Federal Computer Security Program Managers' Forum

August 9, 2012

Electricity Subsector Cybersecurity Risk Management Process

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

DEPARTMENT OF ENERGY · UNITED STATES OF AMERICA

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Risk Management Process Initiative

- The Risk Management Process (RMP) initiative is a public-private collaboration to develop a cybersecurity risk management guideline.

- This work is led by DOE in coordination with NIST and NERC, and includes representatives from the public and private sectors.
  - Utilities are nominated by APPA, EEI, and NRECA and form the core team
  - DOE, NIST, NERC, SGIP-CSWG, DHS and FERC are also part of the core team
  - A subject matter expert (SME) team is composed of utility representatives and other stakeholders to provide additional guidance to the team

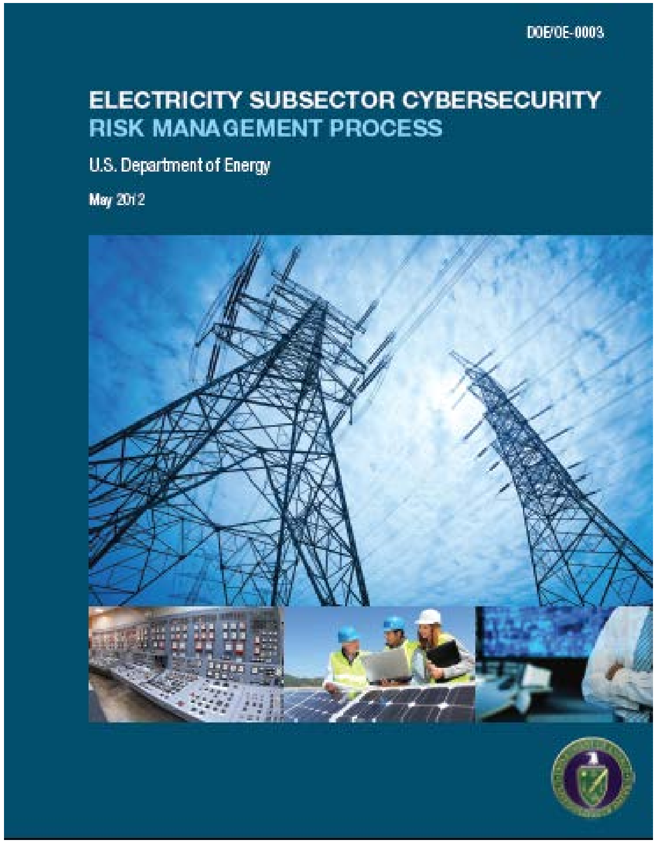
So What is the RMP About?

- It’s about people and the organizations in which they operate
  - How to organize people to effectively make risk informed decisions
  - Target of RMP is cybersecurity risk but fundamentally could be applied to any risk management domain

Electricity subsector organizations deal with risk every day in meeting their business objectives…this management of risk is conducted as an interactive, ongoing process as part of normal operations.

Guiding Principles of the RMP

- Based on NIST 800-39: Managing Information Security Risk
- Describe “what” not “how”
- Adaptable to any size or type of organization
- Cybersecurity alignment with mission and business processes



DOE/OE-0003

ELECTRICITY SUBSECTOR CYBERSECURITY RISK MANAGEMENT PROCESS

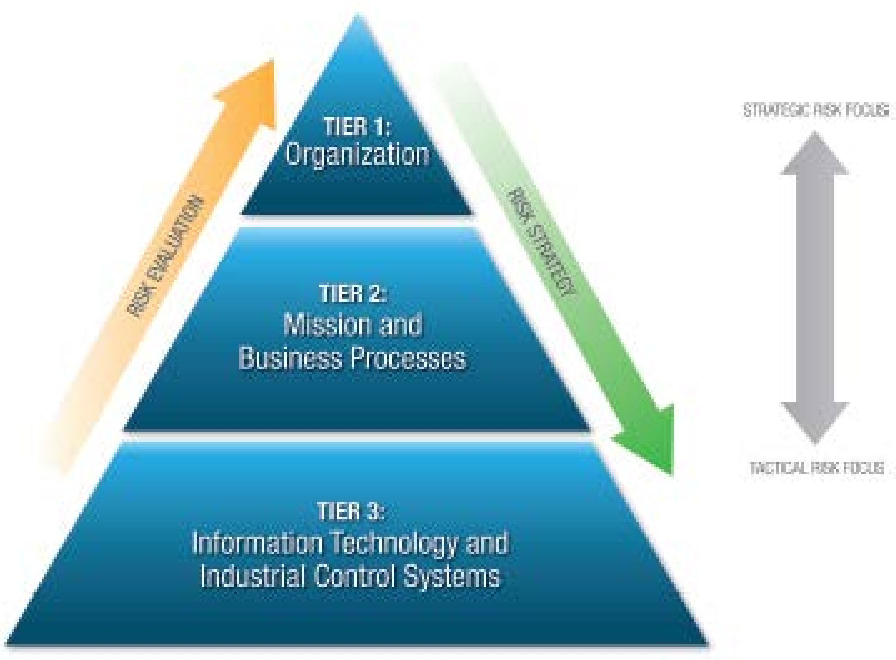
U.S. Department of Energy

May 2012

RMP Overview: Risk Management Model

- The Risk Management Model is a three-tiered structure that provides a comprehensive view of an organization
- It provides a structure for how cybersecurity risk management activities are undertaken across an organization
- Strategy is communicated down through the organization, risk evaluations are communicated up

Figure 1: Risk Management Model

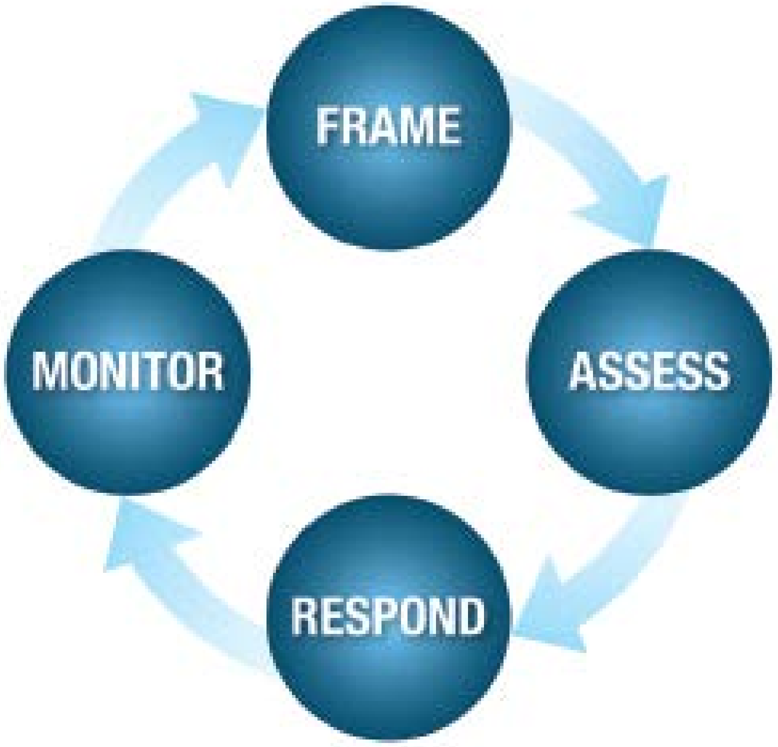


RMP Overview: Risk Management Cycle

- The Risk Management Cycle provides four elements that structure an organization’s approach to cybersecurity risk management

- The Risk Management Cycle is not static but a continuous process, constantly re-informed by the changing risk landscape as well as by organizational priorities and functional changes

