

# Securing the Digital Enterprise using Open Standards for Zero Trust

John Linford, The Open Group

[J.Linford@opengroup.org](mailto:J.Linford@opengroup.org)

<https://www.linkedin.com/in/johndouglaslinford/>

# Who I Am

## The Open Group

- Global consortium that enables the achievement of business objectives through technology standards
- Boundaryless Information Flow™ achieved through global interoperability in a secure, reliable and timely manner








## John Linford

- Security Portfolio Forum Director, responsible for facilitating creation of standards and certification programs
- Manage Security Forum, Open Trusted Technology Forum, and Assured Dependability Work Group

## Zero Trust Key Drivers

## Zero Trust Objectives

## Zero Trust Key Requirements

|  |  |  |
|--|--|--|
|  <b>Evolving Business Models</b>                      |  <b>Dynamic User Identity</b>                     |  <b>Exponentially Increasing Need for Agility</b>                   |
|  <b>Evolving Threat Landscape</b>                     |  <b>Threat Scope Reduction and Risk Avoidance</b> |  <b>Increasing Complexity Requiring Increasing Need to Simplify</b> |
|  <b>Emerging Partnerships</b>                         |  <b>Context-Specific, Policy-Enforced Data</b>    |  <b>Support for Remote Work</b>                                     |
|  <b>Rapidly Changing Technology</b>                   |  <b>Separation of Concerns</b>                    |  <b>Regulatory Requirements</b>                                     |
|  <b>Regulatory, Geopolitical, and Cultural Forces</b> |  <b>Real-Time / Near Real-Time Response</b>       |  <b>Support for Unpredictability</b>                                |
|  <b>Disruptive Events</b>                             |  <b>Automated Audit</b>                           |  <b>Real-Time / Near Real-Time Response</b>                         |
|  <b>Supporting Remote Work</b>                      |  <b>Policy-Driven Access Control</b>              |  <b>Measurable Controls and Automated Audit</b>                   |
|  |  <b>Secured Zones</b>                           |  |

# Zero Trust & ZTA

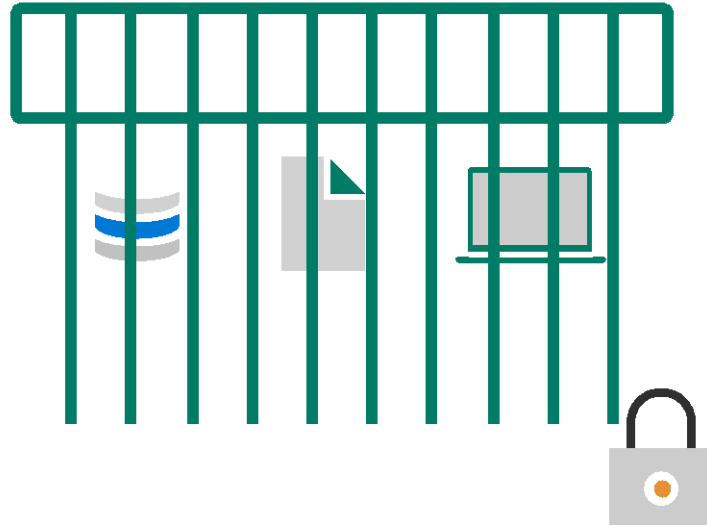
Zero Trust builds on work done by the Jericho Forum® that describes the breakdown of the perimeter security model

- Perimeter-based approaches built on legacy models of identity, authentication, and authorization do not meet the need of a digital business environment
- Zero Trust approaches are based on asset or data-centric security, policy-driven access controls, modern identity management, and secured zones

*Zero Trust brings security to the users, data/information, applications, APIs, devices, networks, cloud, etc. wherever they are – instead of forcing them onto a “secure” network.*

