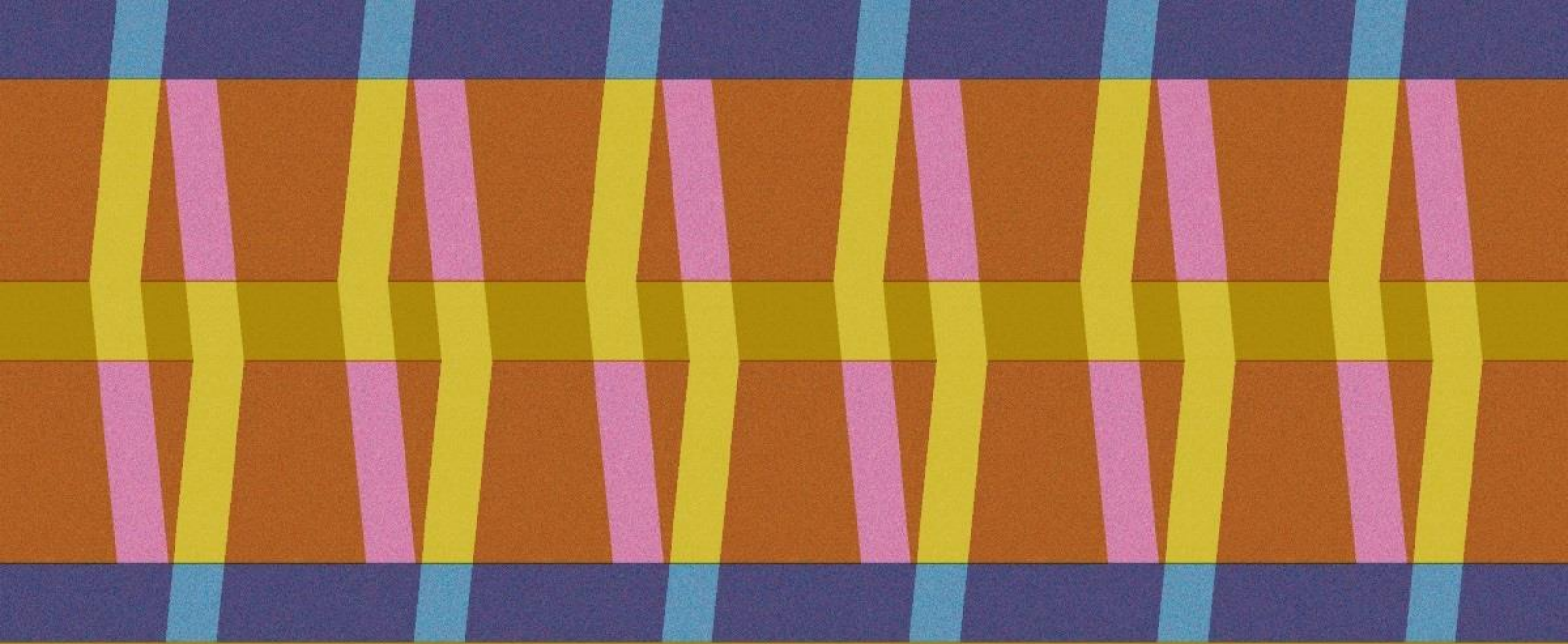


MUNICIPAL DISCLOSURE | MARCH 28-29, 2023

LAKE NATOMA INN | FOLSOM, CALIFORNIA

Session 3

Assessment, Mitigation and Disclosure of Cybersecurity Risks

Donald Hester, Cybersecurity Manager, City of Livermore

Omid Rahmani, Associate Director, Fitch Ratings Agency

Joseph Santiesteban, Partner, Orrick Herrington & Sutcliffe LLP

Sean Yates, Managing Associate, Orrick Herrington & Sutcliffe LLP

CDIAC

The FBI is investigating a ransomware attack on the city of Atlanta

By Emanuella Grinberg, CNN
Updated 9:35 AM ET, Fri March 23, 2018

Cyberattacks, like the one on CDOT, a wakeup call for local governments to prepare

After two attacks Colorado transportation department sped up implementation of security

By THE ASSOCIATED PRESS

Mar. 29, 2018 12:42 pm

City: Cyber attack against Baltimore's 911 computer-aided dispatch system was ransomware

According to Baltimore's CIO, the vulnerability was left open during troubleshooting. Ransomware is among the most common attacks against public safety agencies, said SecuLore's Tim Lorello.

