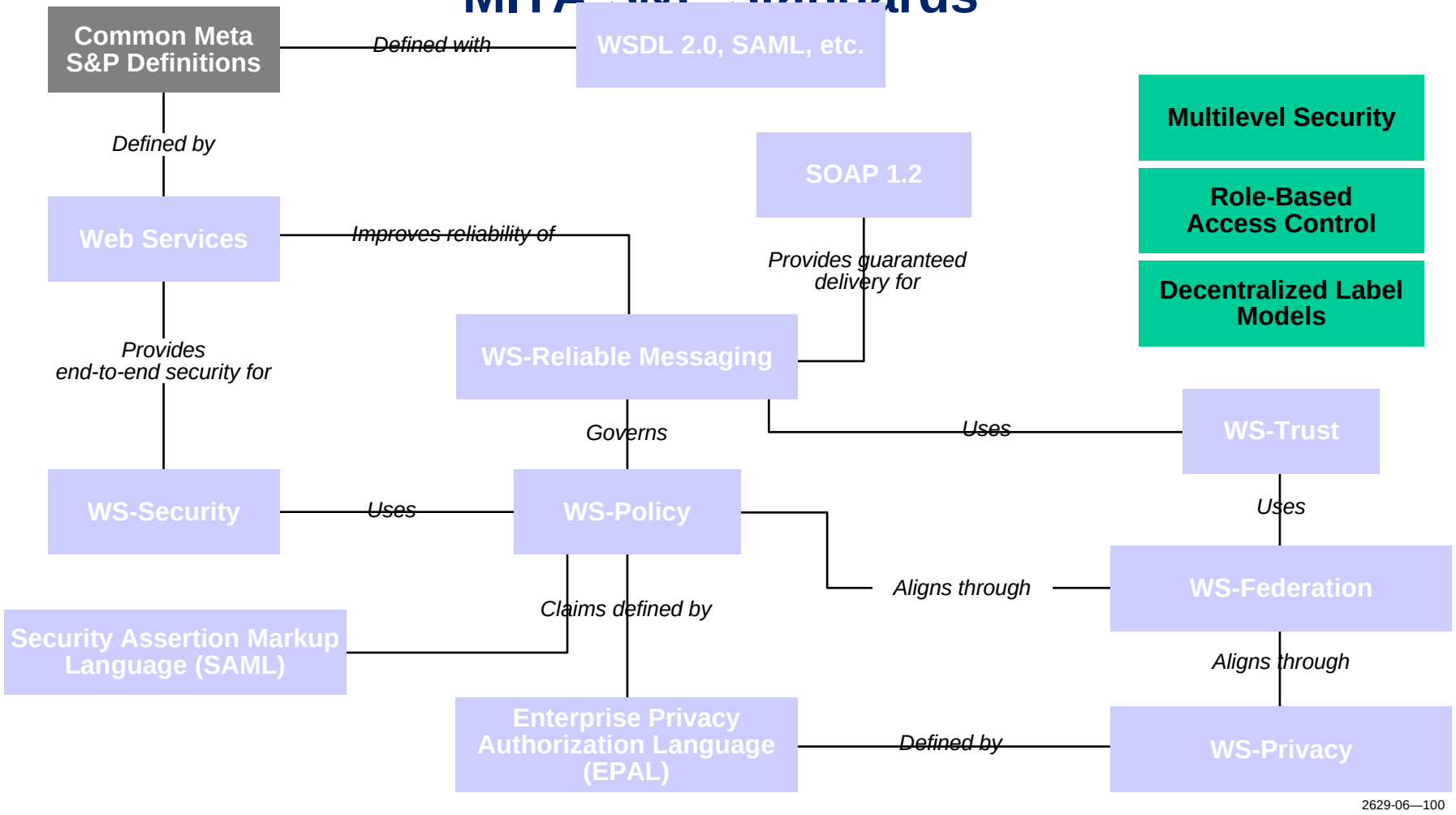


Aligning S&P and Strategy Architecture

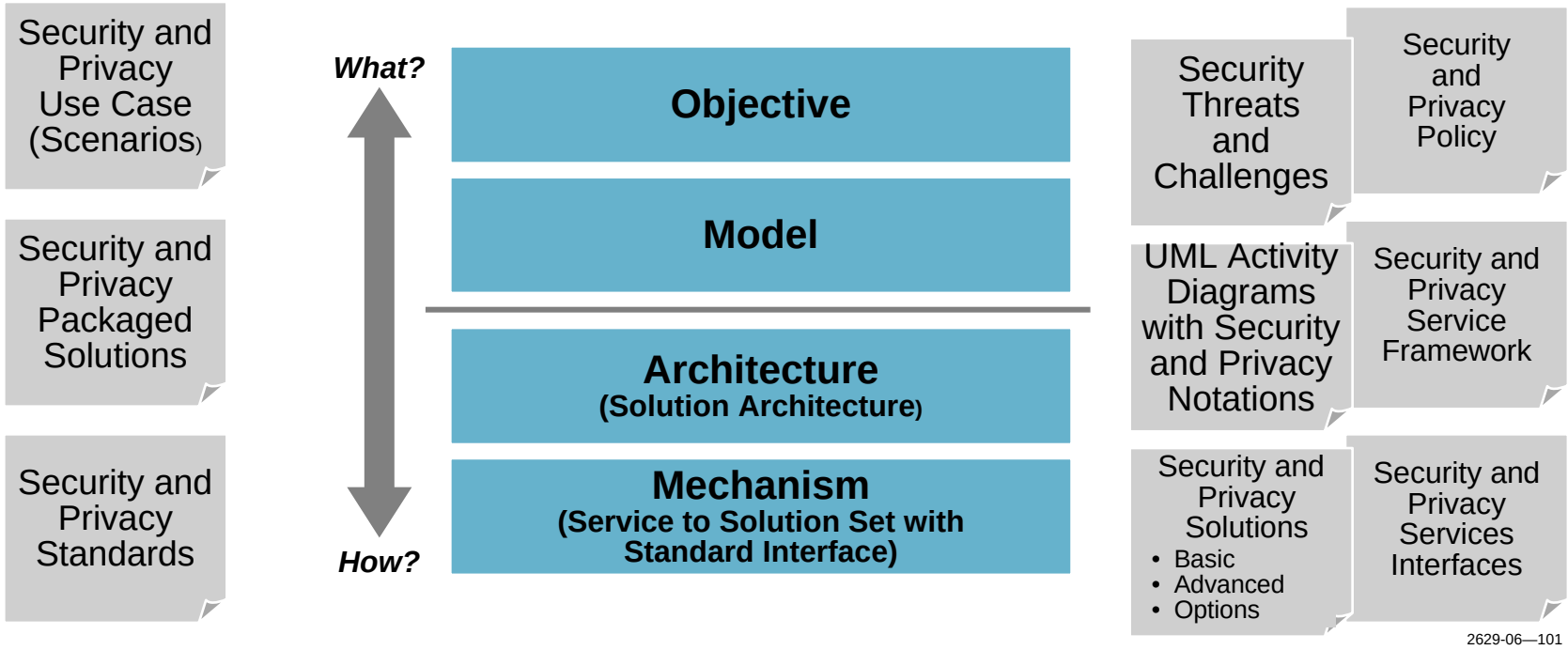


2629-06—099

MITA S&P Standards

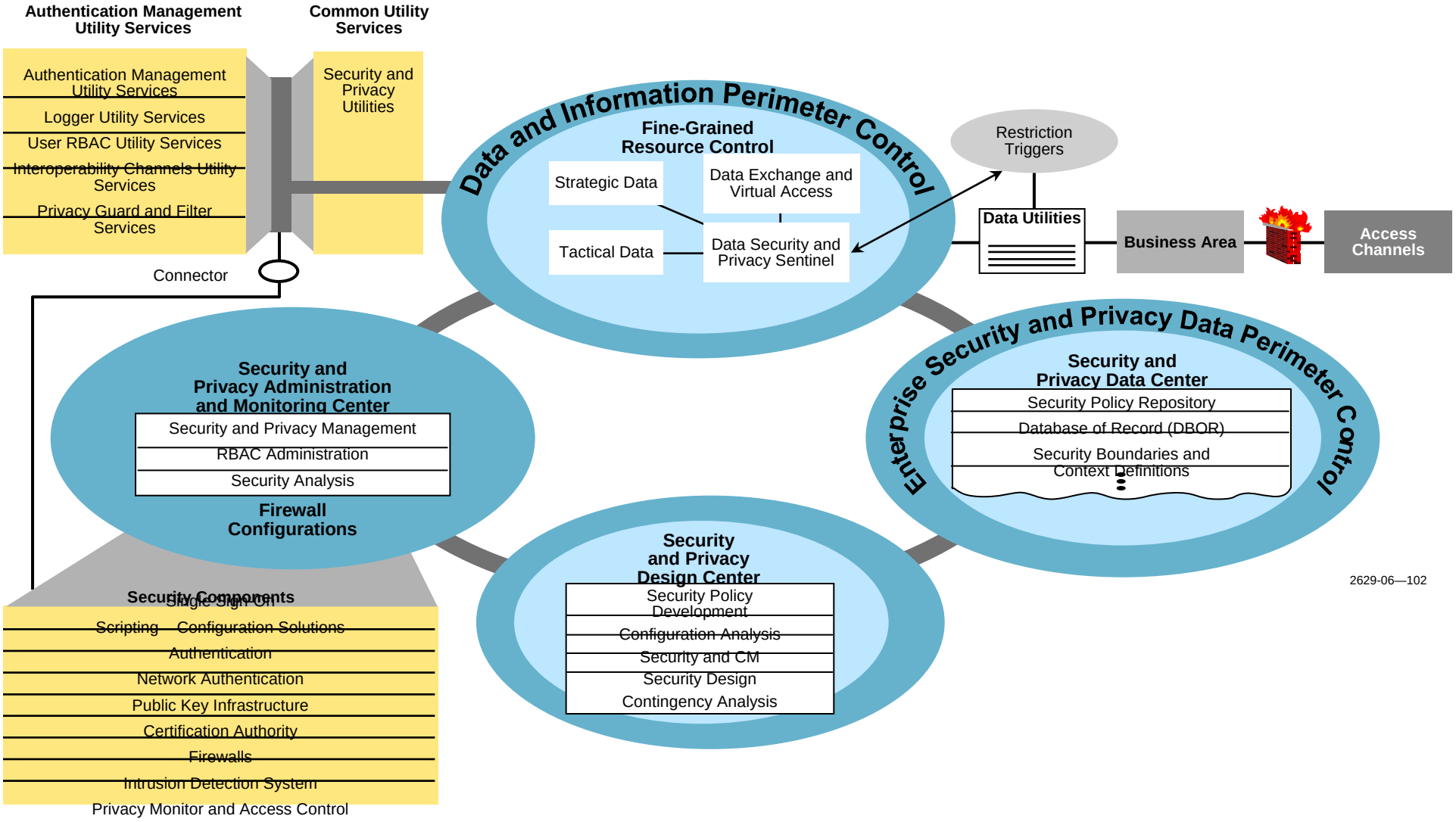


S&P and the OM-AM Model



OM-AM Framework Becomes Actionable with Structure Information

S&P Goals and Policies



Security and Privacy Utility Services, Features and Connections to Related Components

S&P Utility Service	Features
Authentication Management Utility Services	Passes the business area, user/State identification, and responsible security and development person to the authentication component
Logger Utility Services	Provides a consistent approach to logging information Provides controls that can increase or decrease logging levels
User RBAC Utility Services	Connects roles to business areas, users who requested services, and context the user works in
Interoperability Channels Utility Services	Each interoperability channel and access channel will have rights of access defined. These functions will be mapped to the RBAC utilities.
