Keys to Prudent IT and Fiscal Management

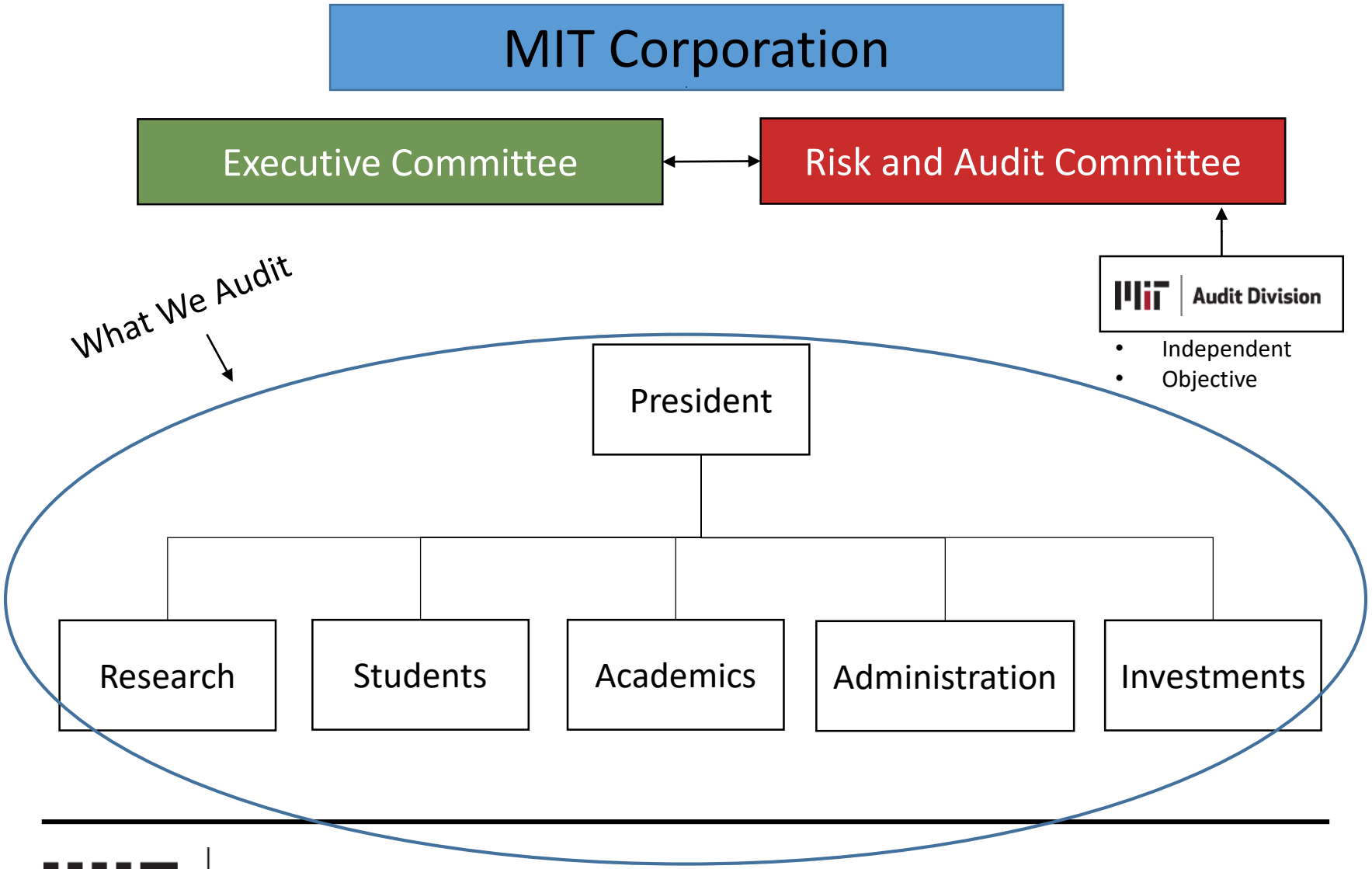
Meeting

April 29, 2021

Carter Stubbs, CISA
Audit Services Manager
Information Technology and Advisory Services

Kallie Firestone
Senior Compliance Specialist

MIT Governance



Our Team

- 19 professional certifications
- 20 undergraduate/graduate degrees


Mike Moody


Martha Jane Gagnon


Kim Ahern


Michelle Jackson


Carter Stubbs


Tara Fournier


Edgar Berrios


Erin Coates


Suwen Duan


Kallie Firestone


Jie Jiao


Prachee Kulkarni


Bob Monteith


Emma Bagshaw

https://ist.mit.edu/remote-working-emergency-resources

Work securely from your remote environment

- Protect your devices.
- Make sure devices are running newer operating systems supported by the vendor and that all updates have been applied.
- Ensure software applications are up-to-date; enable automatic updates.
- Install and maintain anti-virus software (including for Macs).
- Perform regular backups.