Figure 2: Risk Management Cycle



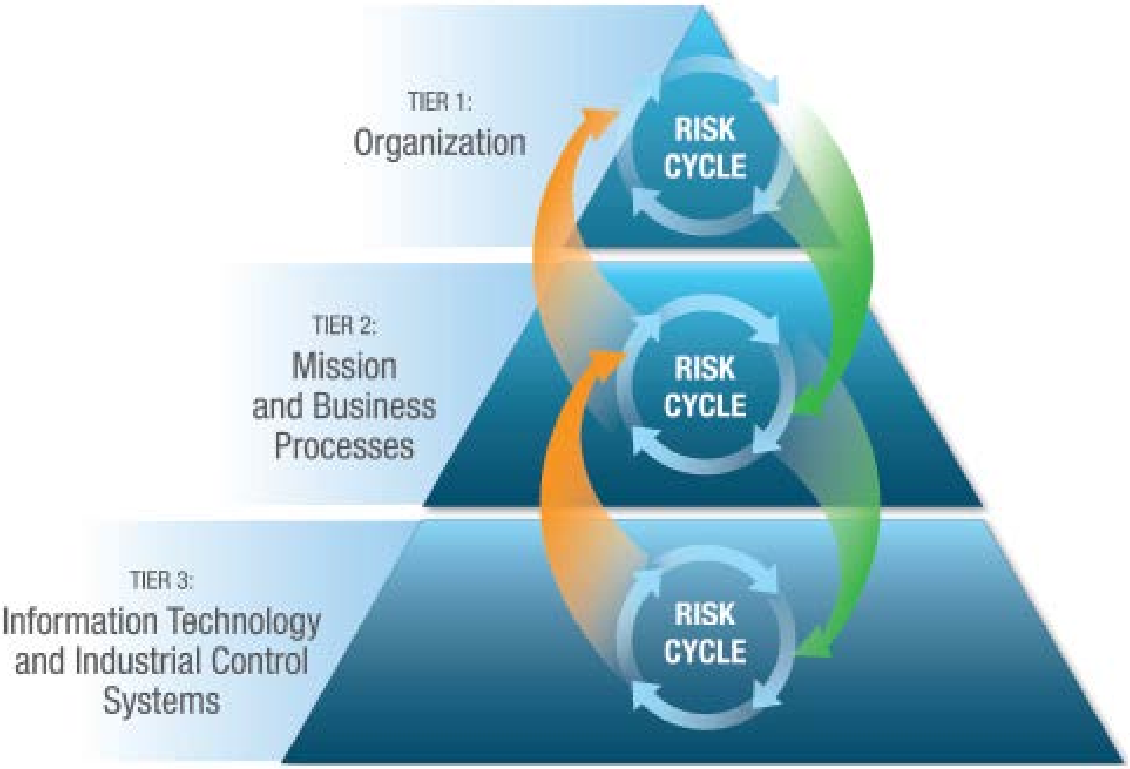
RMP Overview: Risk Management Cycle cont'd

- Risk Framing
  - Describes the environment in which decisions are made
  - Assumptions, constraints, tolerance, priorities
- Risk Assessment
  - Identify, prioritize, and estimate risk to organization
  - Includes supply chain and external service providers
- Risk Response
  - How the organization responds to risk
  - Develop courses of action and implement
- Risk Monitoring
  - How risks are monitored and communicated over time
  - Verify and evaluate risk response measures

RMP Overview: Risk Management Process

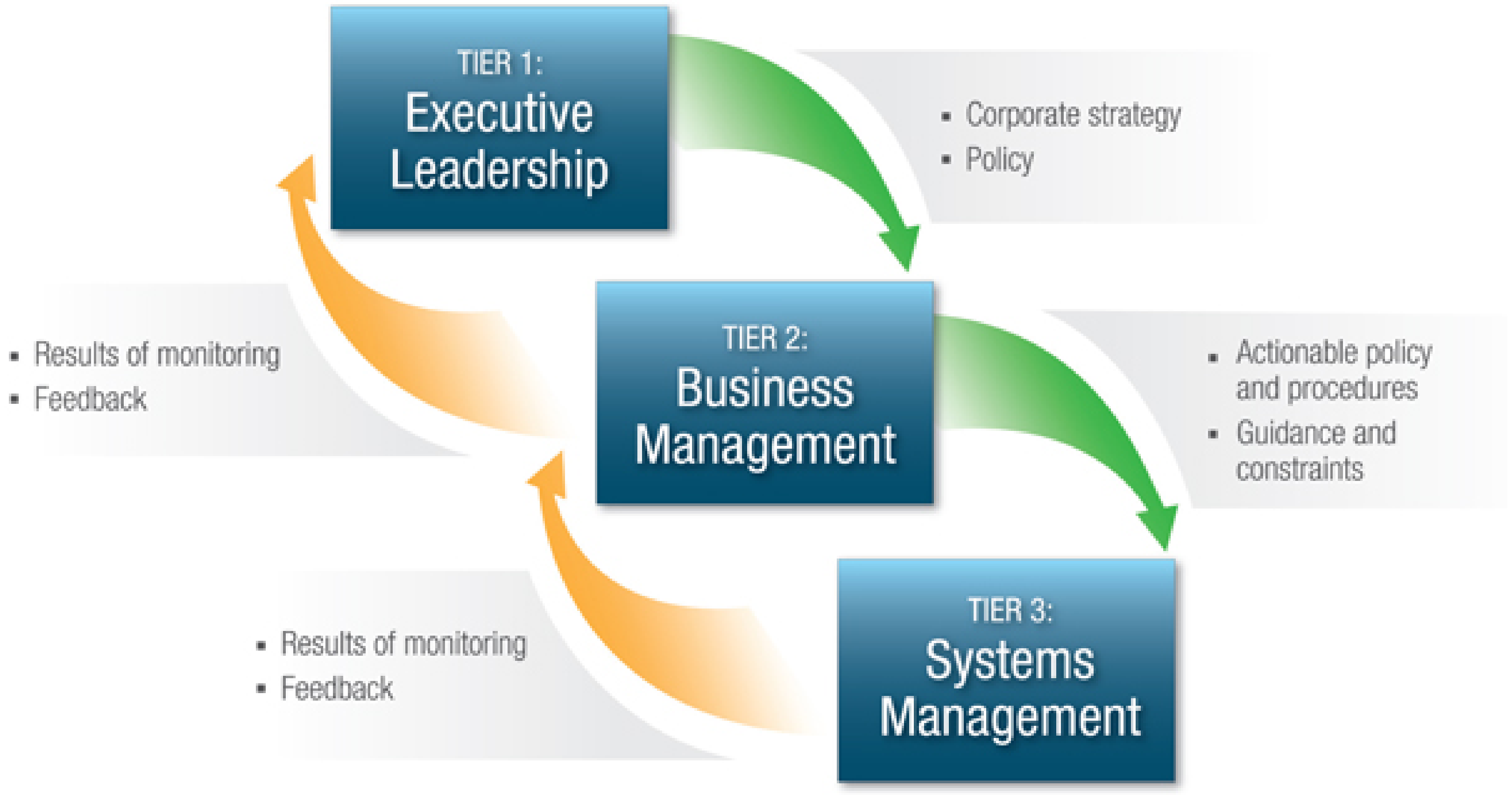
The Risk Management Process is the application of the risk management cycle to each of the tiers in the risk management model

