proarch

# FROM CHECKBOX COMPLIANCE TO HOLISTIC SECURITY

# Who we are

the proarch companies

proarch

iV4
a proarch company

We accelerate value and increase resilience for our clients with consulting and technology - enabled by cloud, guided by data, fueled by apps, and secured by design.

- Cloud
- Security
- Consulting
- Data & AI
- Application Development
- Managed IT Solutions

Atlanta, GA
Syracuse, NY
Rochester, NY
Buffalo, NY

London, UK
Hyderabad, India
Bangalore, India
Singapore

# Presenter

## Michael Montagliano, Chief Technology Officer

Certified Information System Security Professional (CISSP)

# Compliance is One Step above Negligence

# A False Sense of Security

Another year and another audit passed!

This can bring great relief and mark the end to a very stressful time period.

The basic question of “are we secure?” should remain even after the auditor has left.

Auditors do not have the time nor the ability to inspect each asset and system to verify all controls are in place and functioning as intended.

Security is an on-going effort built into every aspect of information technology.

# Definitions

Compliance focuses on the kind of data handled and stored by a company and what regulatory requirements (frameworks) apply to its protection.

- Compliance means ensuring an organization is complying to the minimum of security-related requirements at a point in time
- A company may have to align with multiple frameworks.
- Dictate policies, regulations, and laws and cover physical, financial, legal, or other types of risk.
- It can be multifaceted and is based on a company's data type and security processes.

Security is a clear set of technical systems and tools and processes which are put in place to protect and defend the information and technology assets of an enterprise.

- Compliance is not the primary concern or prerogative of a security team, despite being a critical business requirement.
- It can include technical and physical controls, for example, who has access to a network or the building
- Standardized methods and tools provided by specialist vendors make security simpler than compliance.

# What are the differences? Why are they necessary?

**Compliance**

- Regulatory Frameworks
- Risks
- Policies
- Documentation
- Standards

Is practiced to satisfy external requirements and facilitate business operations

Is driven by business needs rather than technical needs

Is "done" when the third party is satisfied

**Security**

- Physical Controls
- Authentic Mechanisms
- Business Processes
- Network Access
- Secure IT Environment

Is practiced for its own sake, not to satisfy a third party's needs

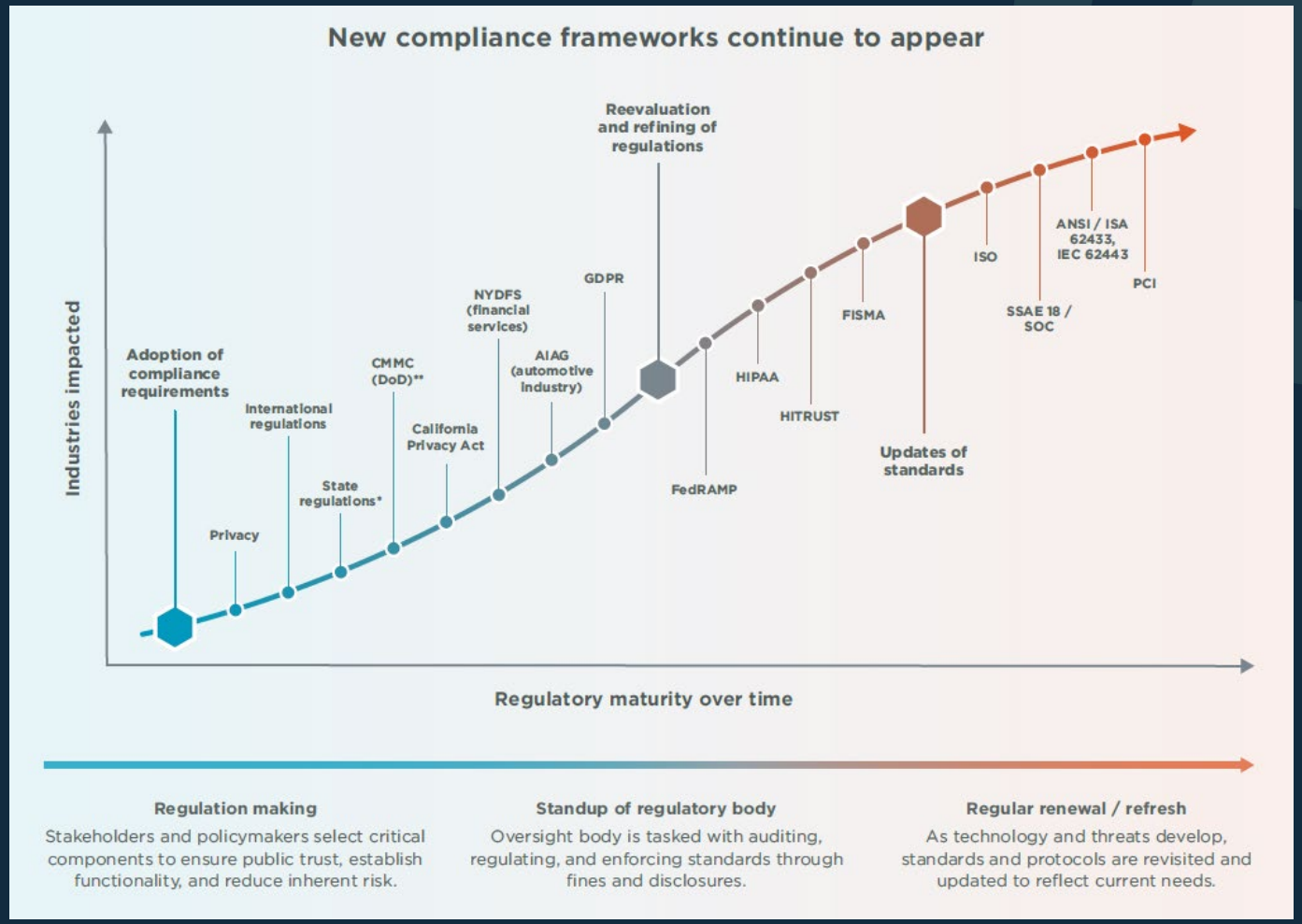
Is driven by the need to protect against constant threats to an organization's assets