Secure your home WiFi

- Make sure your router's firmware is up-to-date, that you're using a strong password.
- ConfirmWPA2 encryption has been enabled for your home WiFi network.

https://ist.mit.edu/remote-working-emergency-resources

Practice safe video conferencing

- Use MIT-approved conferencing tools.
- Follow suggested best security practices.
- Be aware of others in your household, including digital assistants, during conferencing to protect confidential data.
- Lock your screen when you're not using your computer.

Be aware of COVID-19 related scams

- Protect yourself and your information by using caution when opening emails and attachments.
- Be wary, in particular, of phishing attacks and also of scams that try to trick you into making donations or revealing sensitive information to fraudulent organizations or causes.

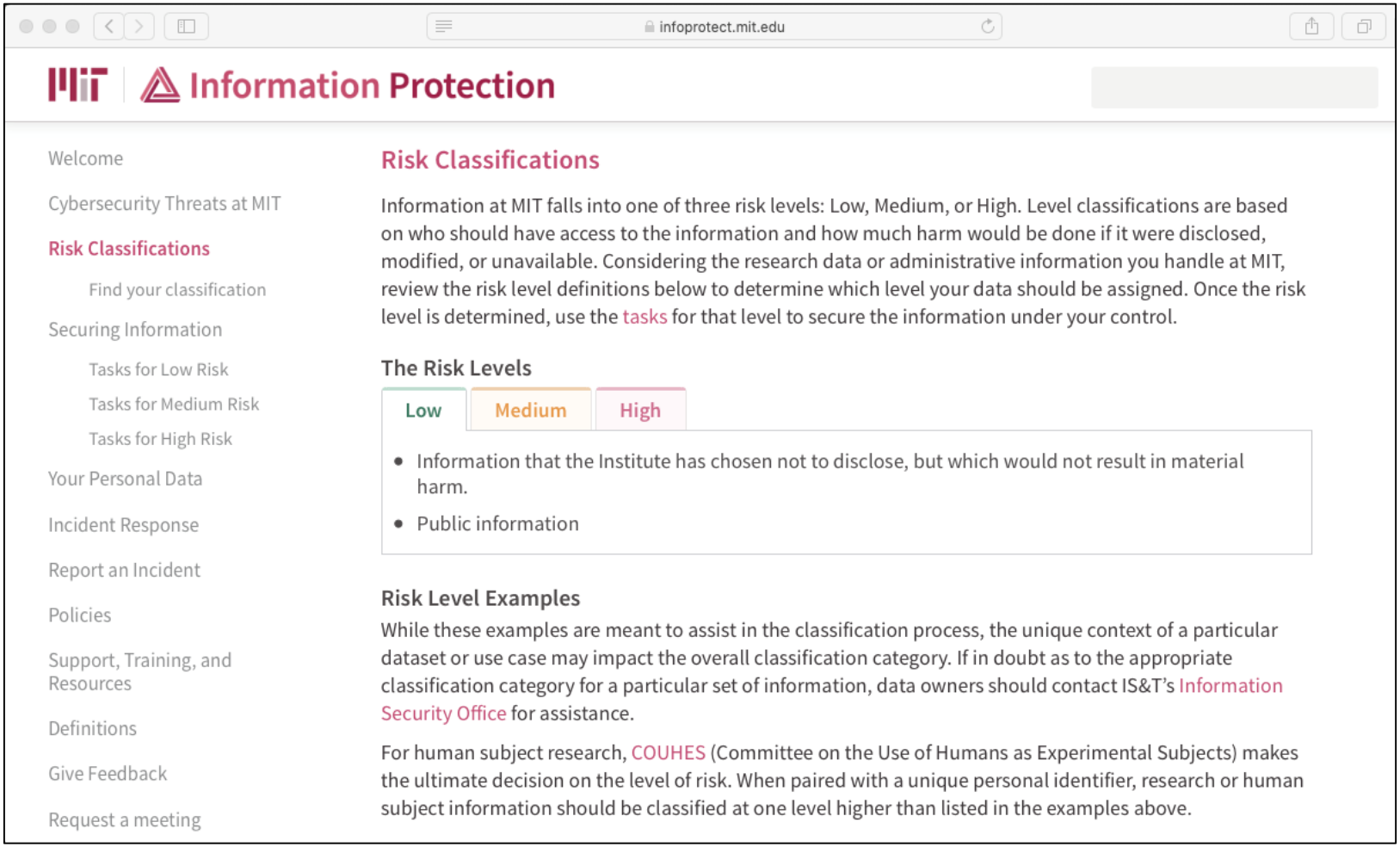
https://ist.mit.edu/remote-working-emergency-resources

