OHIO GFOA

38th Annual Conference & Membership Meeting

September 17-19, 2025 – Columbus, OH

rea

Under the Cybersecurity Microscope: Auditor's Look Deeper into Cyber Events

By: Travis Strong

Travis Strong, CISA, CMMC-RP

Principal

Travis.Strong@reamanaged.com

www.linkedin.com/in/travis-strong-cisa

Travis is a Principal with Rea Information Services. Travis' 18-year career has focused on IT risk management and cybersecurity for organizations.

Agenda

Why cybersecurity matters to you

Top 5 cyber threats

An auditor’s lens in cybersecurity

Ohio’s cybersecurity law

Practical takeaways

Questions

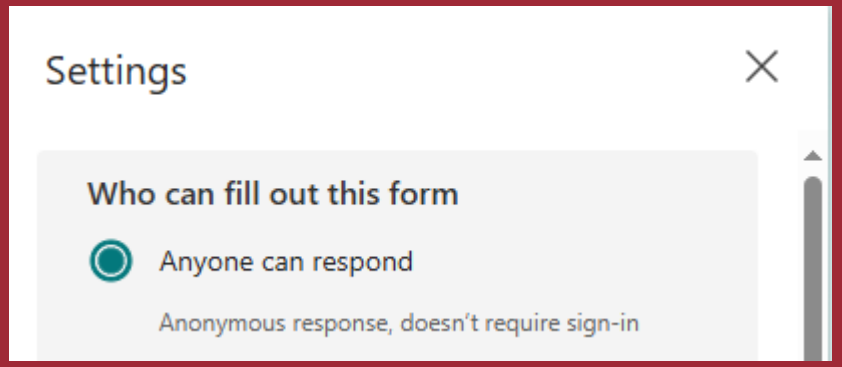
2025 Ohio GFOA - Poll question #1

https://forms.office.com/r/htjJqNnWZt

Poll #1

What concerns you most about cybersecurity in your organization?

Completely anonymous – I do not capture anything about you



Why cybersecurity matters for you

Why cybersecurity matters for you

Cyber attacks are financial events:

- operational disruptions
- ransom demands
- reputational damage

Why cybersecurity matters for you

Public entities are increasingly targeted:

- budget, staff, or skill constraints
- outdated, legacy systems
- critical services & valuable data

Why cybersecurity matters for you

Finance officers are on the front-line:

- risk & compliance
- incident response
- funding

Top 5 cyber threats

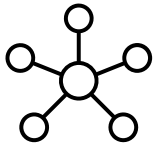
CYBER THREAT LANDSCAPE

Business email compromise

- Vendor changes; impersonations
- Artificial intelligence is making it more difficult

Ransomware attacks

- Remains one of the most prevalent threats
- Double-extortion tactics
- Outdated systems, weak passwords, flat networks

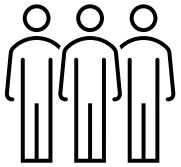


3rd parties, cloud & supply chain security

- Reliance on 3rd parties expands the threat landscape
- Attack surface expands beyond your four walls
- An attack of one party can impact another party

Phishing & social engineering

- Phishing remains a leading attack vector
- Attackers use social engineering to trick users



Insider threats

- Malicious or accidental actions; manipulation
- Individuals may obtain, leak, or misuse sensitive data
- Excessive/outdated permissions; onboarding/offboarding

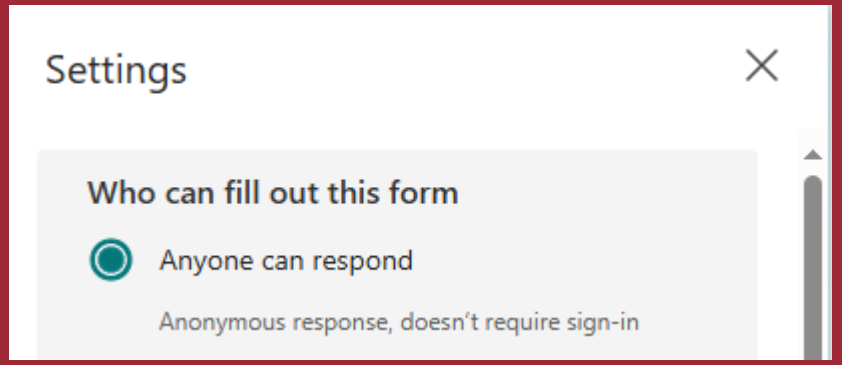
2025 Ohio GFOA - Poll question #2

https://forms.office.com/r/v99GpRid4C

Poll #2

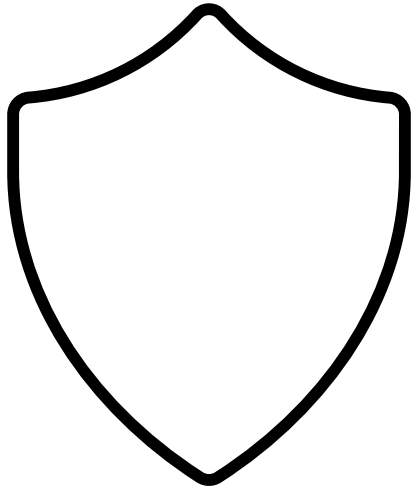
How confident are you in your organization's ability to detect and respond to a cyber incident?

Completely anonymous – I do not capture anything about you

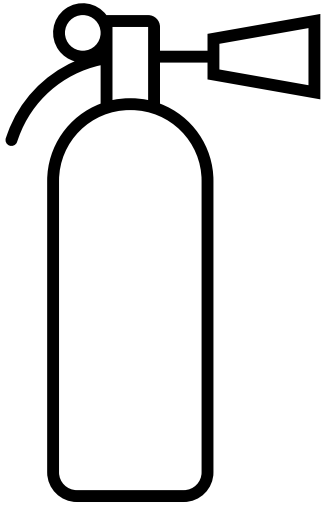


An auditor’s lens in cybersecurity

Cybersecurity mindset



Proactive = Preventive



Reactive = Responsive

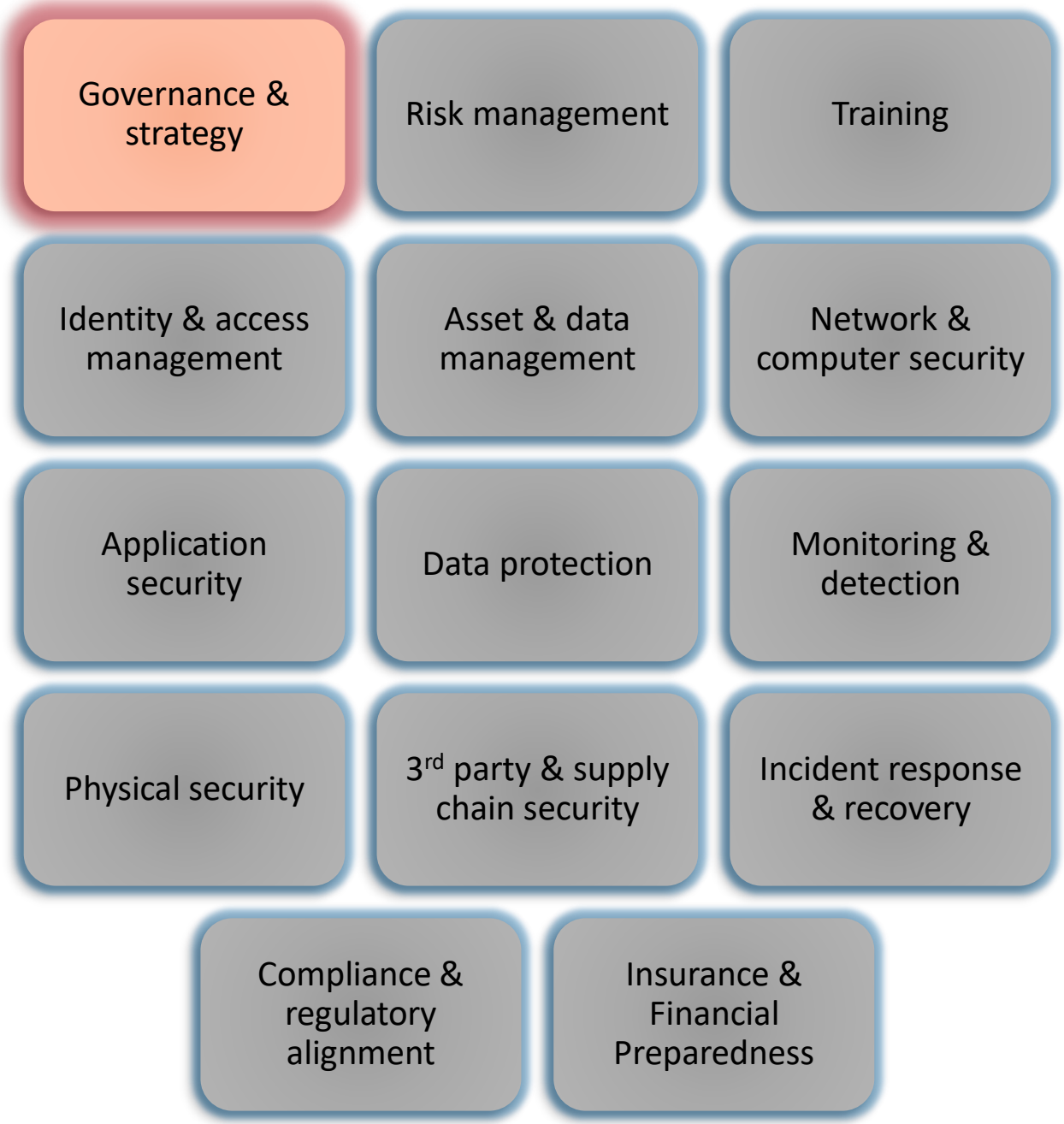
Do we lock our doors to prevent a break-in or only after a break-in has occurred?