NOV 28, 2016 @ 08:31 AM 39,687 VIEWS

Ransomware Crooks Demand $70,000 After Hacking San Francisco Transport System -- UPDATED

Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms. FULL BIO

State Department warns staff of surge in hacking attempts

By ERIC GELLER | 04/12/2018 04:57 PM EDT | Updated 04/12/2018 06:28 PM EDT

76% of local government organisations suffered a cyber attack in the past year

Get the ITPro Newsletter

Get FREE weekly newsletters from ITPro - delivering the latest news, reviews, insight and case studies.

Click here

SECURITY

Local Governments: Attractive Targets for Cybercriminals?

Cities and counties are attractive targets in part because they're connected to state systems or other large networks.

BY ANDY MATARRESE, THE COLUMBIAN, VANCOUVER, WASH. / MAY 4, 2016

SEC's Proposed Cybersecurity Disclosure Requirements

- Proposed rules in March 2022 apply to public companies

- Provide context and guidance for the municipal market

- Designed to:
  1. Better inform investors about a public company's risk management, strategy, and governance;

  2. Provide timely notification of material cybersecurity incidents; and

  3. Create consistent, comparable, and decision-useful disclosures regarding (1) and (2).

Two Overarching Categories

- Periodic Disclosure
  - Focus on risk management, strategy, and governance
  - Changes to Regulation S-K, and corresponding changes to Form 10-K and Form 10-Q
  - Informs an issuer's or borrower’s:
    1. Annual and/or quarterly continuing disclosure reports
    2. Voluntary event filings;
    3. Offering documents; and
    4. Other communications to the market

- Incident Reporting
  - Focus on timely disclosure of material cybersecurity incidents
  - Changes to Form 8-K
  - Informs an issuer's or borrower's:
    1. Material event notices;
    2. Offering documents; and
    3. Other communications to the market

Periodic Disclosure – SEC Rules

The SEC's Proposed Rules Would Require Public Companies:

1. To disclose cybersecurity policies and procedures

2. To provide detailed disclosures describing board-level governance, including:
   - How the board learns about and discusses cybersecurity issues;
   - Whether the board evaluates risks as part of business strategy, risk management and financial oversight; and
   - Which directors have cybersecurity credentials.

3. To disclose cybersecurity management processes, including whether it has a chief information security officer (and their credentials) and, any consultants, auditors or other third parties to help assess cybersecurity risks

Periodic Disclosure – Muni Market

The SEC's Proposed Rules Indicate that Muni Market Participants Should:

1. Review and bolster cybersecurity policies and disclosure policies
    - Consider whether you have had any privacy or security incidents that involve confidential or personal data, and if so, whether those incidents were disclosed to the market.
    - Evaluate your procedures for periodic risk assessments both internally and with respect to third parties

2. Collect information regarding cybersecurity expertise of the governing board and key staff members (including a CISO)

3. Evaluate whether your current cybersecurity insurance coverage aligns with the entity's current risk profile

4. Develop disclosures relating to updated cybersecurity policies and procedures
    - Goal is to create forms to update and adapt for quarterly and annual reports and offering documents

Case Study

In re First American Financial Corporation (2021)

- First American's security personnel identified a vulnerability in January 2019 exposing over 800 million documents containing social security numbers and other personal financial data.

- First American failed to remediate the vulnerability.

- On May 24, 2019, a cybersecurity journalist discovered the vulnerability and contacted and received a statement from First American. On May 28, 2019, First American published an 8-K.

- First American executives were not informed about the January 2019 discovery prior to the publication of the Form 8-K.

- The SEC determined that First American failed to maintain disclosure controls and procedures to ensure that information required to be disclosed is timely disclosed, and imposed a $487,616 penalty.

Incident Reporting – SEC Rules

The SEC's Proposed Rules Would Require Public Companies:

1. To disclose material cybersecurity incidents within four business days from the materiality determination
   - No guidance regarding materiality determinations.
   - Extends to compromises of the company's "information system," including systems owned or used by the company and third-parties such as cloud infrastructure and service providers.
   - No exceptions for delayed reporting for law enforcement or national security reasons.