Privacy Guard and Filter Services	Certain data and information will have specific additional privacy and filtering services because of their value.

Security and Privacy Data and Information Subject Area Model

Security Policy Repository	Security Boundaries and Context Definitions
Security Configuration Repository, Security and Privacy Components, Connectors, Utilities, and Configuratic Models	User Role Access Rights Repository
Application Asset Security Model	Data and Information Asset Model, Databases of Record, Meta Record Index, and Recovery Process Models
Threat Repository	Vulnerability Repository
Security and Policy Process and Procedures	
Security and Privacy Patterns	
Disclosure Reporting	Privacy Suspension Records
Beneficiary Privacy Action	Security Issue Tracking

2629-06—103

Medicaid Information Technology Architecture

Security and Privacy Q & A

Question	Answer
Why is the S&P model important to MITA?	The S&P model shows a consistent way of implementing security across the network. Key concepts are single sign-on/log-in, use of standards, and a wide range of security components.
Who should understand the S&P model?	Designers and implementers of systems and networks should review the model to ensure that it has addressed all appropriate levels of security.
How will the S&P model be used?	The S&P model offers many implementation options. System designers and implementers should review it and select components appropriate for data sharing and for access needed to meet business needs.
How will the S&P model be refined and updated?	The S&P Portfolio team will update the S&P model. Further details, including detailed specifications and minimum-security requirements, will be provided in coming years.
How will the S&P model support ongoing business decision making?	New IT procurements should specify the appropriate security components to support data sharing.