Figure 3: Risk Management Process

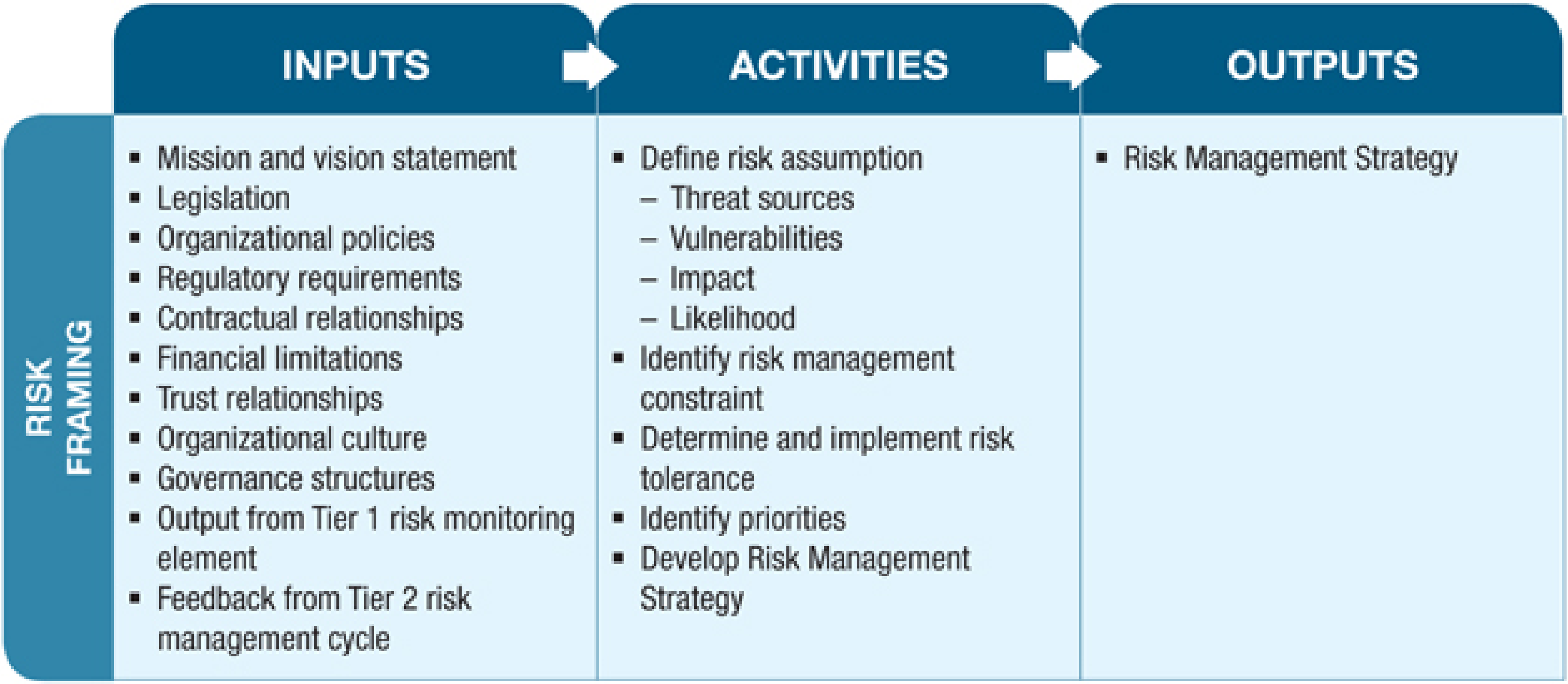

TIER 1:
Organization
RISK CYCLE
TIER 2:
Mission and Business Processes
RISK CYCLE
TIER 3:
Information Technology and Industrial Control Systems
RISK CYCLE

RMP Overview: Information Flowchart

Figure 4: RMP Information Flowchart

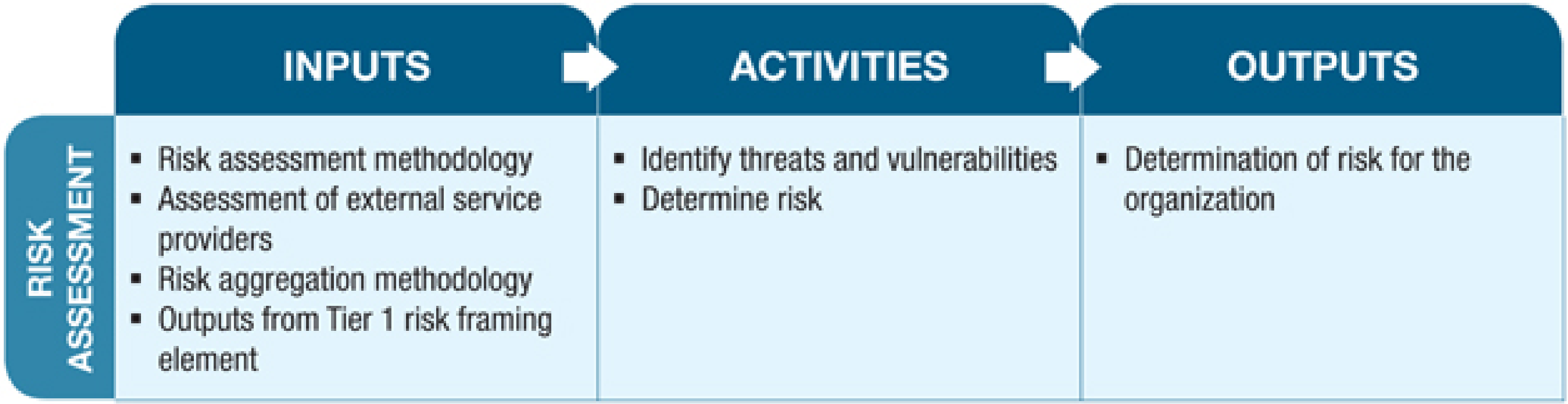


Tier 1: Organization Risk Framing



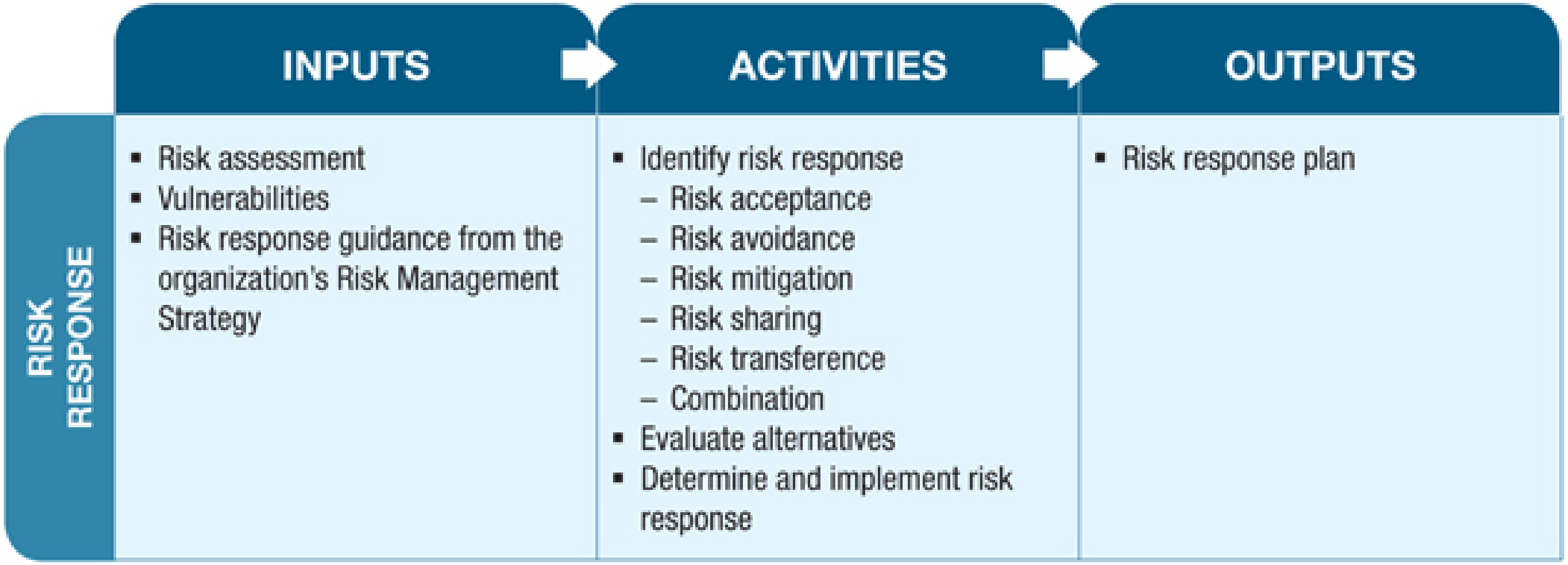
	INPUTS	ACTIVITIES	OUTPUTS
RISK FRAMING	▪ Mission and vision statement ▪ Legislation ▪ Organizational policies ▪ Regulatory requirements ▪ Contractual relationships ▪ Financial limitations ▪ Trust relationships ▪ Organizational culture ▪ Governance structures ▪ Output from Tier 1 risk monitoring element ▪ Feedback from Tier 2 risk management cycle	▪ Define risk assumption – Threat sources – Vulnerabilities – Impact – Likelihood ▪ Identify risk management constraint ▪ Determine and implement risk tolerance ▪ Identify priorities ▪ Develop Risk Management Strategy	▪ Risk Management Strategy