2. To provide periodic updates reflecting material changes or additions to previously disclosed incidents (including remediation efforts)

3. To disclose cybersecurity incidents that only become material if aggregated

Incident Reporting – Muni Market

The SEC's Proposed Rules Indicate that Muni Market Participants Should:

1. Revisit and test their incident response plans
   - Consider whether your cybersecurity policies and procedures require employees to quickly escalate cybersecurity incidents to those empowered to make materiality and disclosure determinations.
     - *See in re First American Financial Corporation*.
2. Consider whether contracts with third parties comprising the "information system" provide for incident reporting and cooperation necessary to make materiality and disclosure determinations regarding third-party cybersecurity incidents.
3. Discuss with bond or disclosure counsel the implications of any cybersecurity incidents and possible voluntary disclosures.

Case Study

In re Pearson plc (2021)

- On March 21, 2019, Pearson learned that millions of rows of data had been accessed and downloaded by a sophisticated threat actor.
- On July 19, 2019, Pearson mailed a breach notice to its affected customers.
- On July 25, 2019, Pearson filed its Form 6-K, which included as a risk factor only that the company faced a hypothetical risk of a data privacy incident and failed to disclose that the company had in fact already experienced such a data breach.
- On July 31, 2019, Pearson posted a media statement which misstated the character and contents of the data breach.
- The SEC determined that Pearson's Form 6-K and media statement were misleading, and imposed a $1,000,000 penalty.

ICMA LG Cybersecurity Survey 2020

Local Governments are at Risk

- Top officials in organizations are often not engaged in cybersecurity at high levels
- Top management is not sufficiently well informed about or committed to cybersecurity
- Top officials fail to insist on a cyber safe culture
- Top officials fail to act appropriately in their own cyber responsibilities

> "Understanding these issues will enable local officials not only to see why cybersecurity is crucial to their government's digital well-being, but will help ensure that cybersecurity has their full support and is adequately funded and properly managed."

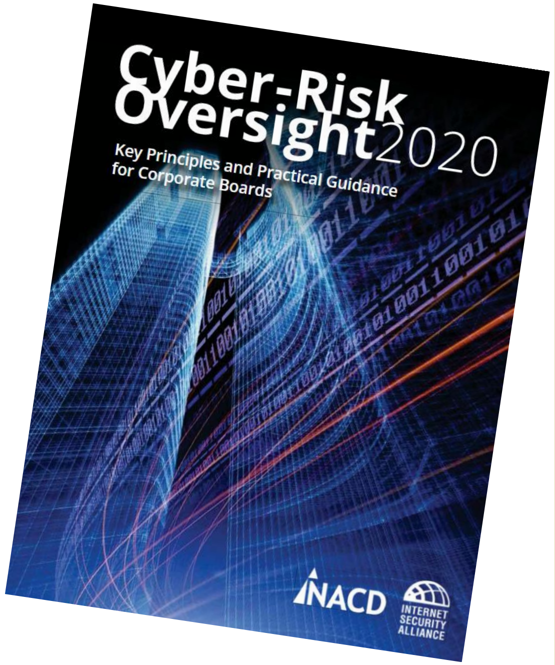
https://icma.org/articles/pm-magazine/look-local-government-cybersecurity-2020

Governance Roles for Boards/Councils

- How should Council (board) view cyber risk?
- What role does Council (board) play in managing cyber risks?
- What expectations should Council (board) set for management?
- What questions should the Council (board) be asking?

Many executives and boards still have dated views about cybersecurity:

"Board members need to ensure that management is fully engaged in making the organization's systems as resilient as economically feasible. This includes developing defense and response plans that are capable of addressing sophisticated attack methods."