What is a cybersecurity program?

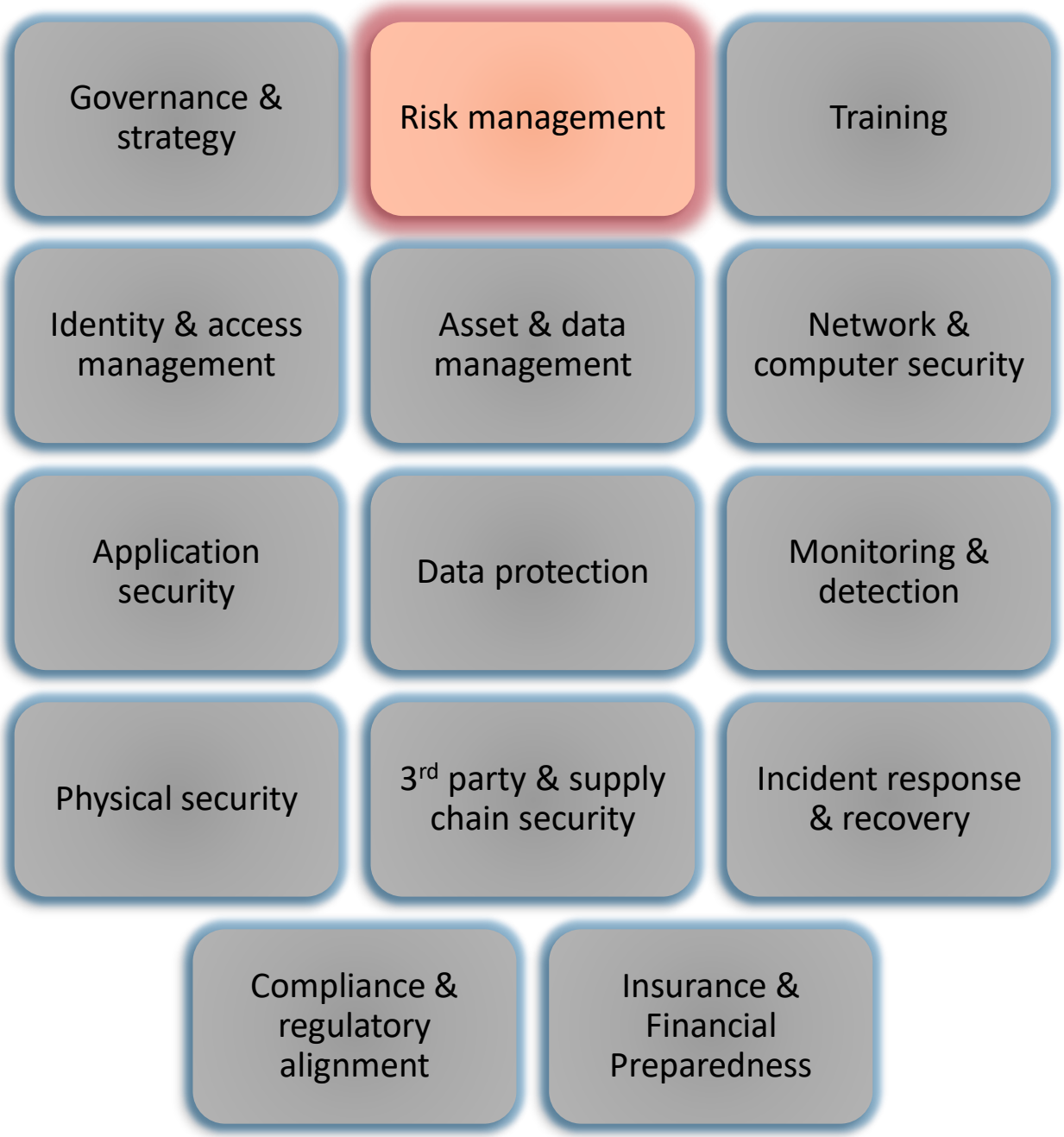
Ongoing activities to safeguard data, IT, and IT resources

Supports confidentiality, integrity, and availability

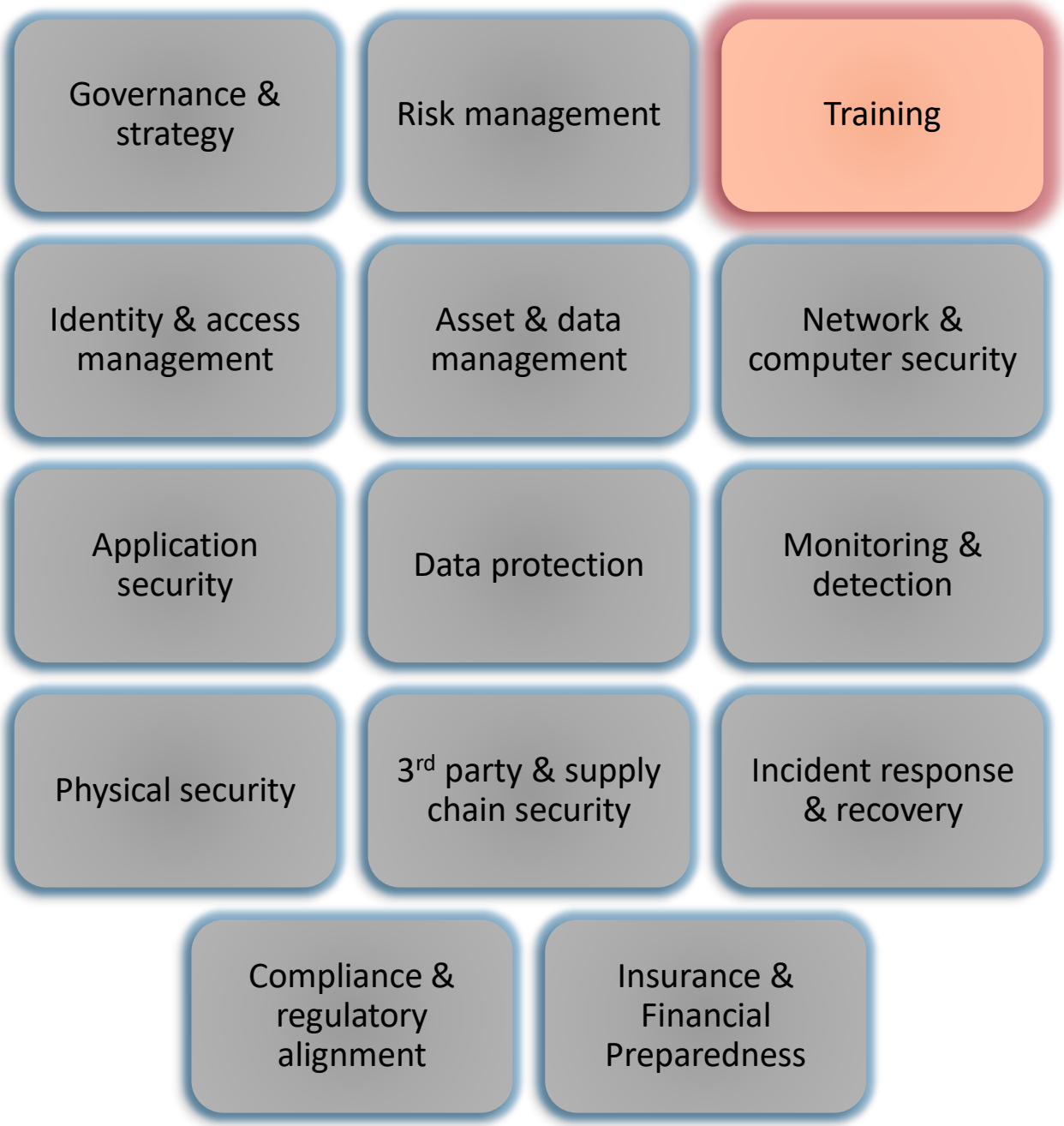
Follows best practices like NIST CSF or CIS