Tier 1: Organization Risk Assessment



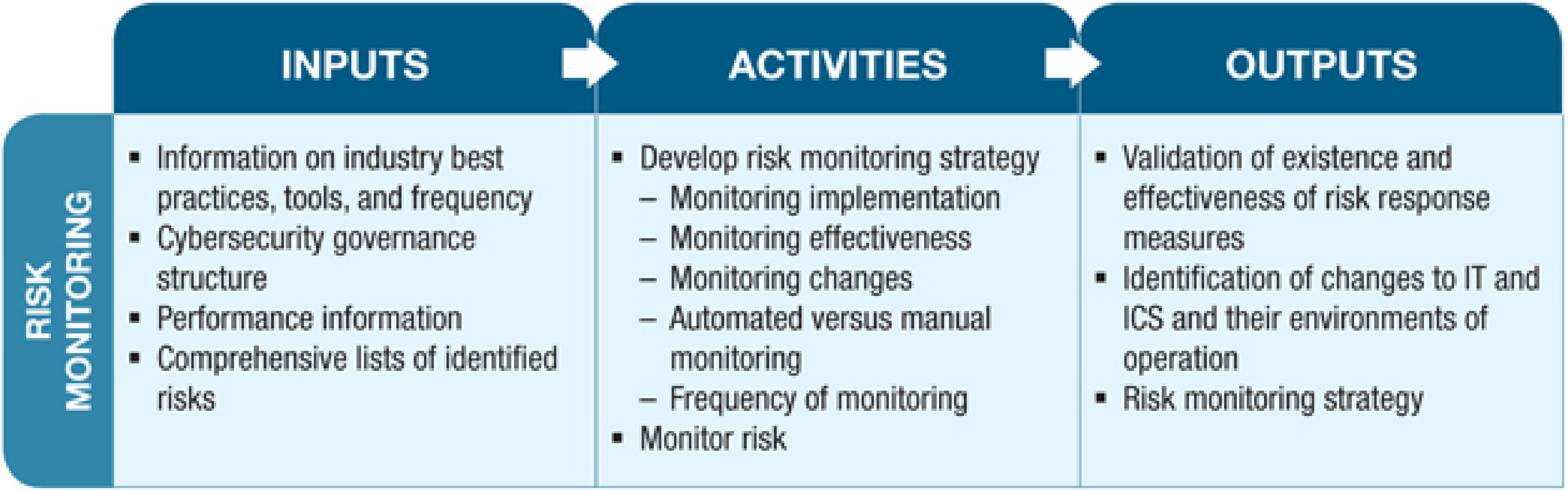
	INPUTS	ACTIVITIES	OUTPUTS
RISK ASSESSMENT	▪ Risk assessment methodology ▪ Assessment of external service providers ▪ Risk aggregation methodology ▪ Outputs from Tier 1 risk framing element	▪ Identify threats and vulnerabilities ▪ Determine risk	▪ Determination of risk for the organization

Tier 1: Organization Risk Response



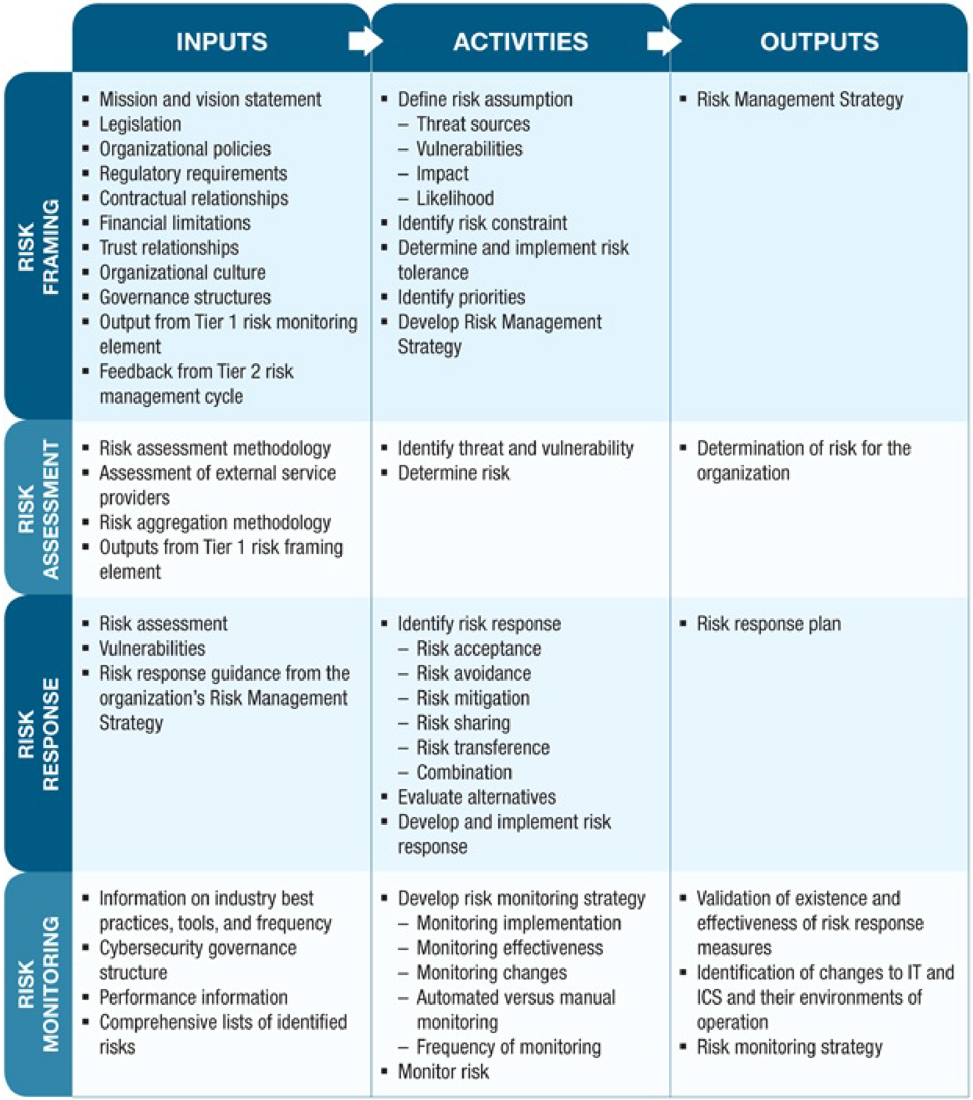
	INPUTS	ACTIVITIES	OUTPUTS
RISK RESPONSE	▪ Risk assessment ▪ Vulnerabilities ▪ Risk response guidance from the organization's Risk Management Strategy	▪ Identify risk response – Risk acceptance – Risk avoidance – Risk mitigation – Risk sharing – Risk transference – Combination ▪ Evaluate alternatives ▪ Determine and implement risk response	▪ Risk response plan

Tier 1: Organization Risk Monitoring



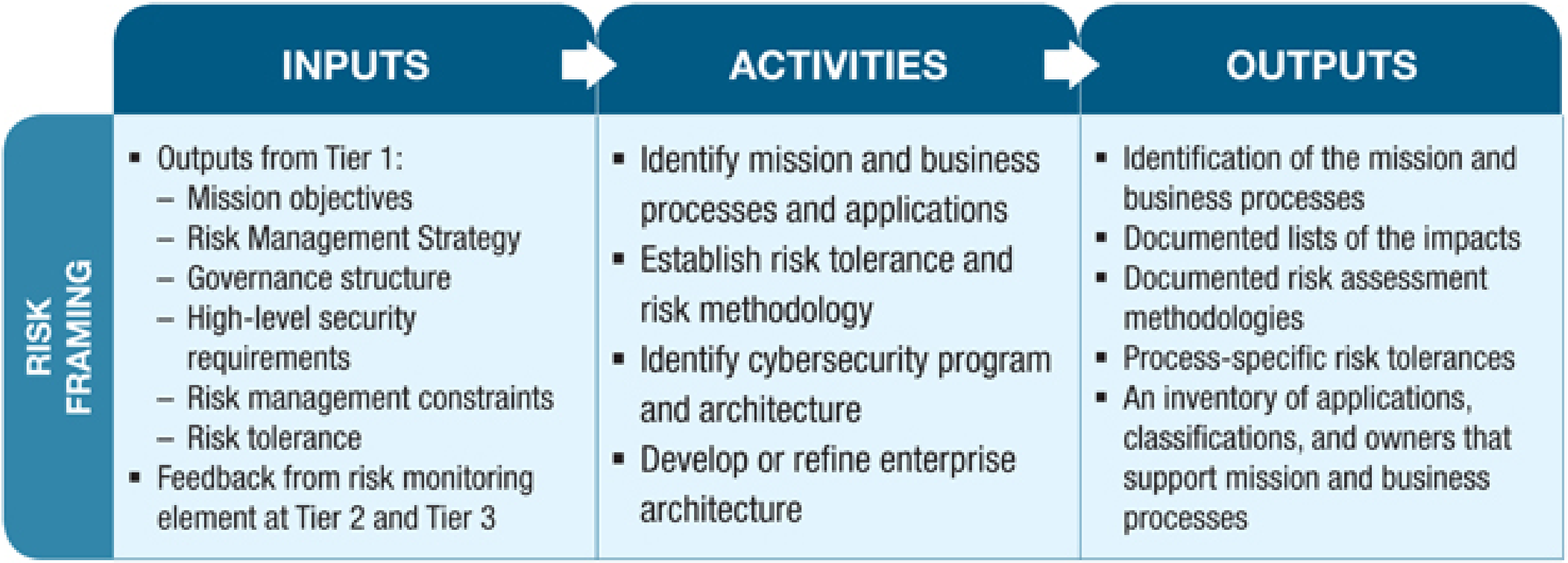
	INPUTS	ACTIVITIES	OUTPUTS
RISK MONITORING	▪ Information on industry best practices, tools, and frequency ▪ Cybersecurity governance structure ▪ Performance information ▪ Comprehensive lists of identified risks	▪ Develop risk monitoring strategy – Monitoring implementation – Monitoring effectiveness – Monitoring changes – Automated versus manual monitoring – Frequency of monitoring ▪ Monitor risk	▪ Validation of existence and effectiveness of risk response measures ▪ Identification of changes to IT and ICS and their environments of operation ▪ Risk monitoring strategy