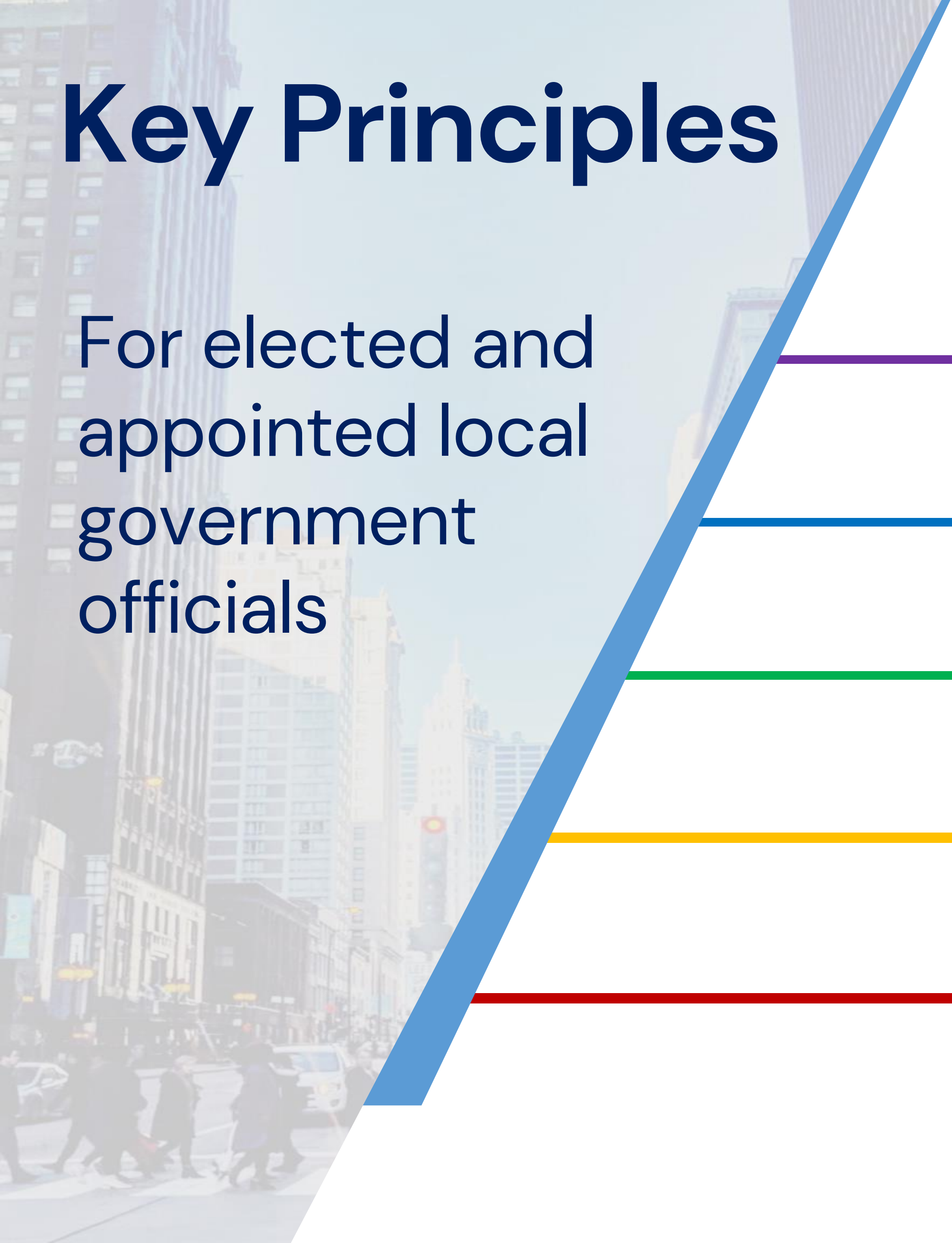
Cyber-Risk Oversight2020

Key Principles and Practical Guidance for Corporate Boards

NACD

INTERNET SECURITY ALLIANCE

Key Principles



For elected and appointed local government officials

Enterprise Risk

Understand cyber risk is enterprise risk and cybersecurity is strategic

Assign Budget

Ensure budget is sufficient to reduce cyber risk to an acceptable level