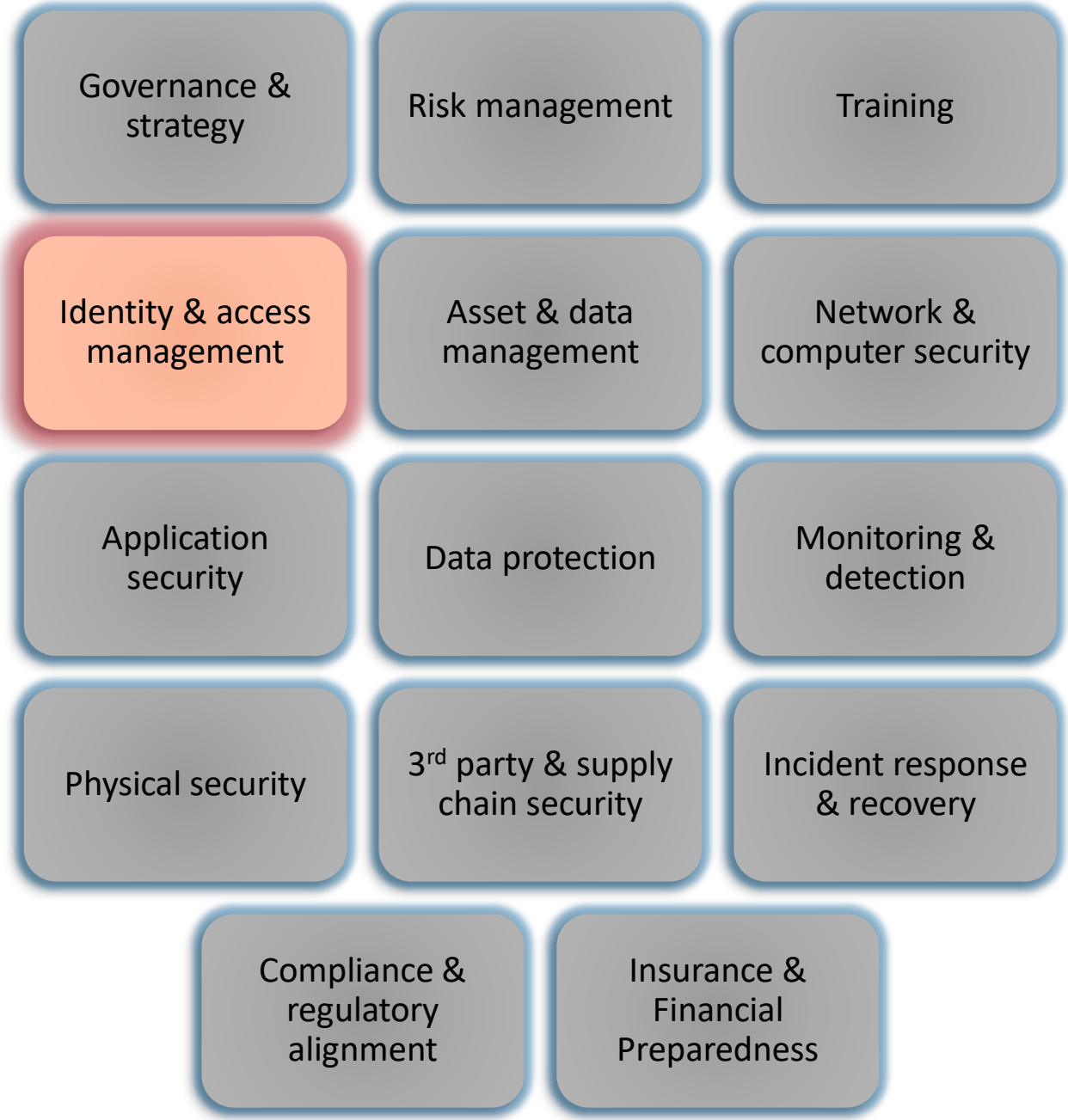
- Leadership commitment and oversight
- Policies, standards, and procedures aligned with frameworks (NIST CSF, CIS Controls)
- Defined roles and responsibilities for accountability



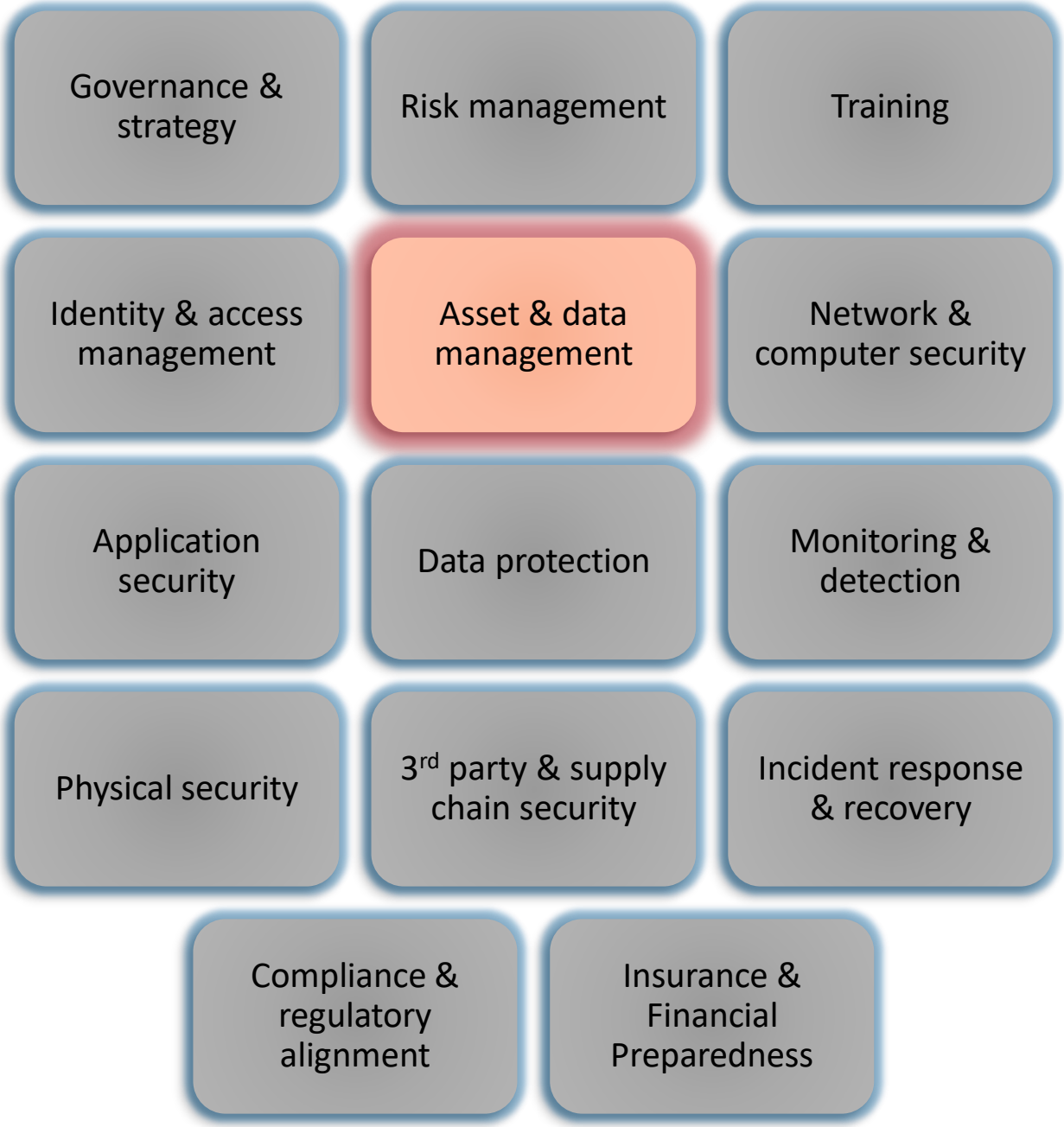
- Identify, assess, and prioritize cyber risks
- Maintain a risk register and apply treatment plans (accept, mitigate, transfer, avoid)
- Align with other risk management for consistency



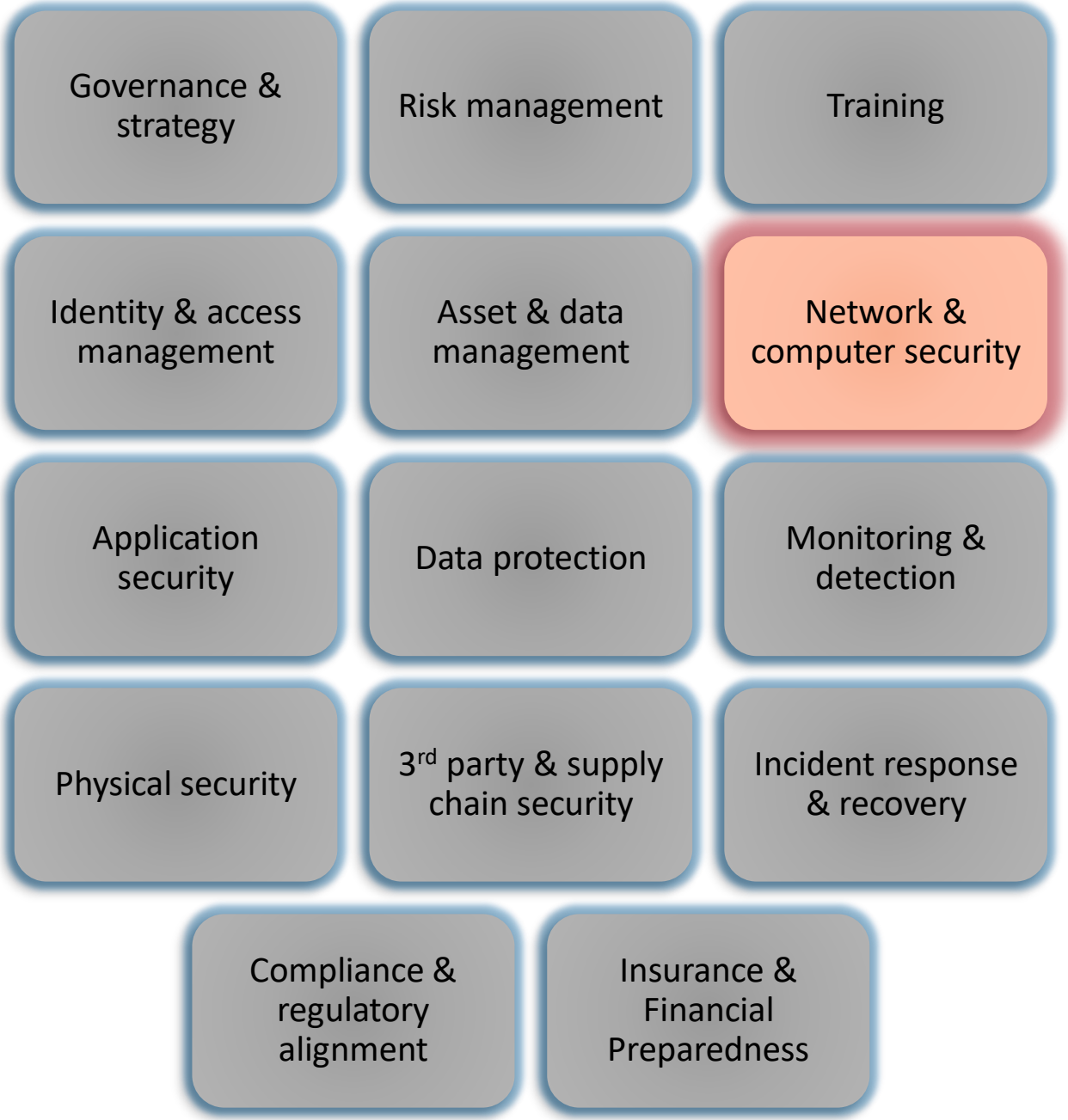
- Ongoing employee training on phishing, social engineering, safe practices
- Simulated phishing and practical exercises
- Clear reporting channels for suspicious activity



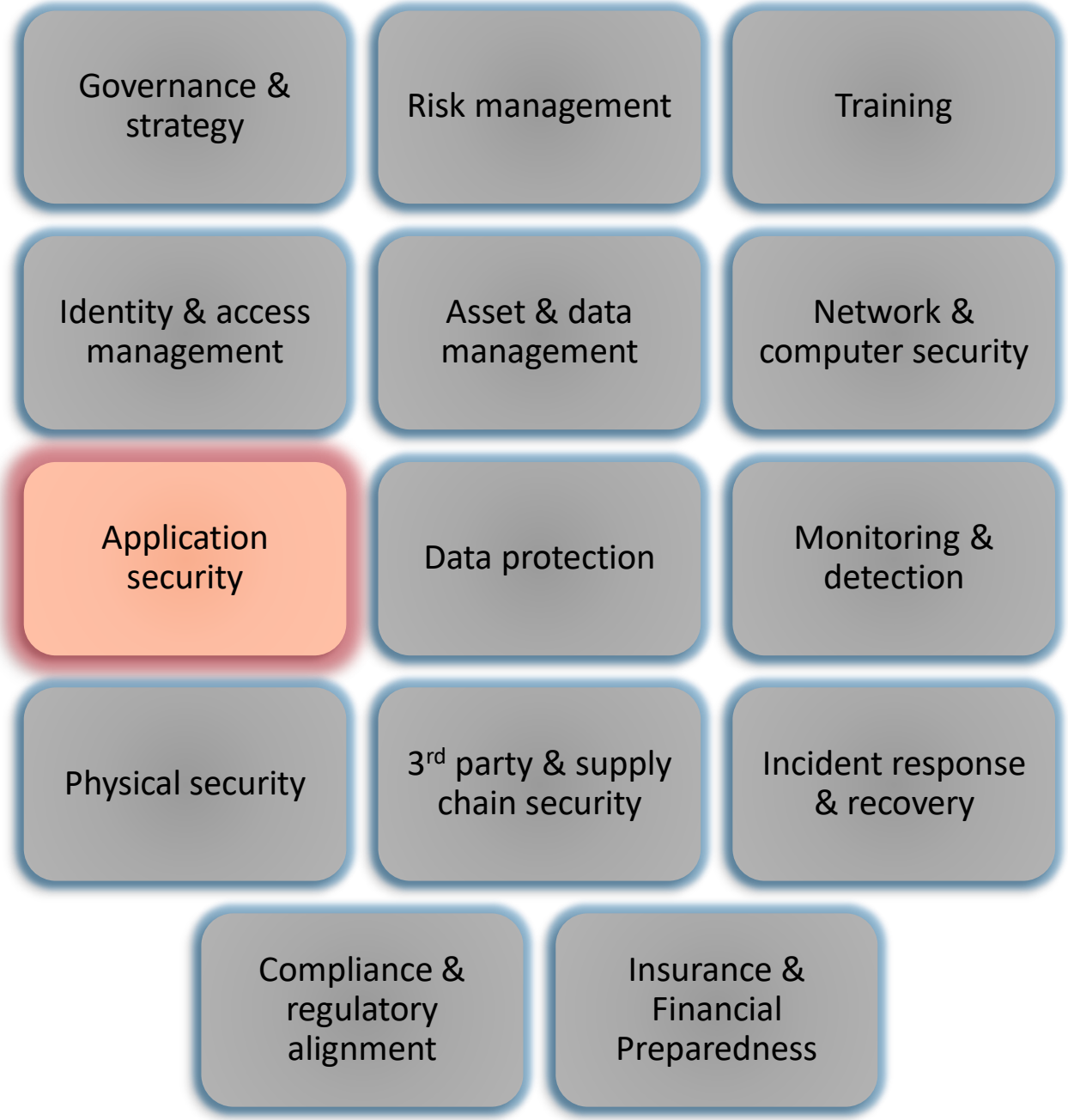
- Strong authentication (MFA, passwords / passphrases)
- Least privilege and role-based access controls
- Segregation of duties
- Regular access reviews and timely onboarding/offboarding processes



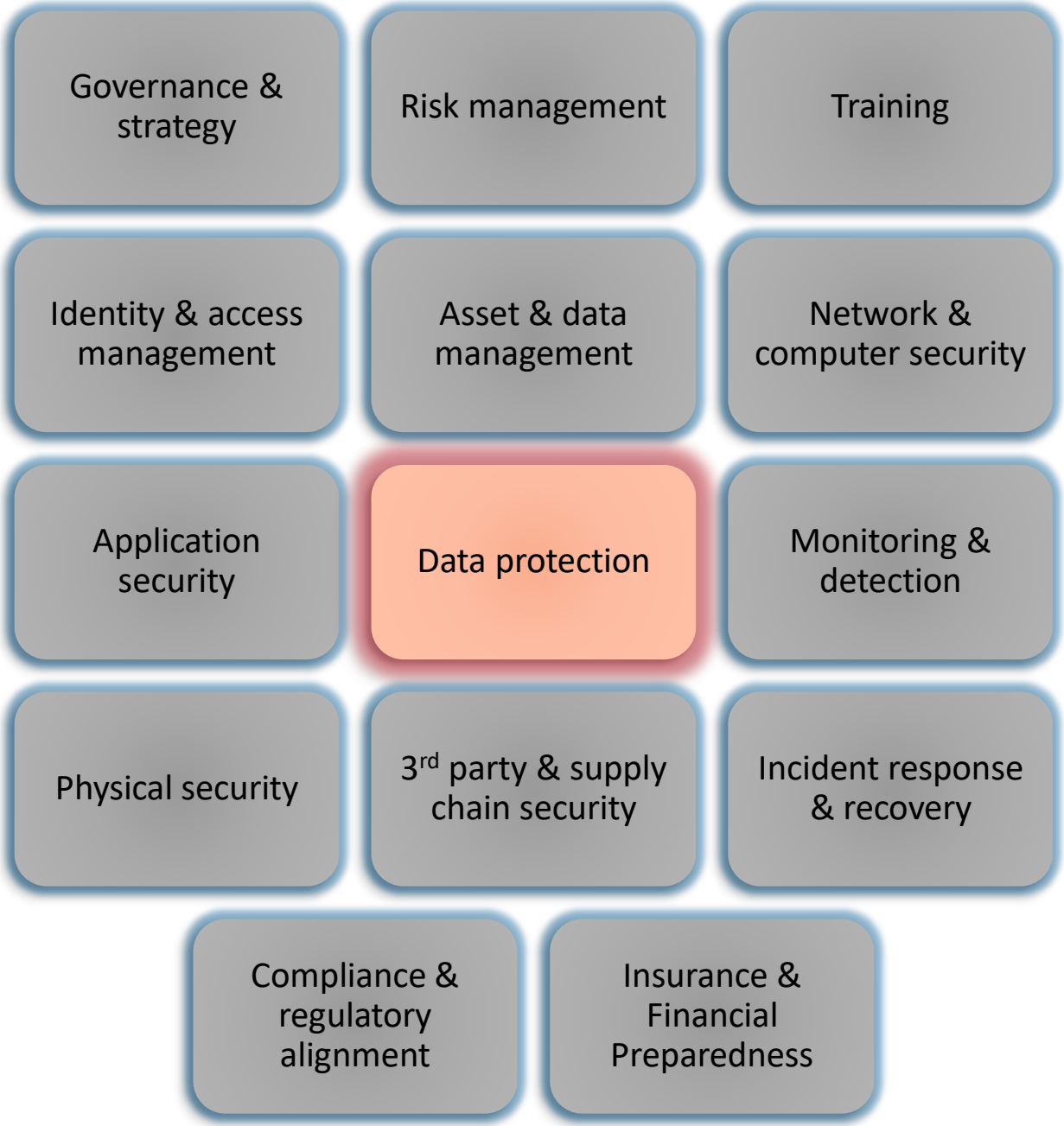
- Inventory of hardware, software, cloud services, and critical data
- Data classification and handling standards (confidential, internal, public)
- Business process mapping to know what systems support what operations