Tier 1: Organization Summary



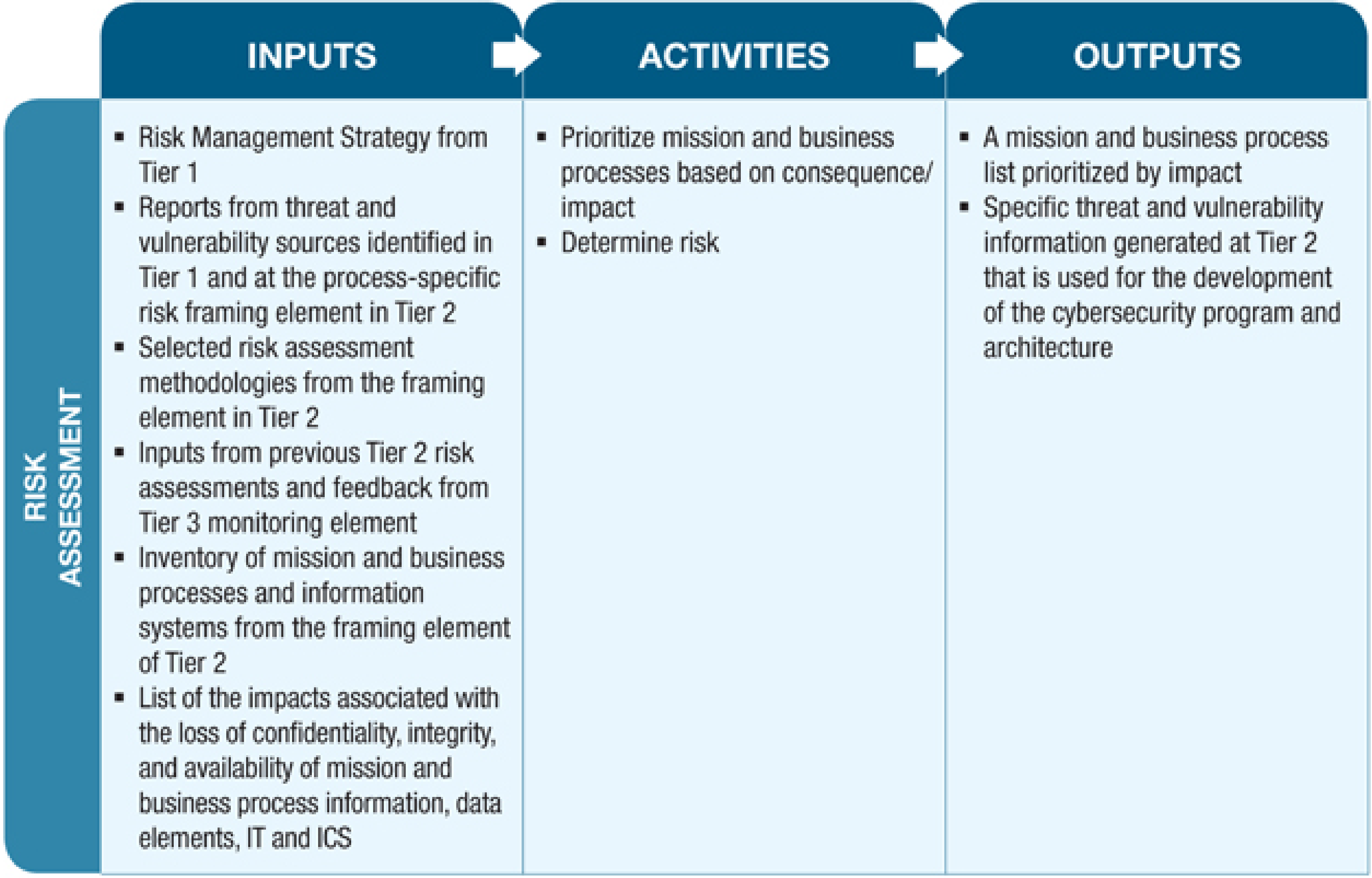
	INPUTS	ACTIVITIES	OUTPUTS
RISK FRAMING	▪ Mission and vision statement ▪ Legislation ▪ Organizational policies ▪ Regulatory requirements ▪ Contractual relationships ▪ Financial limitations ▪ Trust relationships ▪ Organizational culture ▪ Governance structures ▪ Output from Tier 1 risk monitoring element ▪ Feedback from Tier 2 risk management cycle	▪ Define risk assumption – Threat sources – Vulnerabilities – Impact – Likelihood ▪ Identify risk constraint ▪ Determine and implement risk tolerance ▪ Identify priorities ▪ Develop Risk Management Strategy	▪ Risk Management Strategy
RISK ASSESSMENT	▪ Risk assessment methodology ▪ Assessment of external service providers ▪ Risk aggregation methodology ▪ Outputs from Tier 1 risk framing element	▪ Identify threat and vulnerability ▪ Determine risk	▪ Determination of risk for the organization
RISK RESPONSE	▪ Risk assessment ▪ Vulnerabilities ▪ Risk response guidance from the organization's Risk Management Strategy	▪ Identify risk response – Risk acceptance – Risk avoidance – Risk mitigation – Risk sharing – Risk transference – Combination ▪ Evaluate alternatives ▪ Develop and implement risk response	▪ Risk response plan
RISK MONITORING	▪ Information on industry best practices, tools, and frequency ▪ Cybersecurity governance structure ▪ Performance information ▪ Comprehensive lists of identified risks	▪ Develop risk monitoring strategy – Monitoring implementation – Monitoring effectiveness – Monitoring changes – Automated versus manual monitoring – Frequency of monitoring ▪ Monitor risk	▪ Validation of existence and effectiveness of risk response measures ▪ Identification of changes to IT and ICS and their environments of operation ▪ Risk monitoring strategy