Is never truly finished and should be continuously maintained and improved

# Current State of Compliance

**Internal Obstacles**

- Lack of or burnt-out resources
- Poor alignment with a broader cybersecurity program
- Unforgiving reporting schedules
- Differing and sometimes contradictory requirements
- Loosely related compliance obligations and partially mapped controls



# Regulatory Obligation vs. Control Framework

## Regulatory Compliance

- NY Department of Financial Services Cyber Security Regulation (23 NYCRR 500)
- NYS SHIELD Act (NYS 899-bb)
- NYS Department of Health Office of Insurance Programs (OHIP) SSP v.3.1
- NY Education Law 2d and Part 121
- Health Insurance Portability and Accountability Act (HIPAA), Parts C and D
- Defense Federal Acquisition Regulations (DFARS) 204.73
- Cyber Security Maturity Model Certification (CMMC)
- North American Electric Reliability Corporation (NERC) CIP
- GDPR, The General Data Protection Regulation (EU) 2016/679

If your network stores, processes, or transmits any of the regulated data falling under the regulation, you MUST comply with all controls

## Security Control Frameworks

- NIST SP 800-53 rev5
- NIST Cyber-Security Framework (CSF)
- NIST 1800-23: Energy Sector Asset Management: For Electric Utilities, Oil & Gas
- 20 Critical Controls
- ISO 27001

Tailor control implementation to organization's identification of risk

# Regulatory Compliance: Is the floor, not the ceiling

Compliance regulations address the minimum-security requirements.

The intent of compliance requirements was to never prescribe a set of actions and policies that would guarantee 100% security and protection.

*A 2011 Government Accountability Office Report to Congress states that the: "…focus [is] on achieving minimum regulatory requirements rather than designing a comprehensive approach to system security."

# Compliance: Not Applicable; therefore, no security is needed?

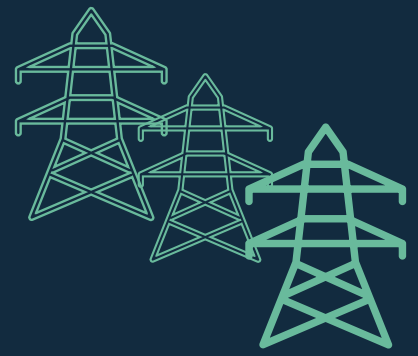
Regulatory standards that require the implementation of protective cybersecurity measures and controls do not apply to all cyber assets.

Only applies to assets that process, store, or transmit regulated data. This does not consider the impact on non-regulated assets.

One side-effect of drawing compliance boundaries is the assumption/misconception that no security is needed for the non-applicable assets.

80-90% or more of the electric infrastructure currently does not fall under any required standards and cybersecurity practices

California Public Utilities Commission "Cybersecurity and the Evolving Role of State Regulation"



# No Longer an ‘IT’ Concern

The goals of both security and compliance, comes down to:

**RISK.**

Compliance + Security + IT = Managing Risk

- A security team lives in the world of technology, a compliance team lives in the world of text.
- A security team is tasked with implementing controls, a compliance team is responsible for ensuring those same controls are implemented.
- Both teams report up to management teams responsible for due diligence and due care.

# Compliance Does Not Guarantee Security

# Energy Industry Cyber-Attack

- In December of 2015, first successful cyber-attack on nation's power grid.
- Allowed malicious actors to turn off power to ~225,000 paying customer.
- Some assets compromised were not classified as critical cyber assets under compliance standards and therefore required no protection under NERC CIP
- $1.7 million penalty on an entity for violating multiple requirements designed to protect cyber assets.

# Energy Critical Infrastructure Protection Standards

## Power Plant Ratings

### High Impact

- Generation equal to or greater than an aggregate of 3000 MW in a single Interconnection
- Control Center or backup Control Center as required by ERO (Electric Reliability Organization).

### Medium Impact

- 1500 MW in a single Interconnection.
- Could, within 15 minutes, adversely impact the reliable operation.
- Transmission Facilities operated at 500 kV or higher.

### Low Impact

- BES systems which do not meet High or Medium standards
- Special Protection Systems that support the reliable operation of BES

# Energy Critical Infrastructure Protection Standards

| Version 6 | Impact Level | Standard Name |
|---|---|---|
| CIP-002-5-1 | Low | BES Cyber System Categorization |
| CIP-003-6 | Low | Security Management Controls |
| CIP-004-6 | Medium\High | Personnel & Training |
| CIP-005-5 | Medium\High | Electronic Security Perimeter(s) |
| CIP-006-6 | Medium\High | Physical Security of BES Cyber Systems |
| CIP-007-6 | Medium\High | System Security Management |
| CIP-008-5 | Medium\High | Incident Reporting and Response Planning |
| CIP-009-6 | Medium\High | Recovery Plans for BES Cyber Systems |
| CIP-010-2 | Medium\High | Configuration Change Management and Vulnerability Assessments |
| CIP-011-2 | Medium\High | Information Protection |
| CIP-014-2 | Medium\High | Physical Security |

# Elements of a Holistic Security & Compliance Strategy

# Compliance AND Security Control Cycle

**CATEGORIZE**
**Information System**

Define criticality /sensitivity of information system according to potential impact of loss

**SELECT Security Controls**

Select baseline (minimum) security controls to protect the information system; apply tailoring guidance as appropriate

**SUPPLEMENT**
**Security Controls**

Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence

**DOCUMENT**
**Security Controls**

Document in the security plan, the security requirements for the information system and the security controls planned or in place

**IMPLEMENT**
**Security Controls**

Implement security controls; apply security configuration settings

**ASSESS**
**Security Controls**

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)

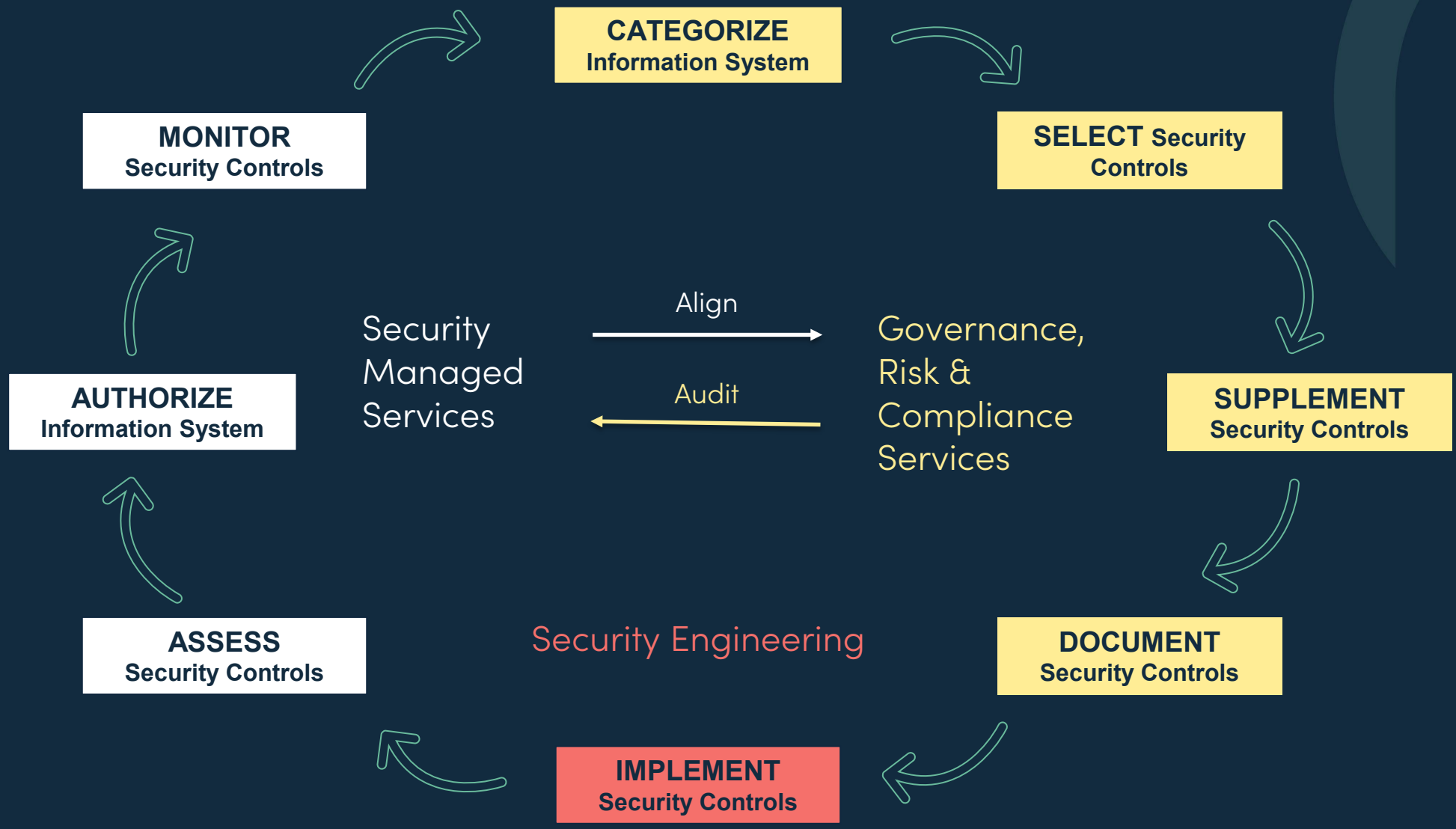
**AUTHORIZE**
**Information System**

Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation

**MONITOR**
**Security Controls**

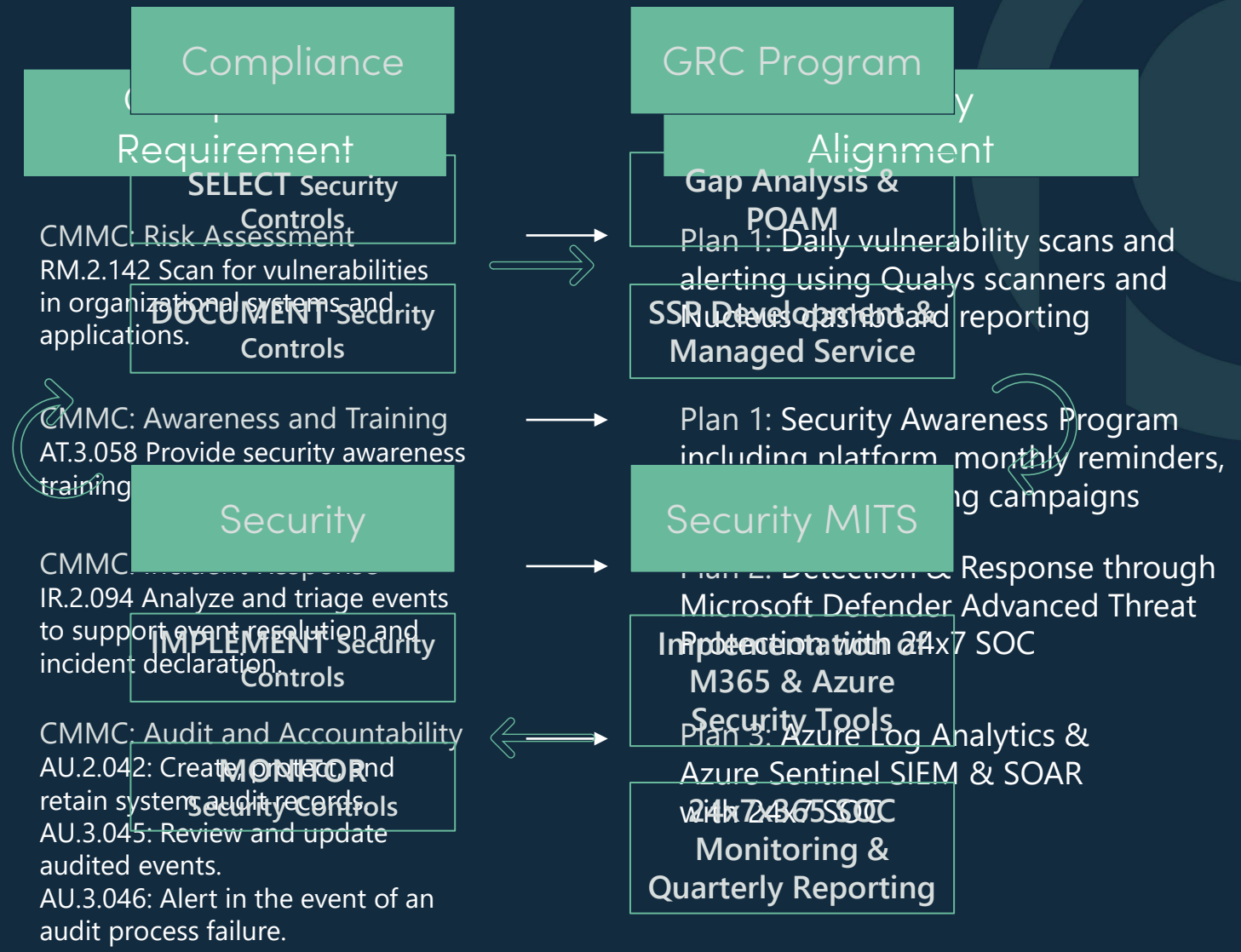
Continuously track changes to the information system that may affect security controls and reassess control effectiveness

# ProArch Security Program Alignment



# Aligning Security & Compliance:

## How ProArch Does It



# Components of Effective Risk Program

## Security

| |
|---|
| Vulnerability Management |
| Security Awareness Training and Phishing Tests |
| Microsoft Office 365 Advanced Threat Protection (email security) |
| Microsoft 365 Security Hardening |
| Incident Response Services |
| Security Information and Event Management (SIEM) |
| Secure Web Content Filtering |
| Microsoft Defender for Endpoint (Microsoft Defender Advanced Threat Protection) |
| Azure Advanced Threat Protection |
| Cloud Identity and Access Management |
| 24x7 Security Operations Center |

## Governance, Risk & Compliance

| |
|---|
| Compliance Gap Analysis |
| System Security Plan Development (documented policies and procedures) |
| On-going System Security Plan Development Maintenance and Updates |

# Aligning Security & Compliance

# Rethinking Compliance Strategy

**Cyber standards are changing dramatically** from checkbox mentality to perpetual compliance integration into overall security programs, business processes and outcomes.

**As cloud adoption continues to grow**, organizations must look at their own compliance efforts and take steps to meet the required guidelines

**Meet budget restraints with compliance coordination** across frameworks to administrative overhead and scope.

Consistently evaluating security controls has become critical to ensuring **even the most basic security posture**

# Business Impacts of Compliance Transformation

## Compliance as a sales driver

Turning compliance from a cost center into a market differentiator provides sales leaders another asset in competitive markets

## Measurable risk reduction

Greater visibility into security posture, helping identify and manage risks

## Demonstrated savings

Reduction in total cost of compliance (audit fees and internal resource costs)

## Resource efficiency

Availability of current resources beyond compliance to support other business initiatives

67% of companies use **compliance** as a marketing differentiator.

49% of companies use **security** as a marketing differentiator.

# Compliance & Security Roadmap

| | |
|---|---|
| **Understand your regulatory requirements** | seek legal advice |
| **Know where regulated data is stored** | System Categorization/ FIPS199 |
| **Studying the requirements related to the framework** | Gap Analysis |
| **Analyzing the gaps in your current controls regarding the requirements** | |
| **Planning the way forward to solve major deficiencies** | Plan Of Action & Milestone (POAM) |
| **Document policies and procedures** | System Security Plan |
| **Implement security tools and processes based on POAM** | |

After applying these steps conducting regular assessments or continuous monitoring is the key to success.

Compliance and security need to work hand in hand; it does not have to be security versus compliance.

They work in unison; Using a compliance framework, assessing security systems, correcting deficiencies, and then beginning assessments which are set on a regular schedule.