Oversight

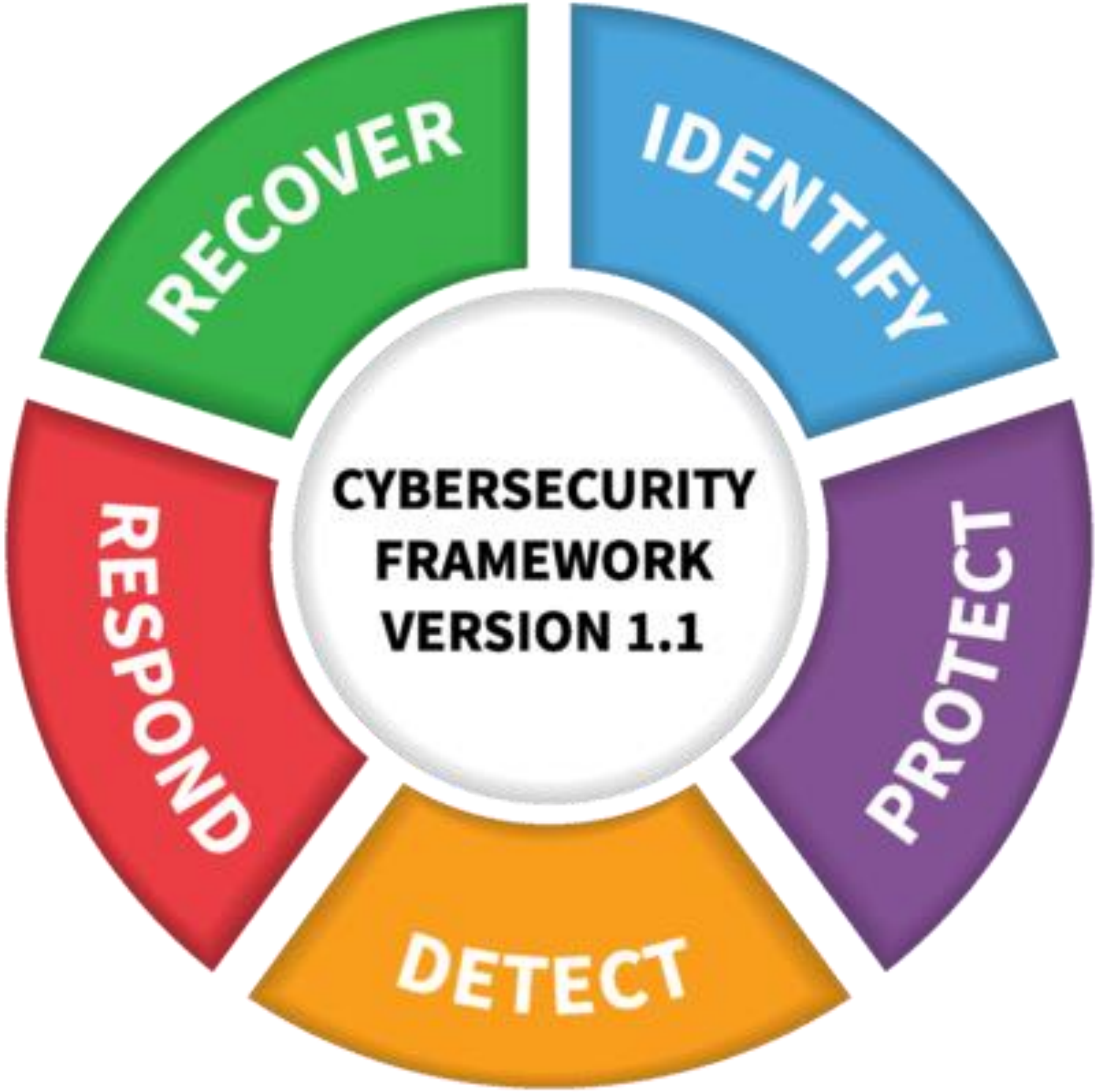
Culture, Cyber Literacy, Clear Expectations, Accountability

Framework

Select a framework and assign responsibility for cybersecurity

Monitor & Report

Data and reporting sufficient for decision making



CYBERSECURITY FRAMEWORK VERSION 1.1
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