Remotely access MITnet

- Install MIT certificates on your remote working computer.
- Register at least two readily available devices with Duo.
- Request a USB hardware token if you need one for use with Duo.
- Install the MIT VPN client and always connect to the MIT remote access VPN when working on a public WiFi network to encrypt your activity.

Get support - IS&T's Service Desk provides 24/7 phone and email support to the MIT community and can be reached at 617-253-1101 and servicedesk@mit.edu.

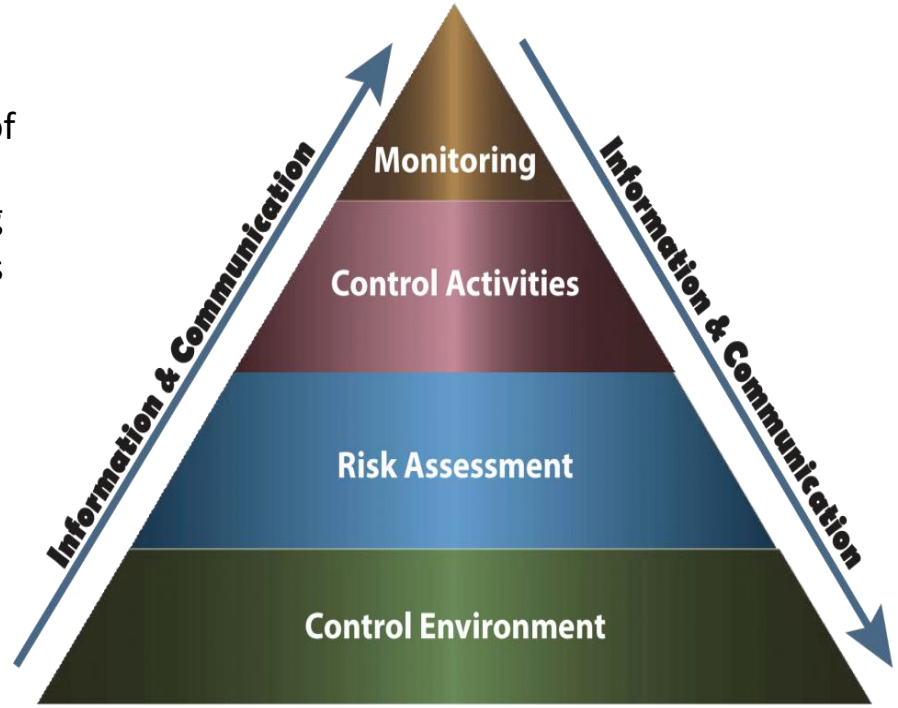
Information Protection: New Website infoprotect.mit.edu



infoprotect.mit.edu

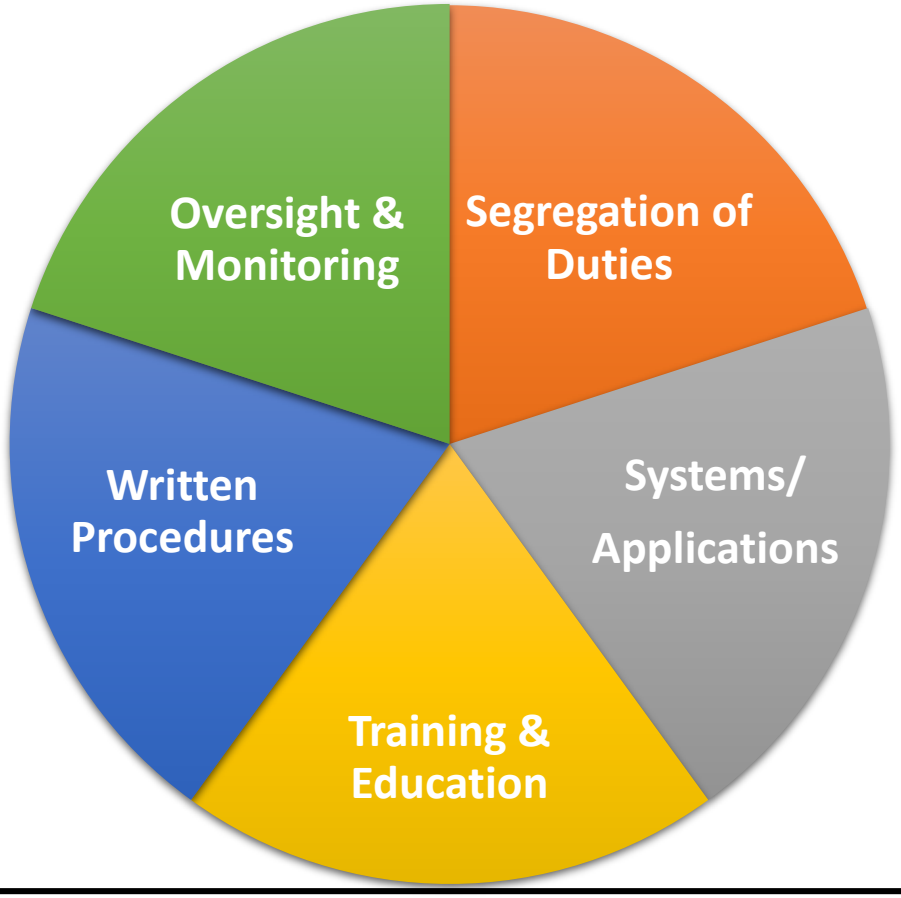
What are Internal Controls?

- A process designed by an organization, to provide reasonable assurance regarding the achievement of objectives in the following areas:
  - Reliability and accuracy of financial reporting
  - Compliance with applicable laws, regulations and policy
  - Effectiveness and Efficiency of operations
- Internal Controls help manage ***risk*** (financial, operational, compliance, safety and behavioral)
- ***People*** **are <u>not</u> controls**



*The **COSO** model defines internal control as "a process designed to provide reasonable assurance of the achievement of objectives"*

Five Keys to Prudent Fiscal Management



Key 1: Oversight & Monitoring

- **A repeatable process to regularly and timely review activities, as well as communicate and resolve issues.**
  - Key control activity to ensure problems are detected early by management.
  - Essential to ensure compliance (costs are allowable, allocable, consistently applied and documented).
  - **FRC (Financial Review and Control) –** A person familiar with activity on an MIT cost object reviews monthly transactions on a cost object as part of the overall system of internal controls. Management provides necessary oversight of this activity.
  - Management controls (approvals and verifications)
    - Review and approval of travel (Concur)
    - Review and approval of purchases (Pcards, B2P, POs, etc..)

Key 2: Segregation of Duties

- Segregation of duties (SoD) is an internal control where at least two individuals are responsible for the separate parts of any task. An individual should not have responsibility for more than one of the three transaction components: authorization, custody, and record keeping.
  - Verifier and Pcard holder should not be the same person.
  - Verifier should not use cards for which they verify charges.
  - Person performing statement review different from the person procuring on the cost object (unless secondary review is performed).
  - Travel reports reviewed by secondary administrator/supervisor.

Key 3: Systems/Applications

- Systems/applications process information based on specific inputs and authorizations.
  - Established for specific processes within Institute procurement functions, i.e. paying faculty and staff, accounting for revenues, expenditures, and other dynamics depicted on the Institute's financial statements.
  - Utilization of systems can improve the efficiency and effectiveness of the operations and enable easy sharing and management of information and data.
    - Adequately assign and update roles in the system (spend and commit)
    - eDACCA, Concur, B2P

Key 4: Training & Education

- Development of skills and knowledge that relates to specific useful competencies.
  - To ensure consistent knowledge of process, procedures, regulations, and/or guidance.
    - Understanding of MIT Policies, Federal regulations, and other external guidance.
    - Knowledge of methodologies for procurement and review is articulated and understood throughout the DLC.

Key 5: Written Procedures

- Policies and procedures provide direction for day-to-day operations.
- Communicate expectations, processes, or procedures within the DLC for consistency in application across functions and staff.
  - Documented procedures streamline internal processes, ensure compliance with regulations, and assist in decision-making.
    - Adequate termination procedures for employees and temporary staff (cancel Pcards or Travel cards, remove access)
    - Statement Review – 100% or Risk Based?
    - Salary Certification – Direct or Proxy; who/how monitored?

Fraud Triangle

Pressure: Motive or incentive

Rationalization: Justification for actions

Opportunity: Ability to carry out fraud

Detecting Irregularities

Financial Review & Control (FRC)

- Make sure costs are reasonable & applicable to the award or cost object.
- Identify and resolve variances early.

Pcard charges

- Verified timely and question “suspicious” or “unusual” purchases.

Travel Costs:

- Review for unusual costs (that appear not business related and justified).

Segregation of Duties

- Secondary review of cost objects when SoDs are not present.
- When person performing statement review is the same as person procuring on the cost object.

Detecting Irregularities

Perform an analysis of

- Portfolio of cost objects and transactions
- Unusual patterns (purchase volume changes)
- Large purchases (over “typical” volume of general supplies i.e. hard drives, toner cartridges)
- Unexpensed travel
- Overruns on cost objects
- Duplicate transactions (i.e. RFPs)

Review roles (at least annually)

Important Tips for Administrators

- Do it correctly the first time …
- Perform monthly review of all charges, and maintain evidence of the review.
- Address questionable charges or situations early – seek advice from Assistant Deans, VPF (Sponsored Accounting), or the Audit Division.
  - Ask yourself: "What would the sponsor say if I asked them?"
- Be aware of developing problems, such as overruns or cost-sharing shortfalls.
- Develop a "culture of compliance" within your sphere of influence – encourage good decision-making.
  - Use good judgment, based upon principles.

DLC Best Practice Recommendations per VPF*

- DLCs should:
  - Review and reinforce policy that card should be used by **cardholder only**
  - Validate that all travel has been processed when an **employee or temporary employee gives notice**
  - Notify VPF Travel and Card Services if the department identifies **suspicious activity**
  - Notify VPF Travel and Card Services of all **temporary employee and student cardholder terminations**
  - Review unexpensed transaction on a **monthly basis**
  - Review travel reports on unexpensed travel transactions accessible through **wikis.mit.edu**. These reports provide data that is in the data warehouse but does not exist in SAP.
    - Link: https://wikis.mit.edu/confluence/display/DATAADMIN/Travel+Reporting

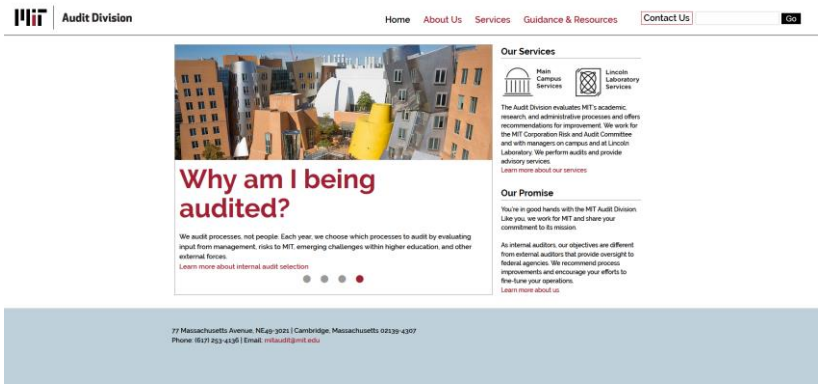
Questions?

For More Information…

Carter Stubs, CISA
stubbsc@mit.edu
3.9811

Kallie Firestone
kalfire@mit.edu
4.9065

https://audit.mit.edu



Resources Page

- MIT Audit Division - https://audit.mit.edu/
- Office of the VP or Research - https://research.mit.edu/
- Research Administration Services (RAS) - https://ras.mit.edu/

Policies and Procedures:

- Research - https://research.mit.edu/research-policies-and-procedures
- Research Compliance - https://research.mit.edu/integrity-and-compliance
- Record Retention - https://vpf.mit.edu/record-retention-guidelines
- Uniform Guidance - https://ras.mit.edu/grant-and-contract-administration/sponsored-programs-basics/ombs-uniform-guidance/uniform-guidance