Tier 2: Mission and Business Process Risk Framing



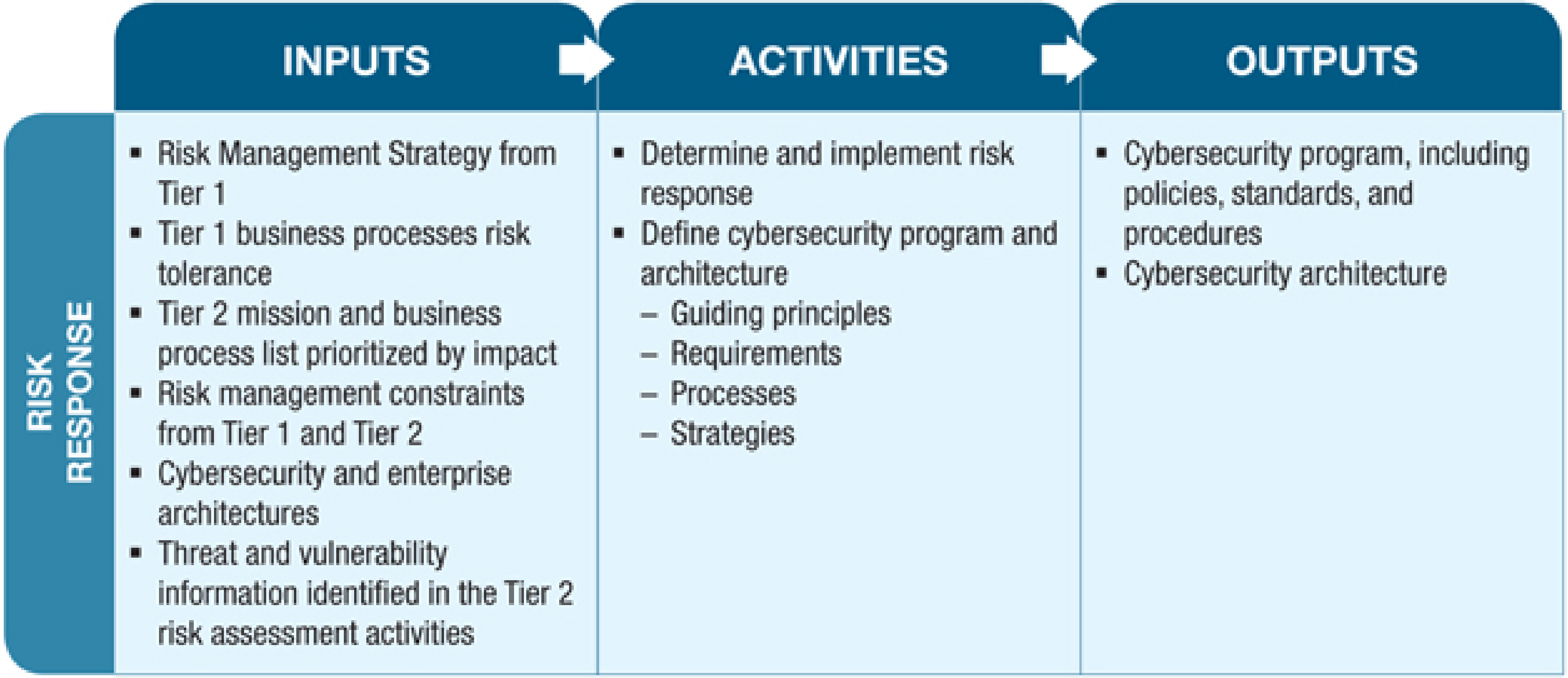
	INPUTS	ACTIVITIES	OUTPUTS
RISK FRAMING	▪ Outputs from Tier 1: – Mission objectives – Risk Management Strategy – Governance structure – High-level security requirements – Risk management constraints – Risk tolerance ▪ Feedback from risk monitoring element at Tier 2 and Tier 3	▪ Identify mission and business processes and applications ▪ Establish risk tolerance and risk methodology ▪ Identify cybersecurity program and architecture ▪ Develop or refine enterprise architecture	▪ Identification of the mission and business processes ▪ Documented lists of the impacts ▪ Documented risk assessment methodologies ▪ Process-specific risk tolerances ▪ An inventory of applications, classifications, and owners that support mission and business processes

Tier 2: Mission and Business Process Risk Assessment



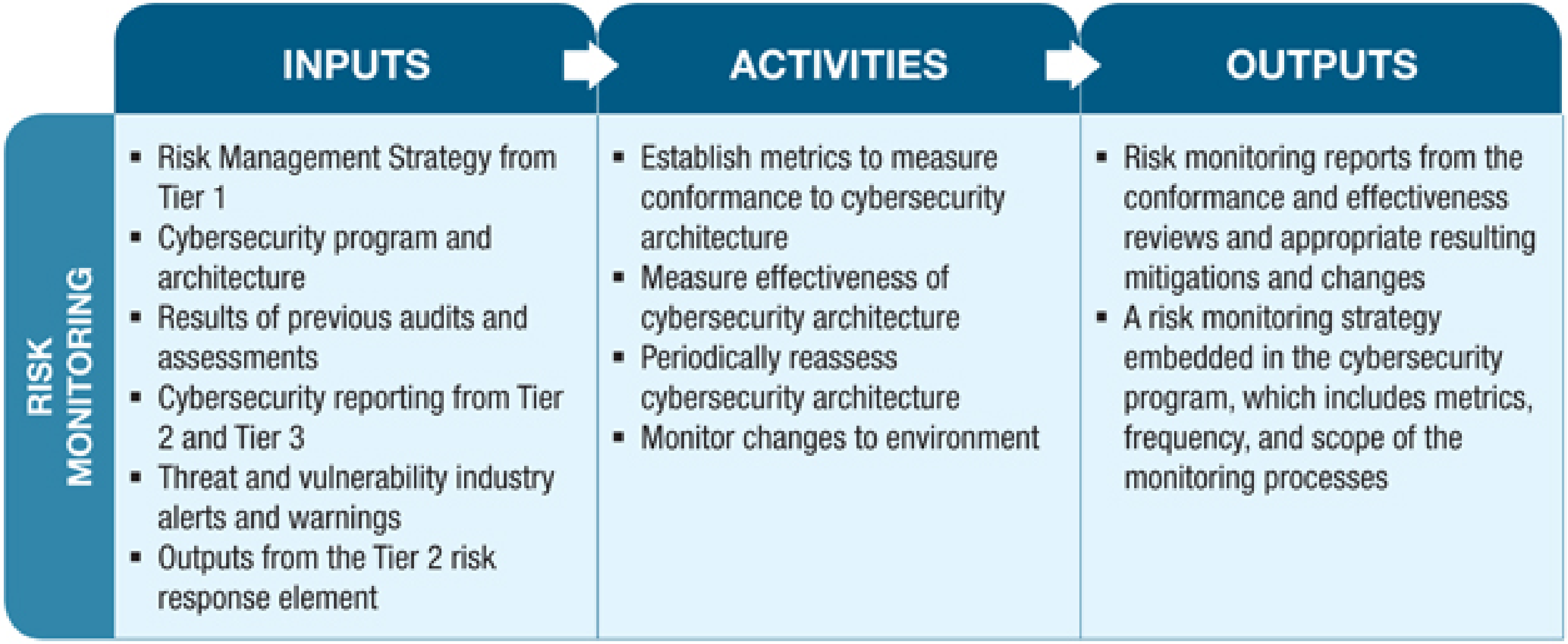
	INPUTS	ACTIVITIES	OUTPUTS
RISK ASSESSMENT	▪ Risk Management Strategy from Tier 1 ▪ Reports from threat and vulnerability sources identified in Tier 1 and at the process-specific risk framing element in Tier 2 ▪ Selected risk assessment methodologies from the framing element in Tier 2 ▪ Inputs from previous Tier 2 risk assessments and feedback from Tier 3 monitoring element ▪ Inventory of mission and business processes and information systems from the framing element of Tier 2 ▪ List of the impacts associated with the loss of confidentiality, integrity, and availability of mission and business process information, data elements, IT and ICS	▪ Prioritize mission and business processes based on consequence/ impact ▪ Determine risk	▪ A mission and business process list prioritized by impact ▪ Specific threat and vulnerability information generated at Tier 2 that is used for the development of the cybersecurity program and architecture

Tier 2: Mission and Business Process Risk Response



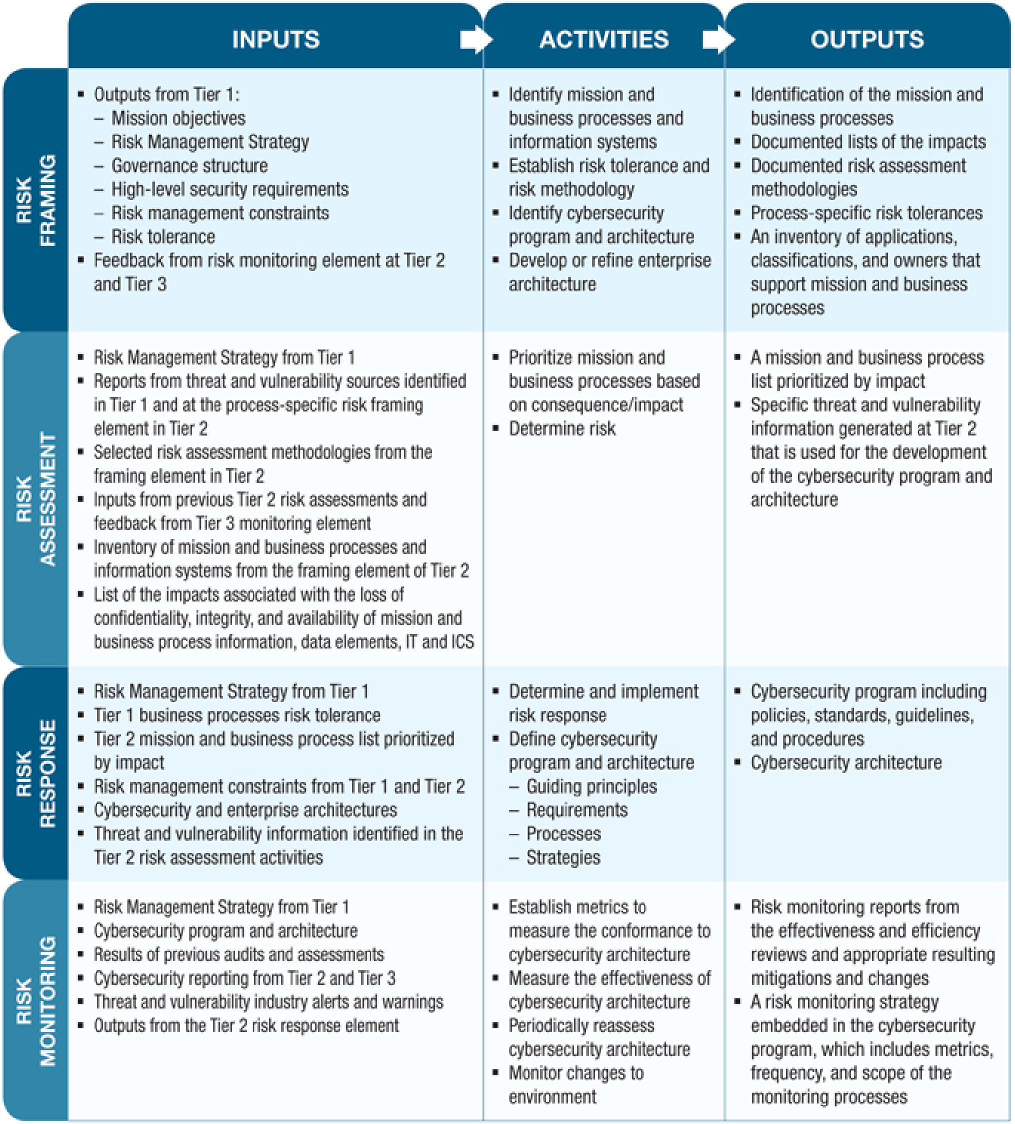
	INPUTS	ACTIVITIES	OUTPUTS
RISK RESPONSE	▪ Risk Management Strategy from Tier 1 ▪ Tier 1 business processes risk tolerance ▪ Tier 2 mission and business process list prioritized by impact ▪ Risk management constraints from Tier 1 and Tier 2 ▪ Cybersecurity and enterprise architectures ▪ Threat and vulnerability information identified in the Tier 2 risk assessment activities	▪ Determine and implement risk response ▪ Define cybersecurity program and architecture – Guiding principles – Requirements – Processes – Strategies	▪ Cybersecurity program, including policies, standards, and procedures ▪ Cybersecurity architecture

Tier 2: Mission and Business Process Risk Monitoring



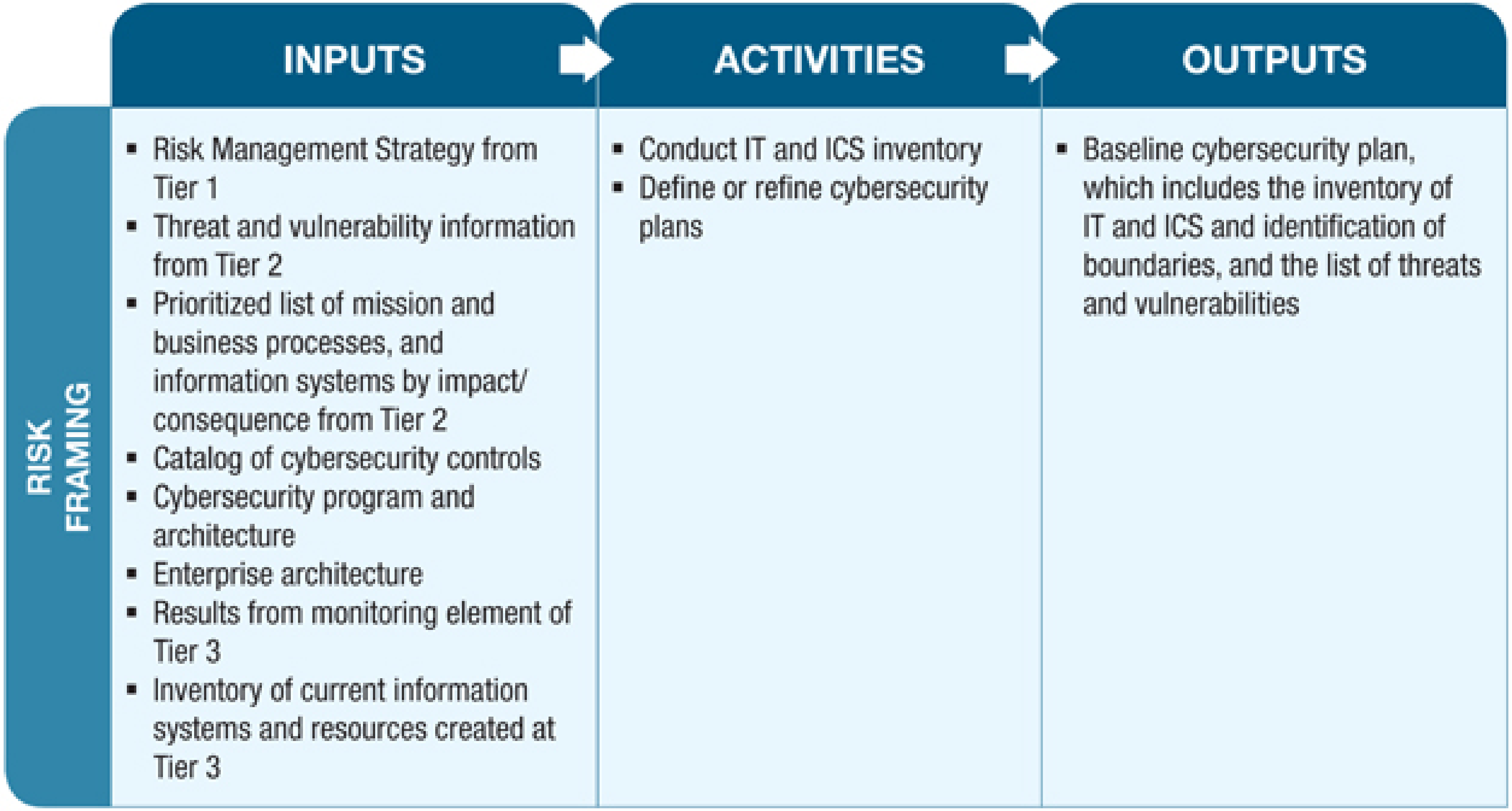
	INPUTS	ACTIVITIES	OUTPUTS
RISK MONITORING	▪ Risk Management Strategy from Tier 1 ▪ Cybersecurity program and architecture ▪ Results of previous audits and assessments ▪ Cybersecurity reporting from Tier 2 and Tier 3 ▪ Threat and vulnerability industry alerts and warnings ▪ Outputs from the Tier 2 risk response element	▪ Establish metrics to measure conformance to cybersecurity architecture ▪ Measure effectiveness of cybersecurity architecture ▪ Periodically reassess cybersecurity architecture ▪ Monitor changes to environment	▪ Risk monitoring reports from the conformance and effectiveness reviews and appropriate resulting mitigations and changes ▪ A risk monitoring strategy embedded in the cybersecurity program, which includes metrics, frequency, and scope of the monitoring processes