Incident Preparedness

Exercises

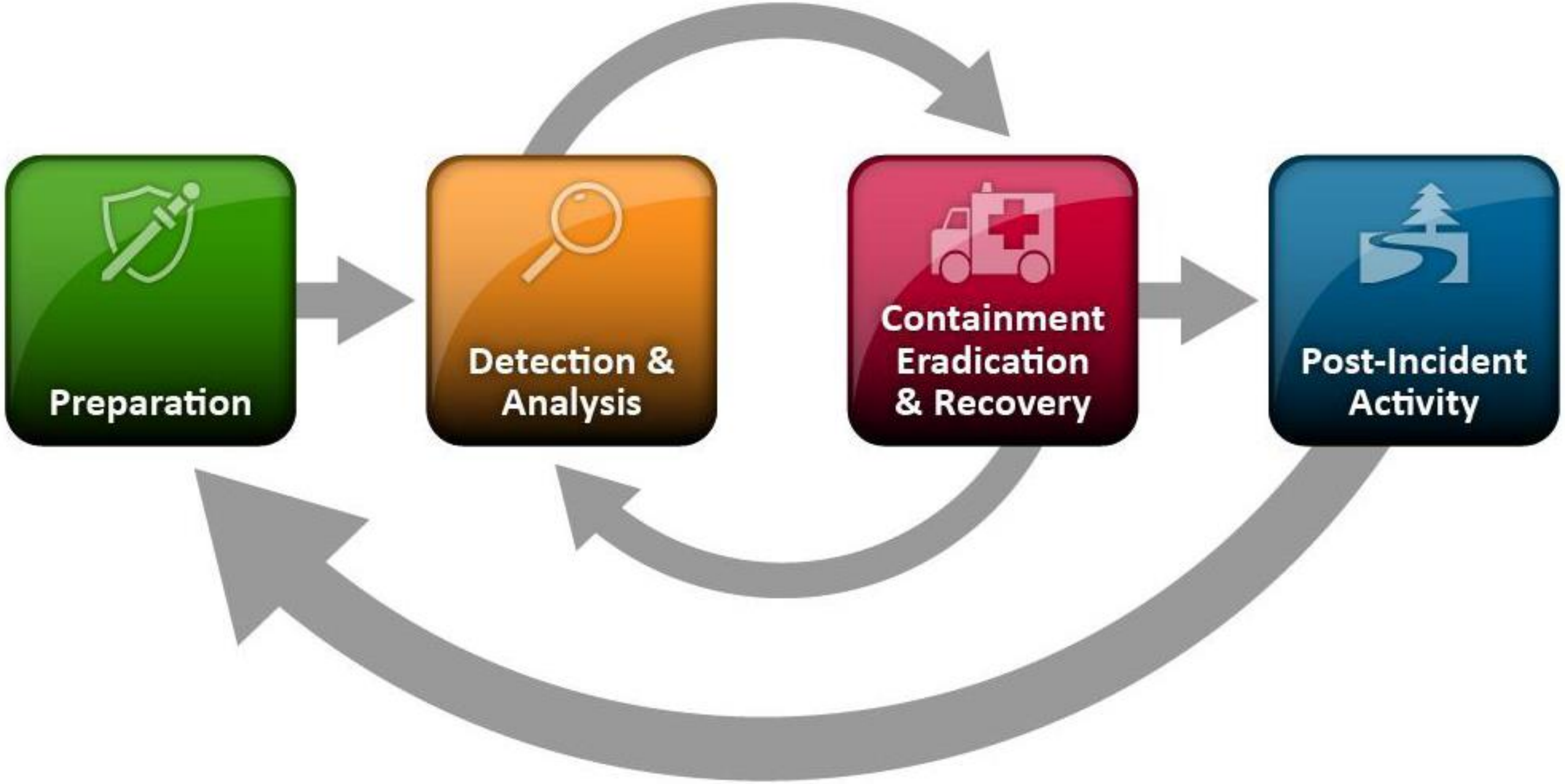
Purpose

Examine the coordination, preparation, and capabilities in response to a significant cyber incident within the organization, and identify areas for improvement in policies, plans, and procedures.

Objectives

- Strengthen the organization’s cybersecurity awareness to enhance the effectiveness of protecting the community’s systems and services.
- Examine information sharing processes with internal and external stakeholders.
- Assess preparedness to respond to, mitigate, and recover from cybersecurity incidents.
- Explore processes for requesting state/federal incident response resources once county/state resources are exhausted.
- Understand potential threat and how incident might materialize.

Incident Response



Source: NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide