Crowe

Smart decisions. Lasting value.™

Florida Board of Governors

Budget and Finance Committee Meeting

Management Controls and Business Process Assessment

January 29, 2020

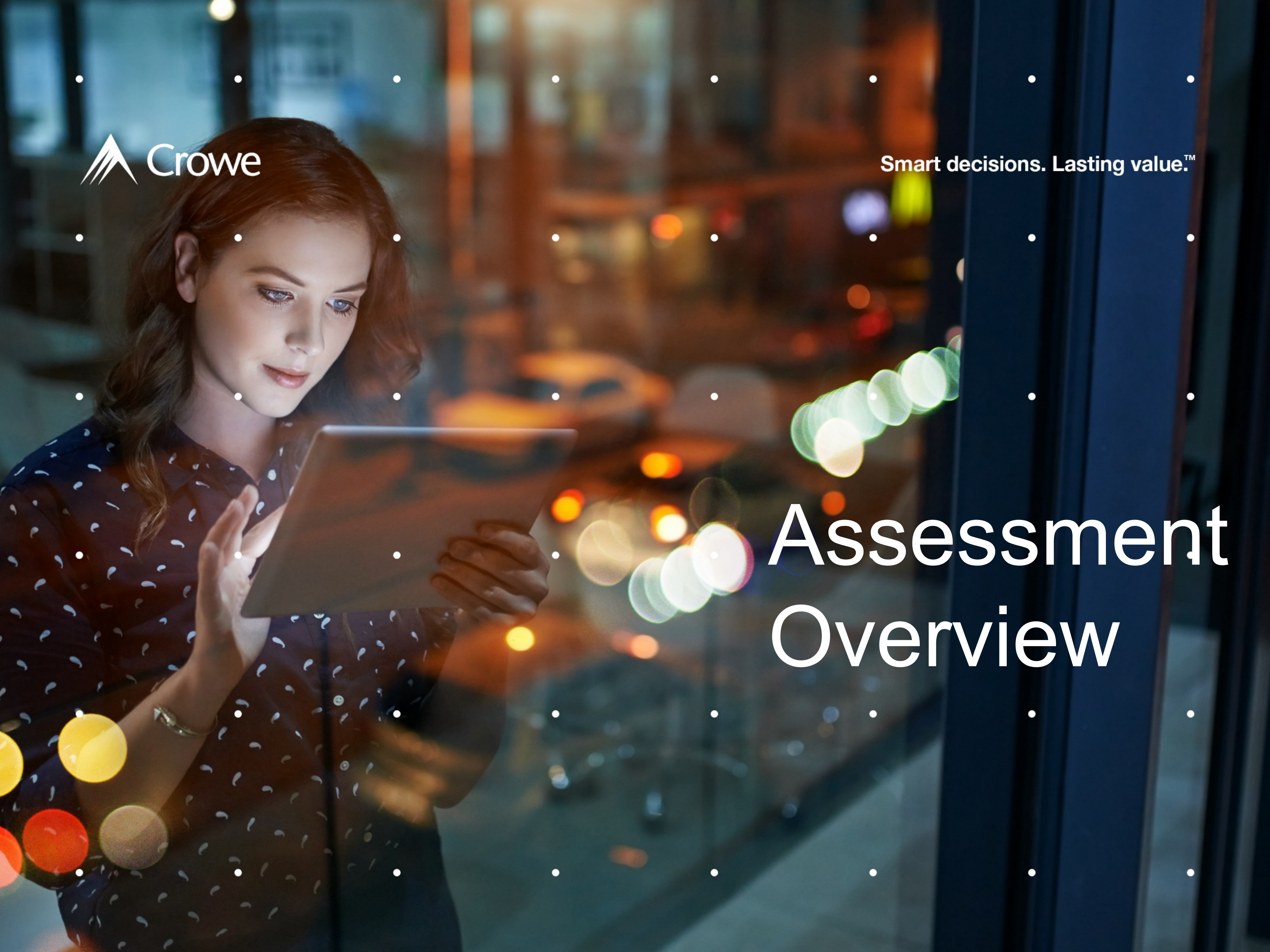
Agenda

1. Assessment Overview

2. Observations and Themes

3. Recommendations

5 Q&A



Crowe

Smart decisions. Lasting value.™

Assessment Overview

Project Objectives & Scope

Objectives.

Conduct an internal management and accounting/financial control assessment to evaluate the existing internal controls and business processes to identify any areas of risk for the SUS

Scope.

The internal management and accounting controls of the SUS.

Project Update – Completed Activities

We have completed our procedures for all 12 universities within the SUS which included:

1) Assessing BOG regulations, university policies, procedures, processes and business requirements.

2) Preparing inherent risk assessments arising from our assessment of the above as well as our experience in common risks within higher education

3) Distributing risk/control questionnaires to university management and conducting interviews onsite to understand risk management and control practices

4) Completing evaluations of each university's risk management and control structure

5) Identifying gaps in controls and process improvement opportunities as observations and recommendations which have been discussed with management.

6) Submitting draft reports to university management for their written response to our observations and recommendations.

A Collaborative Approach

- We worked closely with university management who were cooperative and supportive of this engagement.
- Our process was built upon collaboration and dialogue with management. For example:
  - We sent requests for materials in advance of onsite visits (polices/procedures, org charts, strategic plans, risk assessments, previous audits, etc.)
  - We distributed an Information Technology controls questionnaire and reviewed the responses with management to confirm our understanding.
  - We held Fieldwork Exit Conferences with university management to review draft observations for factual accuracy.
    - Where management disagreed we requested additional documentation/evidence to support their assertions.
    - We were able to resolve numerous observations prior to drafting the report.
  - We sent draft reports to management and provided the opportunity to respond in writing to our observations and recommendations.
    - Level of agreement (Agree, partially agree, or disagree).
    - Action Plans.

Risk Rating Methodology

- **Inherent Risk**
  - Establishes a baseline for risk assessment
  - Considers “environmental” and “industry” factors
  - Does not focus on specific risk mitigation or controls.
- **Control Effectiveness**
  - Identifies specific risk mitigation/control activities.
  - Evaluates the adequacy of their design
  - Evaluates their relevance to addressing specific risks (identified above).
- **Residual Risk**
  - Measures risk levels after the effect of controls
  - Typically is evaluated against risk appetite or tolerances
  - Provides a view into control effectiveness
  - Can be evaluated over time to measure risk management performance

Risk Rating Methodology (Continued)

- Five-point scale
  - Not required – organization should select a model that work best for them.
  - Selected in the absence of a SUS-wide risk assessment methodology.
  - Provides more granularity than the three-point scale.

Impact

- Measures the effect on the related objectives if a risk event were to occur.
  - Inherent impact measures the environment or industry before controls.
  - Residual impact measures controls' ability to reduce impact of risk events if they occur.

Likelihood

- Measures the probability that the risk event will occur (i.e. usually within a 12 month period)
  - Inherent likelihood measures the environment or industry before controls.
  - Residual likelihood measures controls' ability to reduce probability of risk events' occurrence.

Smart decisions. Lasting value.™

Observations and Themes

Themes

1. Overall, our procedures indicated that controls over internal management and accounting controls of the SUS appeared to be in place.

2. Control gaps or weaknesses were rated “Low” or “Moderate”

- Intended to convey control “improvement opportunities” not significant issues.
- Represent lower tiers on the five-point rating scale.

3. Greatest threats to control structure:

- Management override of controls/collusion.
- Informal information security control practices.
- Clear roles and responsibilities for third-party oversight.
- Varying interpretations of active BOG regulations.

Observations

Financial Reporting Observations	Risk Rating	Number of Occurrences SUS-Wide: (3)
Restricted Funds – Interfund Transfers	Moderate	2
Monitoring of Budget-to-Actual Performance	Low	1

Procurement Observations	Risk Rating	Number of Occurrences SUS-Wide: (2)
Contract Management - Shared Services Agreements	Moderate	1
Policies and Procedures – Vendor Setup and Monitoring	Moderate	1

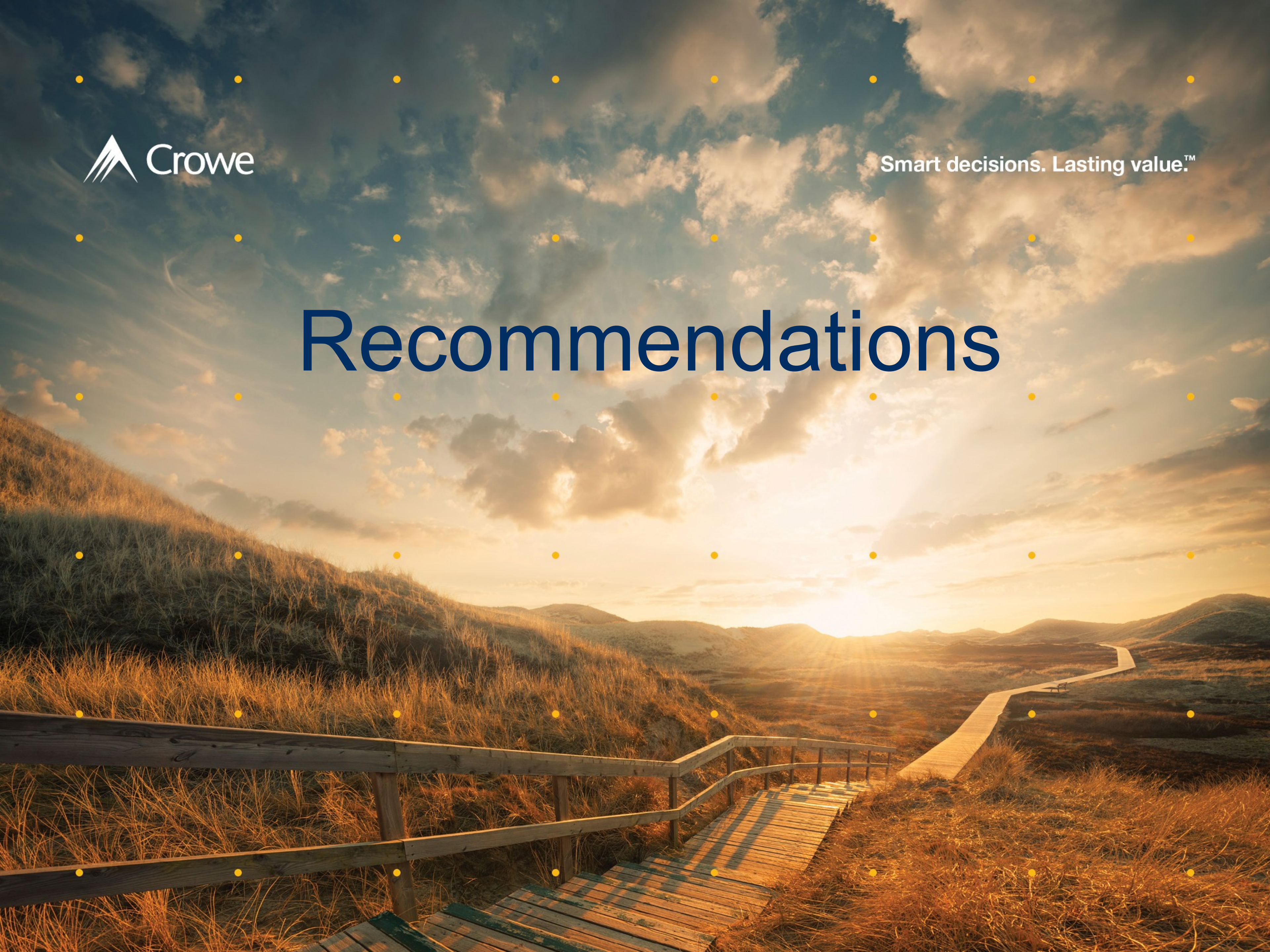
Grant Management Observation	Risk Rating	Number of Occurrences SUS-Wide: (1)
Segregation of Duties: Grant Drawdown Process	Moderate	1

Observations (continued)

Information Technology Observations	Risk Rating	Number of Occurrences SUS-Wide (39)
Configuration Management Program	Moderate	3
Business Continuity Management – Incident Classification	Moderate	1
Information Security Governance Key Risk and Performance Indicators (2) Cybersecurity Risk Management Program (2) Policies and Procedures (2) “Clean Desk” Policy (4)	Low - Moderate	10
Employee Security Awareness Training	Low	6
Data Protection Employee Removable Media (6) Employee Mobile Device Management Policy (5) Sensitive Data-Tracking (1) Data Handling and Classification (1) Data Center Moisture Detection Systems (1)	Low	14
Logging and Monitoring Policy	Low	1
Monitoring of Third-Party Service Providers	Low	1
User Termination and Role Changes	Low	2
IT Operations – Asset Tracking	Low	1

Observations (continued)

Risk Category	Observation	UWF	FSU	UNF	UF	UCF	FAMU	FPU	USF	NCF	FIU	FAU	FGCU
Financial Reporting	Monitoring of Budget-to-Actual Performance									Low			
Financial Reporting	Restricted Funds – Interfund Transfers					Moderate				Moderate			
Procurement	Contract Management - Shared Service Contracts	Moderate											
Procurement	Policies and Procedures - Vendor Setup and Monitoring	Moderate											
Grant Management	Segregation of Duties - Grant Drawdown Process												Moderate
Information Technology	Business Continuity Management - Incident Classification	Moderate											
Information Technology	Configuration Management - Configuration Management Program		Moderate			Moderate					Moderate		
Information Technology	Data Protection - Data Handling and Classification Policy										Low		
Information Technology	Data Protection - Employee Mobile Device Management Policy	Low		Low						Low	Low	Low	
Information Technology	Data Protection – Employee Removable Media	Low	Low			Low	Low	Low				Low	
Information Technology	Data Protection - Sensitive Data-Tracking		Low										
Information Technology	Employee Management – Employee Security Awareness Training	Low			Low	Low	Low					Low	Low
Information Technology	Employee Management - User Termination and Role Change		Low		Low								
Information Technology	Information Security Governance – Clean Desk Policy			Low		Low				Low		Low	
Information Technology	Information Security Governance - Cybersecurity Risk Management Program					Low					Low		
Information Technology	Information Security Governance - Key Risk and Performance Indicators		Moderate									Moderate	
Information Technology	Information Security Governance - Policies and Procedures						Low	Low					
Information Technology	Logging and Monitoring - Logging and Monitoring Policy											Low	
Information Technology	Data Protection - Data Center Moisture Detection									Low			
Information Technology	IT Operations - Asset Tracking											Low	
Information Technology	Monitoring of Third-Party Service Providers		Low										



Smart decisions. Lasting value.™

Recommendations

Conclusions

- A series of minor-moderate improvements in financial and **information technology controls** could significantly improve assurance over reliability of data (e.g. guidance on data protection considering Sunshine State laws)
- An enhanced focus on **third-party risk management** would increase transparency and accountability among university service providers (and help manage costs).
- Building upon initiatives that **share information, dialogue, and resources** across the SUS could help address major challenges (e.g. best practices in controls, managing shared services agreements, interpreting BOG regulations).
- Establishing an **enterprise risk management (ERM) program** for the SUS could be an effective way to address the observations and themes and numerous other challenges using a comprehensive, structured, and methodical approach.

Smart decisions. Lasting value.™

Questions?