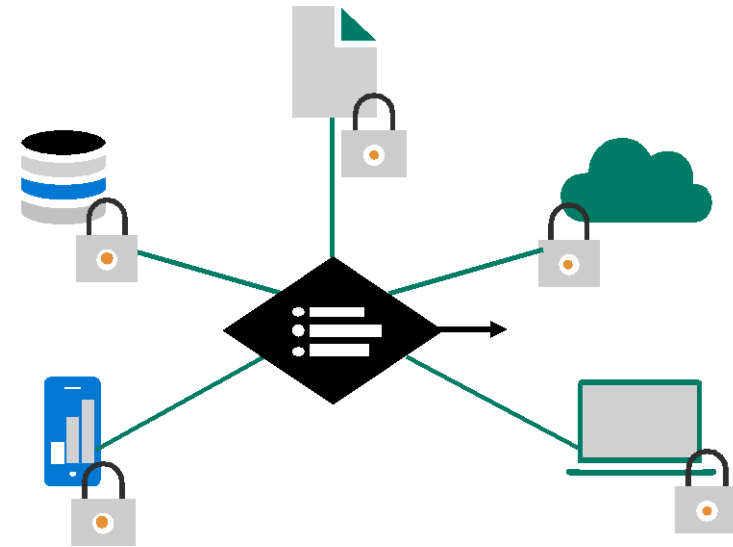
# Secure Assets where they are with Zero Trust

Simplify security and make it more effective



## Classic Approach

Restrict everything to a 'secure' network



## Zero Trust

Protect assets anywhere with central policy

# Zero Trust & ZTA

- **Zero Trust** – an information security approach that focuses on data/information security, including lifecycle, on any platform or network
- **Zero Trust Architecture** – the implementation of a Zero Trust security strategy that follows well-defined and assured standards, technical patterns, and guidance for organizations

# Foundation for Zero Trust

- Assume Failure and Assume Success
  - Anything can go wrong – users will forget or make mistakes; attackers will succeed in gaining control of data and computer systems (in part or as a whole); and trusted insiders will occasionally go bad.
  - The mission and business must and will continue despite any failures that can and will happen: many attacks can be blocked; people will overcome obstacles and learn; systems can be cleaned, restored, or rebuilt – business operations and the mission will continue.
- Advocate for Simplicity
  - Security teams must advocate for simplicity as a means of reducing business risk while the organization undergoes digital, cloud, and Zero Trust transformations.
- View as a Continuous Journey
  - All transformations require investment into change, and Zero Trust ultimately represents a change in strategy or perception of security, ensuring continuous enablement of business objectives while managing risk.

# Zero Trust Commandments

## Practice Deliberate Security

### Secure Assets by Risk

Security controls shall be designed to protect business assets appropriate to required security posture, business value, and associated risk.

### Validate Trust Explicitly

Security assurance shall rely on explicitly validating trust decisions using all relevant available information and telemetry.

## Support Business Objectives

### Enable Modern Work

Security discipline shall enable productivity and manage risk as the organizational capabilities, goals, environment, and infrastructure continuously evolve.

### Implement Asset-Centric Controls

Asset-specific security controls shall be implemented whenever available to minimize disruption of productivity, increase precision of security/business visibility, and improve data used to drive security compliance metrics.

### Enable Sustainable Security

Security controls shall be sustainable across the full lifecycle of the business asset.

## Develop a Security-Centric Culture

### Practice Accountability

The entities responsible for accessing and handling assets shall be responsible for their protection and survival throughout their lifetime.

### Enable Pervasive Security

Security discipline shall be explicitly included in the culture, norms, and processes throughout the organization.

### Utilize Least Privilege

Access to systems and data shall be provided only as required, and access shall be removed when no longer required.

### Deploy Simple Security

Security mechanisms shall be as simple as possible while retaining functionality and remaining pervasive, practicable, and scalable.

## Deploy Agile and Adaptive Security

### Make Informed Decisions

Security teams shall make decisions based on the best available information.

### Improve and Evolve Security Controls

Security teams shall continuously evolve and improve to remain successful in an environment that constantly changes.

### Utilize Defense in Depth

Security mechanisms and controls shall be layered to enhance resilience and preserve integrity.

### Enable Resiliency

Security systems shall ensure the organization can operate normally under adverse conditions.