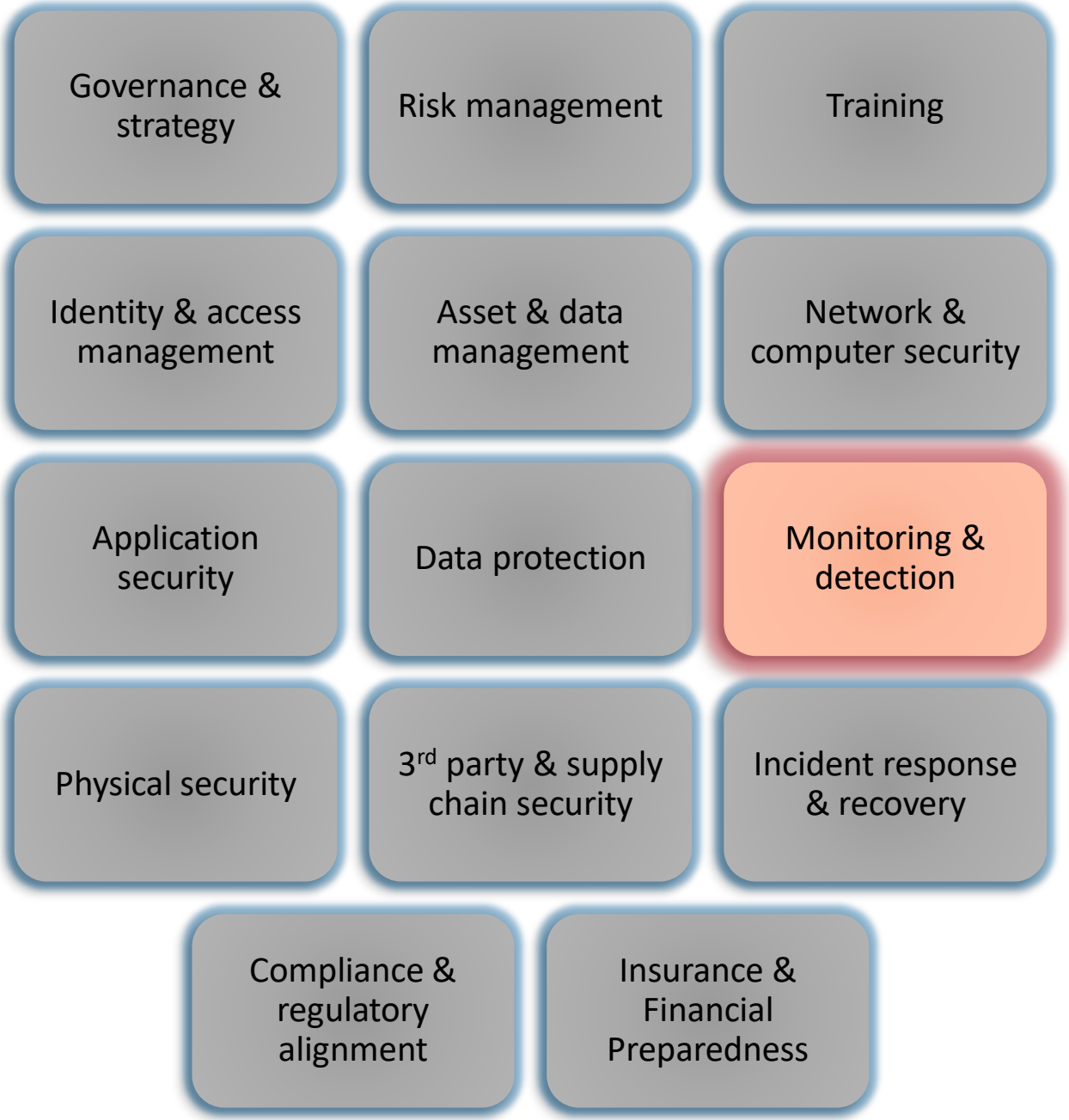
- Firewalls, intrusion prevention, endpoint detection & response
- Secure configurations and patch management
- Segmentation of sensitive systems.



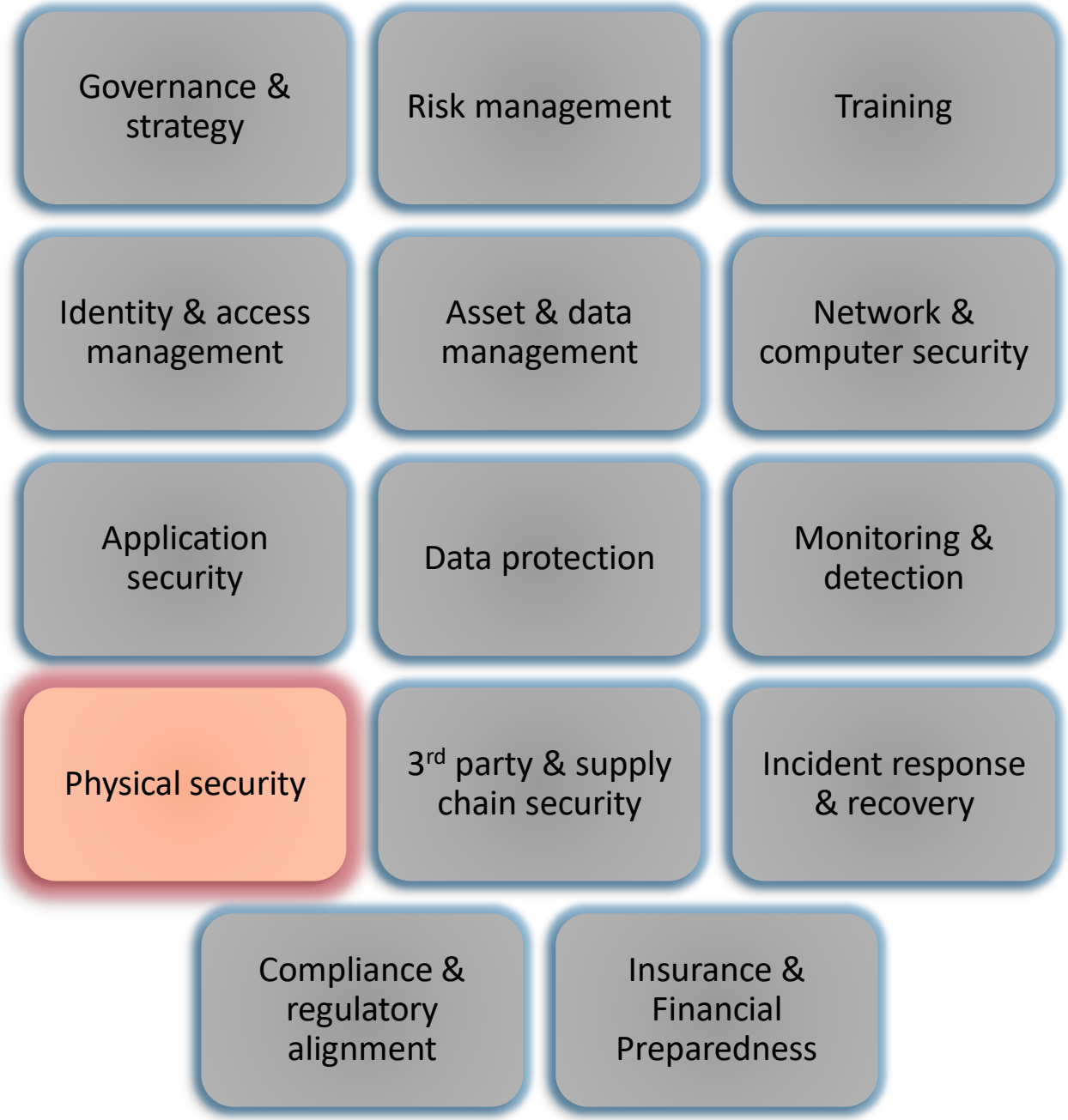
- Secure software development lifecycle
- Vulnerability scanning and penetration testing
- Cloud security configurations



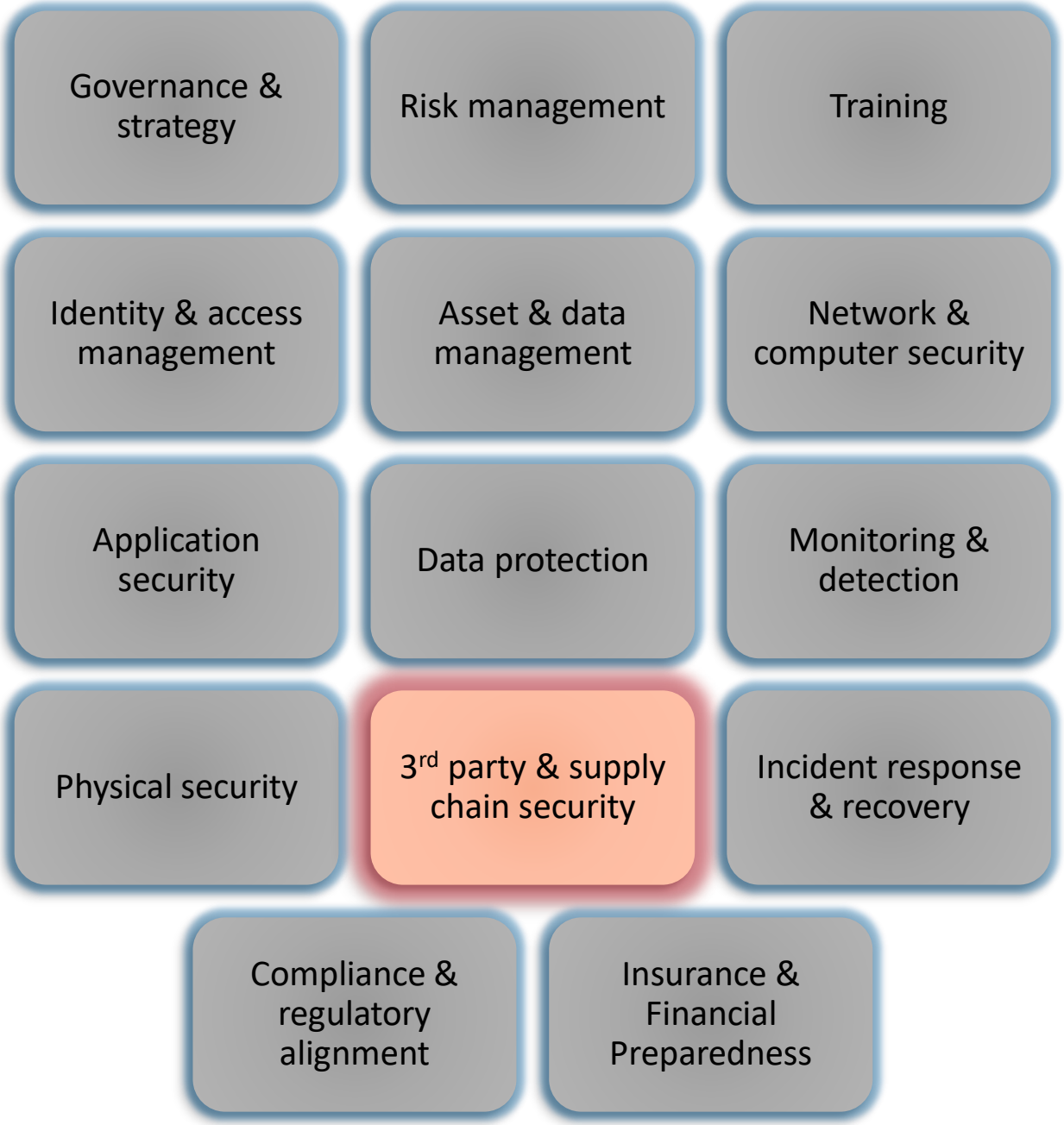
- Know what you have
- Encryption
- Data loss prevention solutions
- Privacy assessments and alignment with laws



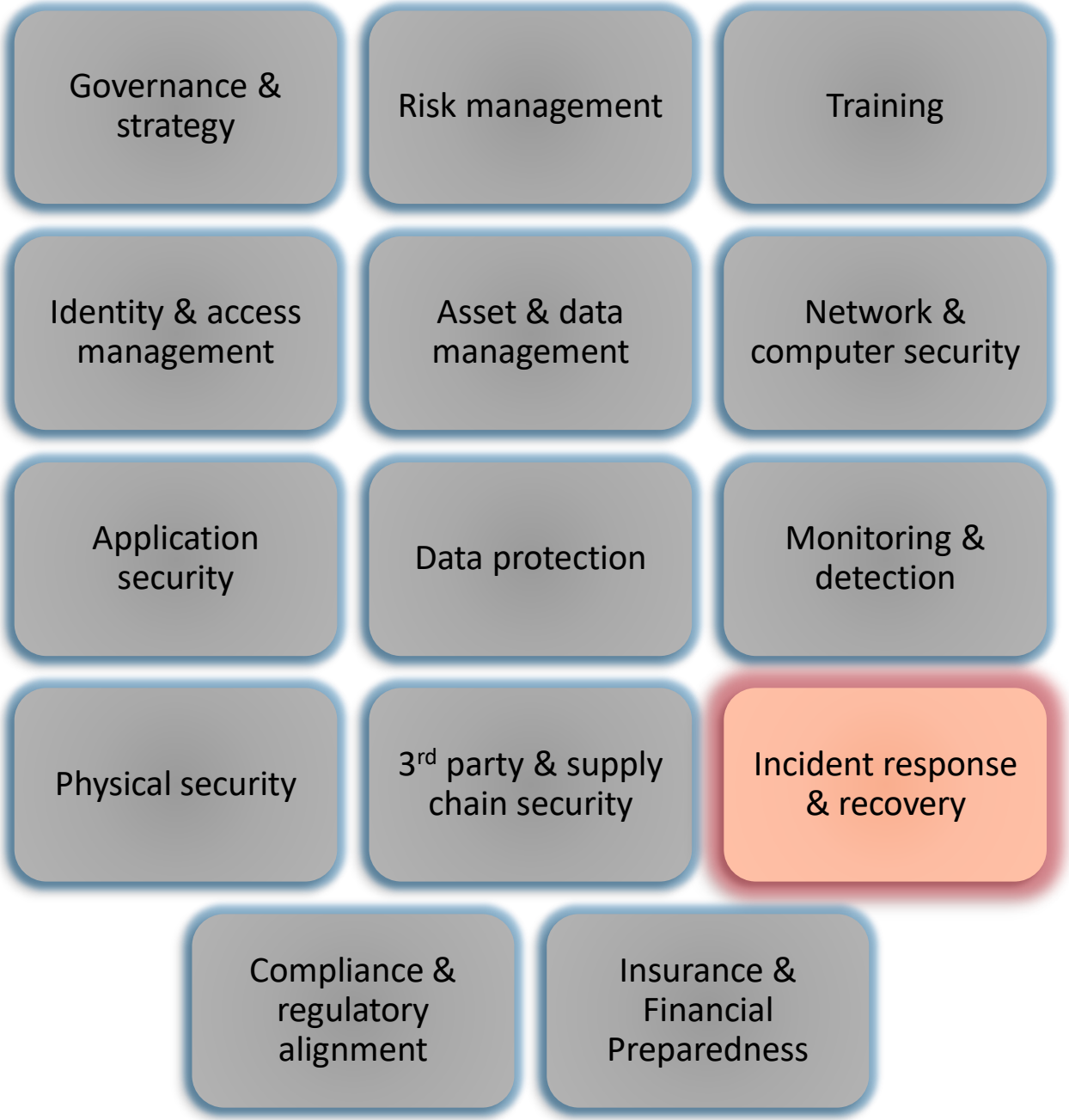
- Centralized logging
- Continuous monitoring for anomalies
- Threat intelligence integration for proactive defense.



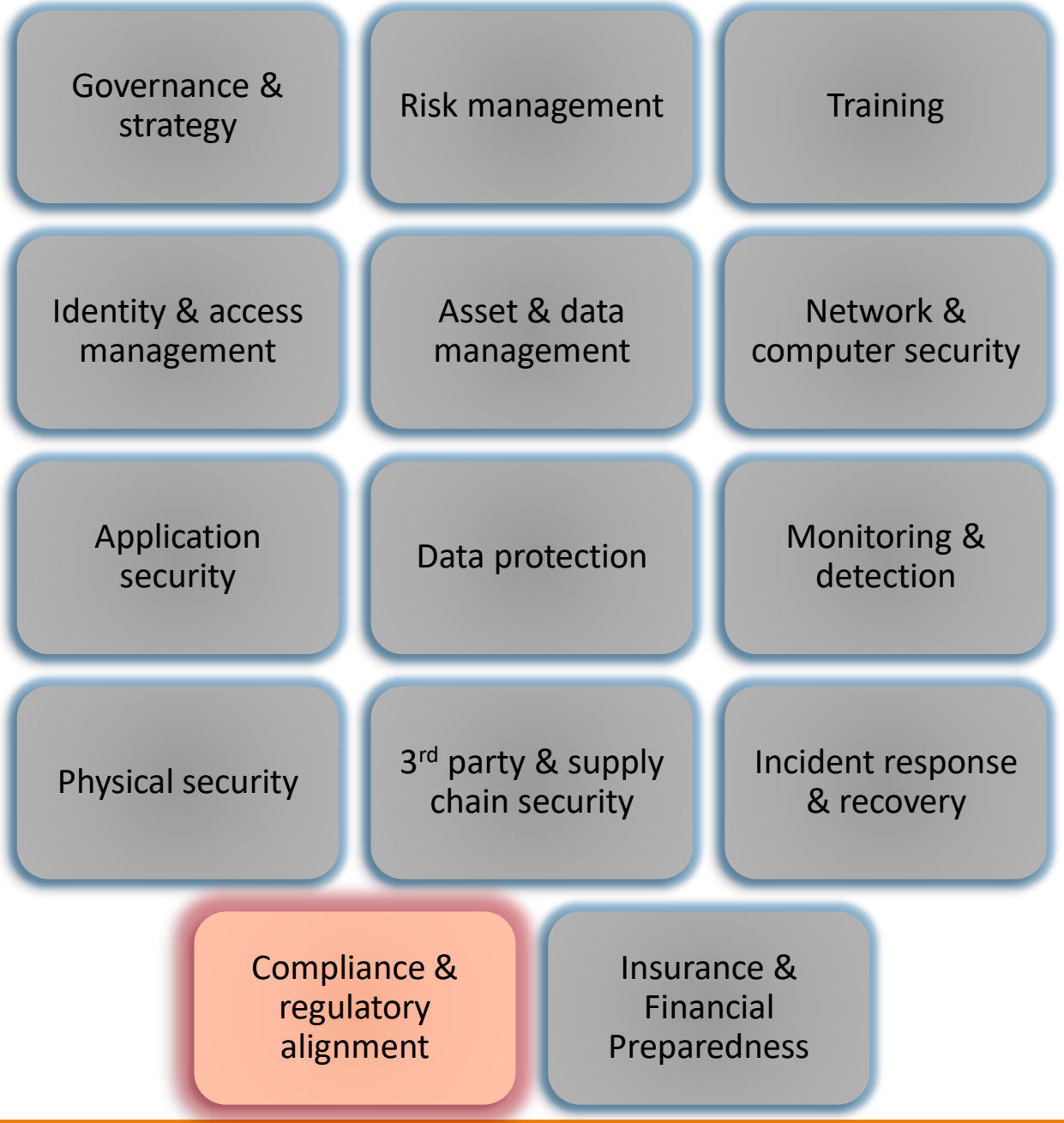
- Secure facilities, access controls, CCTV, alarms
- Protection of server rooms and data centers
- Employee and contractor verification



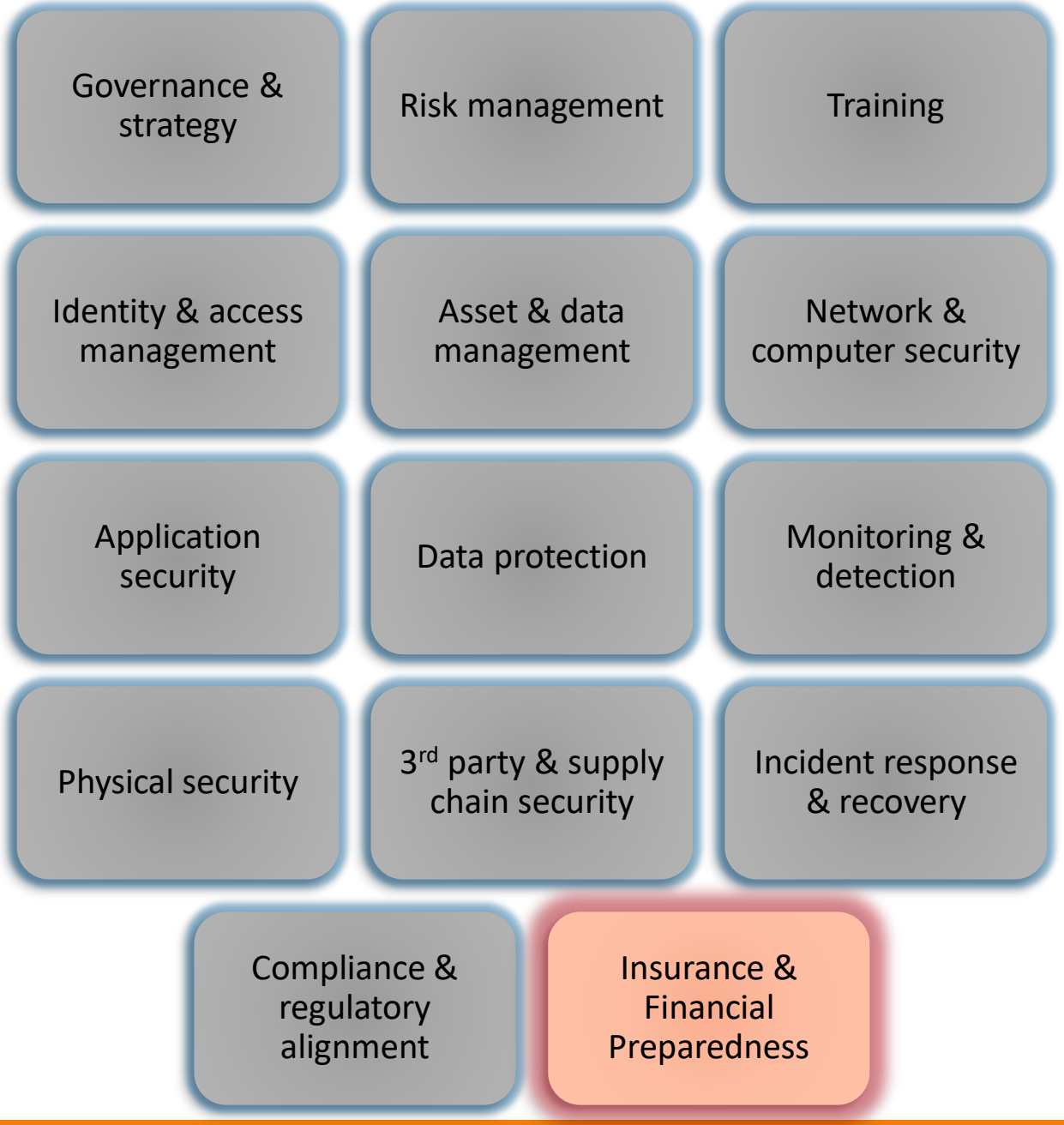
- Vendor due diligence and risk assessments
- Contractual security requirements
- Monitoring of managed service providers and cloud vendors



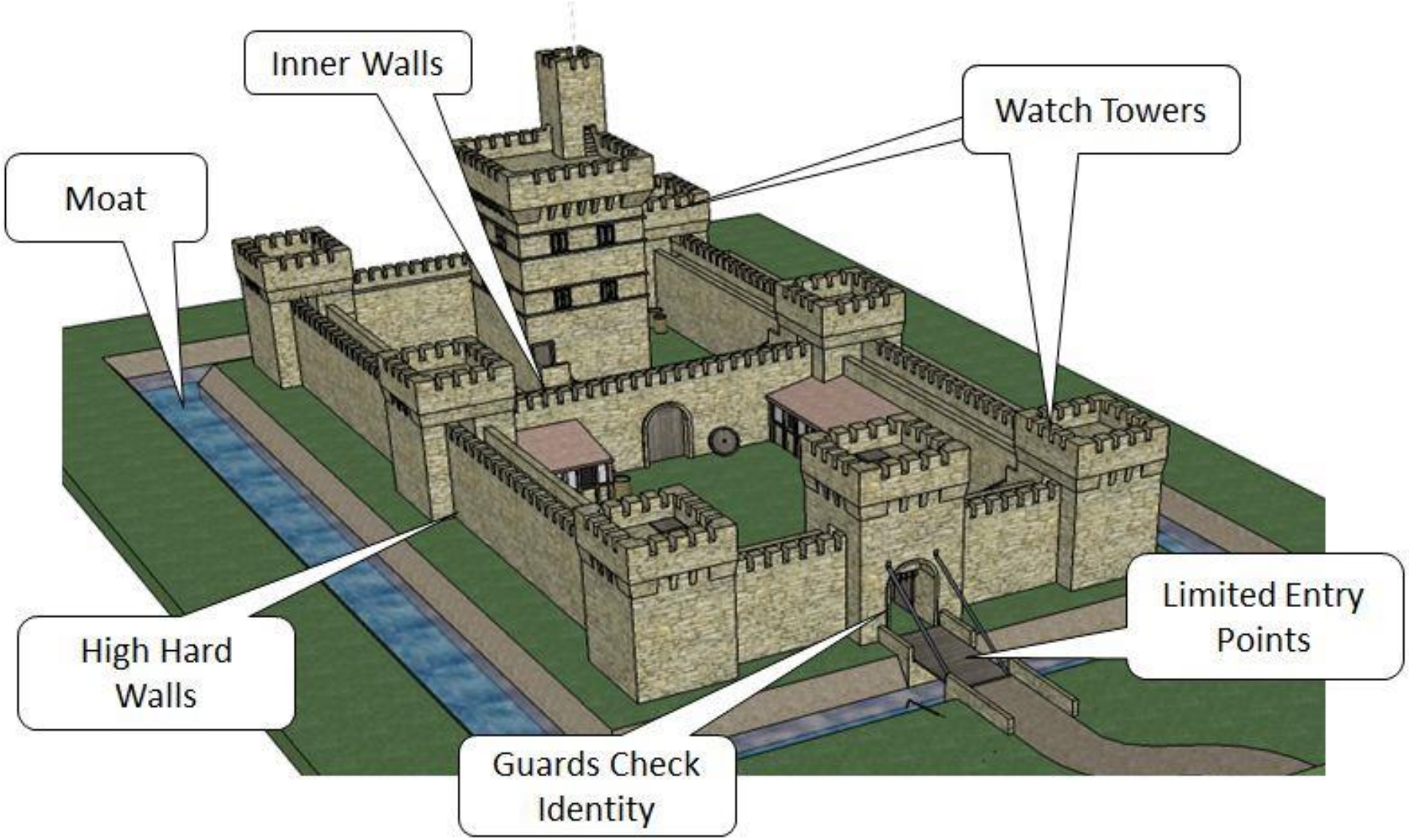
- Documented and tested incident response plan
- Defined roles (technical, communications, legal, executive)
- Disaster recovery and business continuity planning
- Post-incident reviews and lessons learned.



- Map controls to regulatory requirements
- Regular audits and evidence collection
- Reporting mechanisms for compliance obligations



- Evaluating cyber liability insurance coverage
- Linking risk transfer to incident cost recovery
- Aligning policies with risk appetite and residual risks



https://wyzguyscybersecurity.com/there-is-no-perimeter/

Ohio’s new cybersecurity law

Ohio’s new cybersecurity requirements

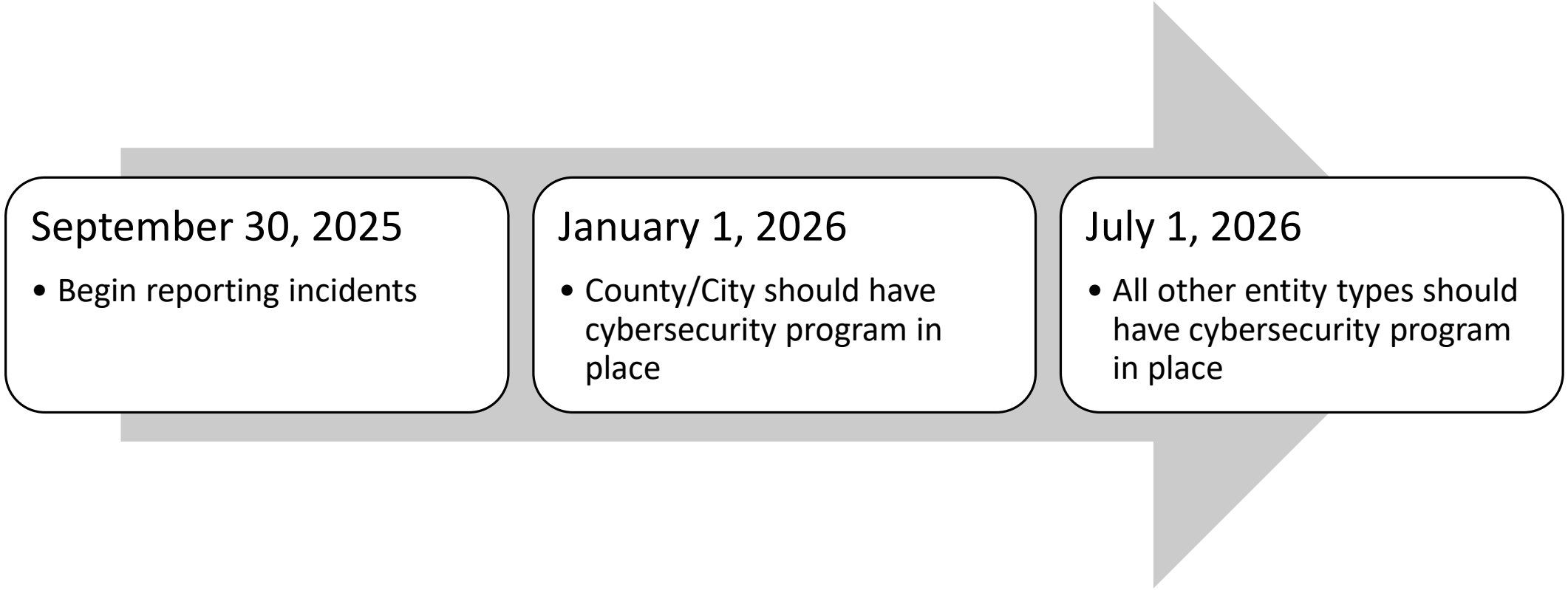
ORC 9.64 ENACTED VIA HB 96

Signed by Governor DeWine on June 30, 2025, effective September 30, 2025. Requires political subdivisions to:

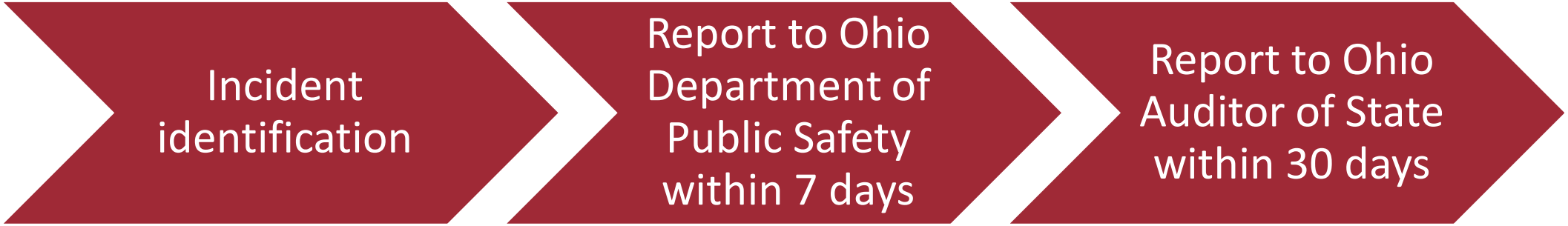
1. Implement a cybersecurity program
2. Obtain approval for ransomware payments from their legislative body
3. Report cyber incidents within specific timeframes

See CyberOhio and AOS websites for all the details.

Timeline


September 30, 2025
• Begin reporting incidents
January 1, 2026
• County/City should have cybersecurity program in place
July 1, 2026
• All other entity types should have cybersecurity program in place

Reporting cyber incidents



Includes:

- Substantial loss of confidentiality, integrity, or availability of an information system or network
- A serious impact on the safety and resiliency of operation systems and processes
- A disruption to engage in business or industrial operations or deliver goods or services
- Unauthorized access to an information system or network, or nonpublic information contained therein, that is facilitated or is caused by a compromise of a third-party or supply chain

Ransomware payments

- Not allowed to pay or comply with a ransom demand unless the legislative authority formally approves the payment

- Must state why the payment or compliance with the ransom demand is in the best interest of the LGE.

Compliance – audit requirements

When AOS conducts a regular audit, we will check that the requirements of this new law are being met. The law allows local officials to design a program that best fits their needs, and AOS staff will audit according to that program.

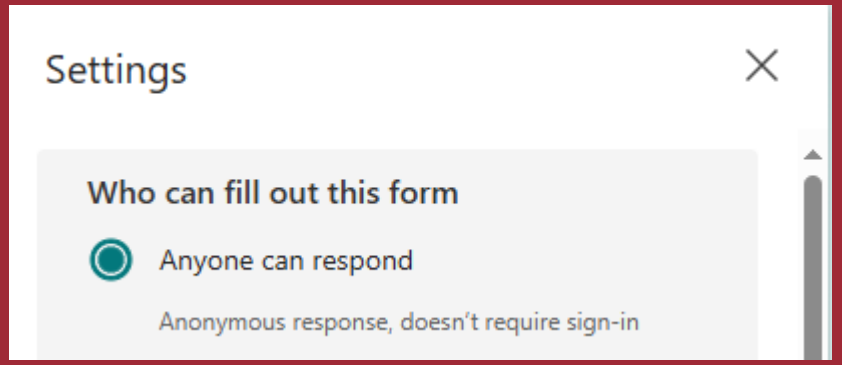
2025 Ohio GFOA - Poll question #3

https://forms.office.com/r/abEDTKP1YS

Poll #3

What would most improve your team's preparedness in the next 12 months?

Completely anonymous – I do not capture anything about you



Practical takeaways

Practical takeaways

- Start now – proactive vs. reactive
- Cybersecurity is an organizational risk, not an IT risk - Finance needs to be aware, involved, and updated on internal controls tied to the cybersecurity program
- Cybersecurity efforts cannot be decentralized, or one department's responsibility
- Strong policies, response plans, and communication across departments are imperative
- Leverage third-party resources and experts