# Secure Assets by Organizational Risk

Security controls shall be designed to protect business assets appropriate to required security posture, business value, and associated risk.

- **Map Technology to Business** – The organization must identify important business assets and translate them into the technical assets that compose them, including consideration of systems with direct administrative control.
- **Classify Information Assets** – Organizations should classify mission-critical assets that drive certain business processes (e.g., for insurance companies, a business process can be life insurance, health, savings, retirements, etc.) essential to meeting end-client business objectives. The classification of assets will support arriving at Confidentiality, Integrity, and Availability (CIA) ratings.
- **Increase Security for Sensitive Assets** – Security controls must match asset value and sensitivity to ensure the protection of high-value data and applications.
- **Reduce Unneeded Sensitivity** – The organization must reduce asset sensitivity where possible to avoid wasting efforts of security and other teams (e.g., retire or replace unneeded sensitive assets, remove sensitive or regulated data with low-value tokens, etc.).
- **Stay Current** – The organization must update security assurances for the asset (CIA, safety) as the asset use-cases, threats, and value change over time.

# Practice Accountability

The entities responsible for accessing and handling assets shall be responsible for their protection and survival throughout their lifetime.

- **Assign Asset Ownership** – Assets must have clear owners who are responsible for them.
- **Ensure Understanding of Ownership** – Asset owners must have a clear understanding of assets under their control, and the implications of failing to adequately protect them.
- **Define Security Impact Correctly** – Security risk definitions must consider the systemic and infectious nature of security risk, where any attack can result in organization-wide risk.
- **Assign Security Risk to Organizational Leadership** – Security risk represents organizational risk that must be managed, delegated, and accepted like any other risk; the security organization must act as subject matter experts to advise organizational leadership on security risk.
- **Assign Security Risk to Asset Owners** – The organization must assign responsibility for mitigating security risk to business asset owners, like all other risks. Security teams must act as subject matter experts to advise asset owners on security risk.

# Enable Pervasive Security

Security discipline shall be explicitly included in the culture, norms, and processes throughout the organization.

- **Integrate in Business Environment** – The organization must integrate security context into business strategy, planning, operations, acquisition, contracting, and outsourcing.
- **Integrate in Technical Environment** – The organization must integrate security controls into workflows, application and solution architectures, migrations to hybrid-cloud and cloud environments, new application development, Artificial Intelligence (AI) and Machine Learning (ML) projects, implementation of Agile practices, and other emerging technologies.
- **Incorporate Security Education and Awareness Training** – The organization must regularly provide Zero Trust security education and awareness training for employees as well as partners, contractors, and suppliers as appropriate; the organization must also verify that relevant external personnel have equivalent training as appropriate.
- **Apply Security to the Organization's Ecosystem** – The organization's security requirements must apply to the employees and assets of the organization and the full supply chain and value chain of the organization, including other entities (e.g., partners, contractors, suppliers, and sometimes customers). This should be done through all reasonable controls on a regular basis in a verifiable manner; associated non-compliance should be monitored, reported, and addressed appropriately.

# Enable Resiliency

Security systems shall ensure the organization can operate normally under adverse conditions.

- **Anticipate Attacks** – Before a security incident, the organization must implement controls that limit the likelihood and magnitude of security incident impact on business operations.
- **Withstand Attacks** – During a security incident, the organization must ensure organizational readiness to rapidly remediate the attack, limit the impact of the attack (i.e., minimize the blast radius), and ensure continuity of critical business operations.
- **Recover from Attacks** – Before an attack, the organization must also ensure that data and associated security elements can be restored in case of technical or major failure; after a security incident, the organization must ensure all impacted business capabilities and services are rapidly restored to operational status.
- **Adapt to Adverse Conditions** – The organization must ensure that lessons learned are continuously documented and integrated into designs and operations.

**Mission and Vision**

**Business Assets**  
*Data and Systems*

**Zero Trust Risk Model**  
*Evaluate Risk and Prioritize/Plan Mitigations*



**Threats**

**Zero Trust Implementation Model (3 Pillar Model)**  
*Strategy, Implementation, Governance and Change Management*

**Zero Trust Capabilities, Roadmap, and Operating Model**

**Zero Trust Information Security Management (ISM) Model**  
*Manage information security risks to the organization*

**Zero Trust Technology Reference Model**  
*Capabilities and Architectural Building Blocks (ABBs) covering Architecture, Operations, Governance*

**Enterprise Solution Architecture**

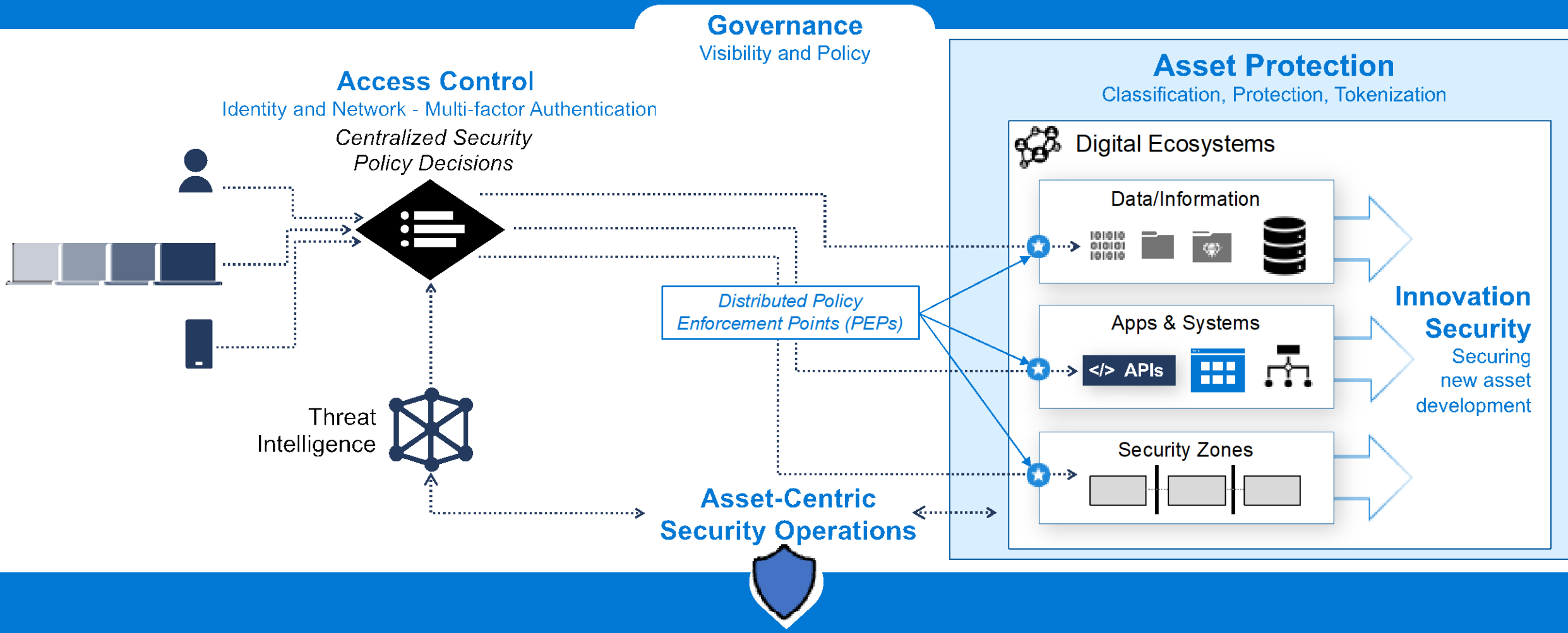
**Information Security Management (ISM)**  
*People, Policy, and Processes*

**Architecture Building Blocks (ABBs)**  
*Technical Capabilities*

**Design/Build**      **Run/Operate**

# Zero Trust Components

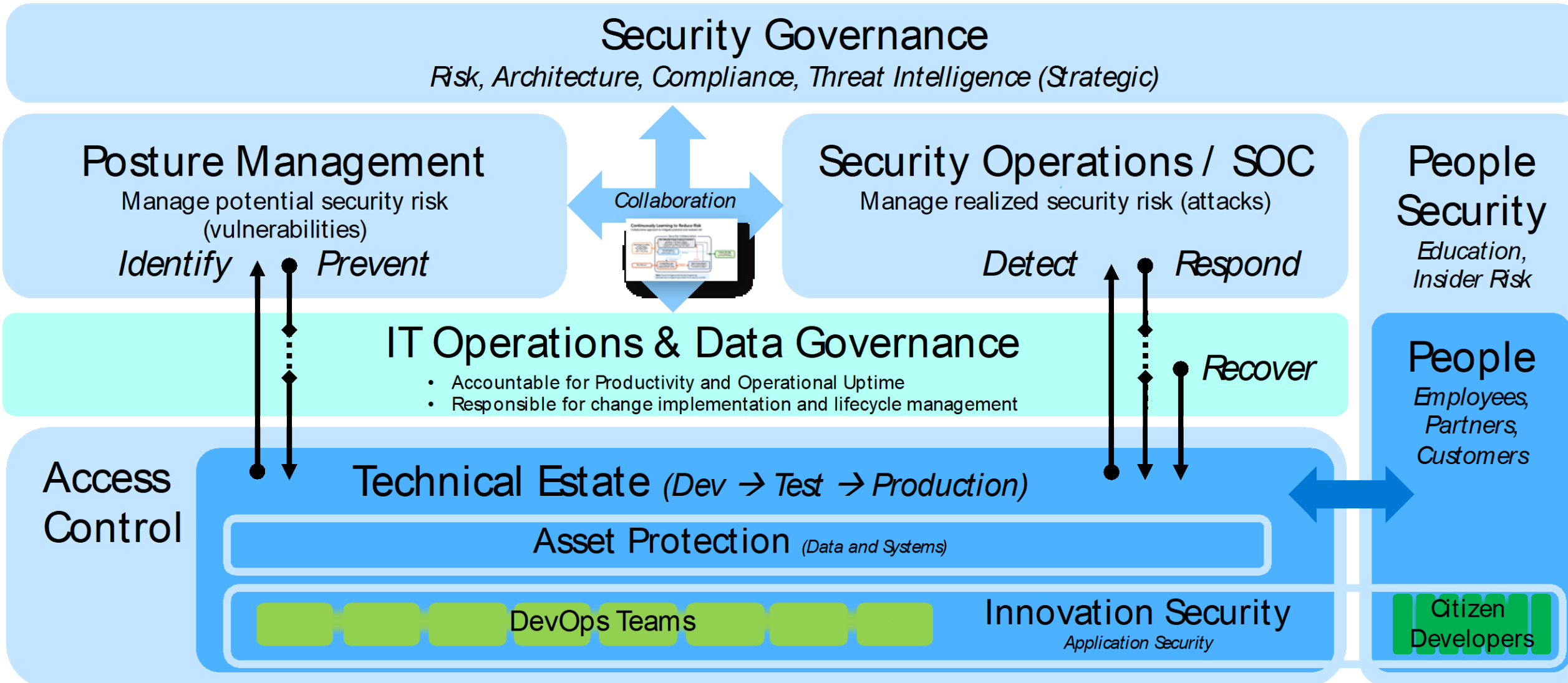
Clarity, Automation, and Metrics-Driven Approach



Rapid Threat Detection, Response, and Recovery



# Security Operating Model



# Call to Action

## The Open Group

- Zero Trust Commandments
- Zero Trust Reference Model
- Zero Trust Implementation Process Guide

## NIST

- NCCoE Zero Trust Architecture Project

## CISA

- Zero Trust Maturity Model

Join the Efforts  
to Refine and  
Finalize  
Standards for  
Zero Trust

John Linford, The Open Group

[J.Linford@opengroup.org](mailto:J.Linford@opengroup.org)

<https://www.linkedin.com/in/johndouglaslinford/>