Tier 2: Mission and Business Process Summary



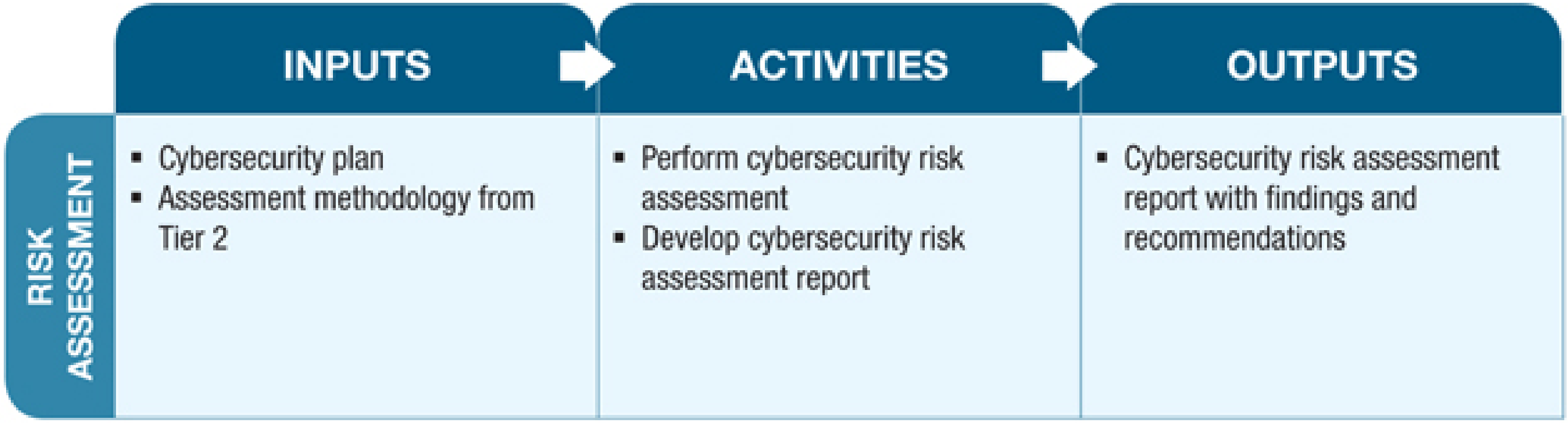
	INPUTS	ACTIVITIES	OUTPUTS
RISK FRAMING	▪ Outputs from Tier 1: – Mission objectives – Risk Management Strategy – Governance structure – High-level security requirements – Risk management constraints – Risk tolerance ▪ Feedback from risk monitoring element at Tier 2 and Tier 3	▪ Identify mission and business processes and information systems ▪ Establish risk tolerance and risk methodology ▪ Identify cybersecurity program and architecture ▪ Develop or refine enterprise architecture	▪ Identification of the mission and business processes ▪ Documented lists of the impacts ▪ Documented risk assessment methodologies ▪ Process-specific risk tolerances ▪ An inventory of applications, classifications, and owners that support mission and business processes
RISK ASSESSMENT	▪ Risk Management Strategy from Tier 1 ▪ Reports from threat and vulnerability sources identified in Tier 1 and at the process-specific risk framing element in Tier 2 ▪ Selected risk assessment methodologies from the framing element in Tier 2 ▪ Inputs from previous Tier 2 risk assessments and feedback from Tier 3 monitoring element ▪ Inventory of mission and business processes and information systems from the framing element of Tier 2 ▪ List of the impacts associated with the loss of confidentiality, integrity, and availability of mission and business process information, data elements, IT and ICS	▪ Prioritize mission and business processes based on consequence/impact ▪ Determine risk	▪ A mission and business process list prioritized by impact ▪ Specific threat and vulnerability information generated at Tier 2 that is used for the development of the cybersecurity program and architecture
RISK RESPONSE	▪ Risk Management Strategy from Tier 1 ▪ Tier 1 business processes risk tolerance ▪ Tier 2 mission and business process list prioritized by impact ▪ Risk management constraints from Tier 1 and Tier 2 ▪ Cybersecurity and enterprise architectures ▪ Threat and vulnerability information identified in the Tier 2 risk assessment activities	▪ Determine and implement risk response ▪ Define cybersecurity program and architecture – Guiding principles – Requirements – Processes – Strategies	▪ Cybersecurity program including policies, standards, guidelines, and procedures ▪ Cybersecurity architecture
RISK MONITORING	▪ Risk Management Strategy from Tier 1 ▪ Cybersecurity program and architecture ▪ Results of previous audits and assessments ▪ Cybersecurity reporting from Tier 2 and Tier 3 ▪ Threat and vulnerability industry alerts and warnings ▪ Outputs from the Tier 2 risk response element	▪ Establish metrics to measure the conformance to cybersecurity architecture ▪ Measure the effectiveness of cybersecurity architecture ▪ Periodically reassess cybersecurity architecture ▪ Monitor changes to environment	▪ Risk monitoring reports from the effectiveness and efficiency reviews and appropriate resulting mitigations and changes ▪ A risk monitoring strategy embedded in the cybersecurity program, which includes metrics, frequency, and scope of the monitoring processes

Tier 3: IT and ICS Risk Framing



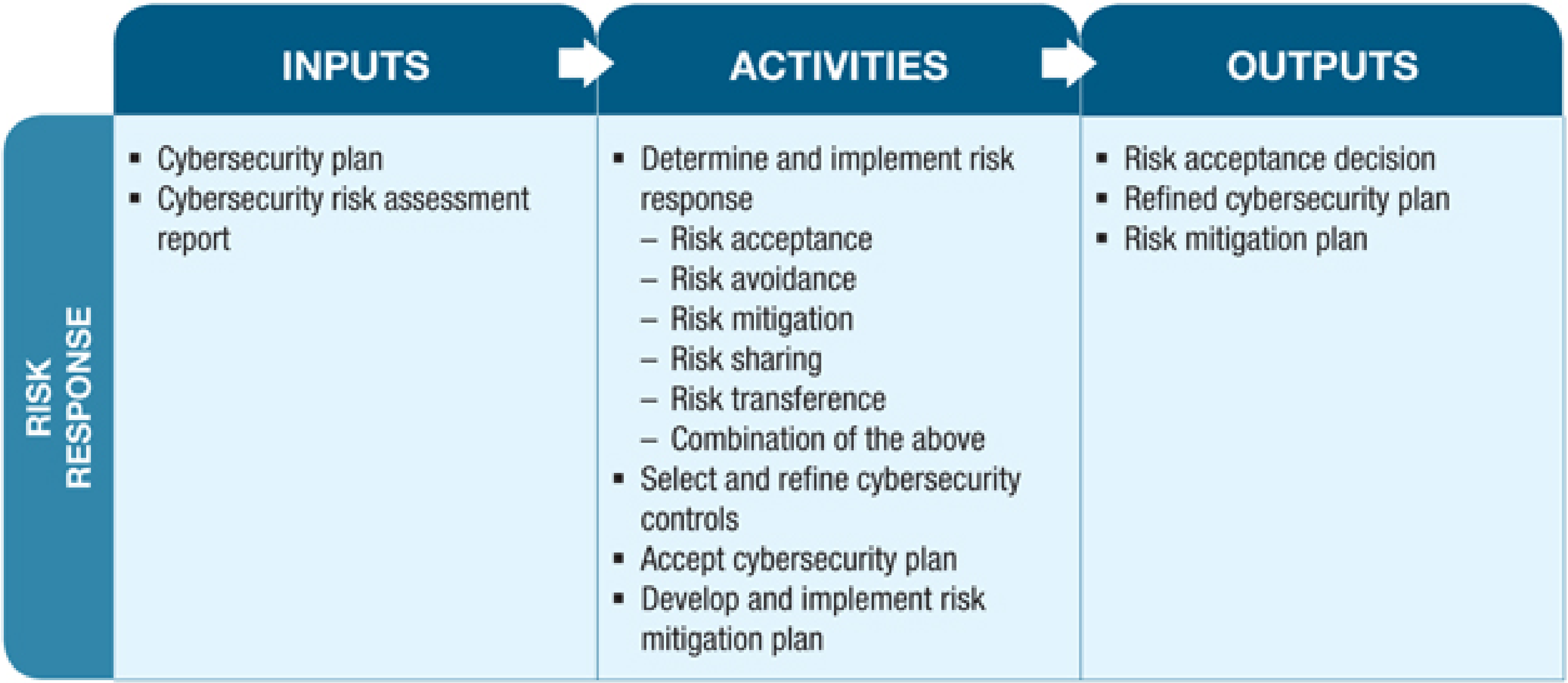
	INPUTS	ACTIVITIES	OUTPUTS
RISK FRAMING	▪ Risk Management Strategy from Tier 1 ▪ Threat and vulnerability information from Tier 2 ▪ Prioritized list of mission and business processes, and information systems by impact/ consequence from Tier 2 ▪ Catalog of cybersecurity controls ▪ Cybersecurity program and architecture ▪ Enterprise architecture ▪ Results from monitoring element of Tier 3 ▪ Inventory of current information systems and resources created at Tier 3	▪ Conduct IT and ICS inventory ▪ Define or refine cybersecurity plans	▪ Baseline cybersecurity plan, which includes the inventory of IT and ICS and identification of boundaries, and the list of threats and vulnerabilities

Tier 3: IT and ICS Risk Assessment



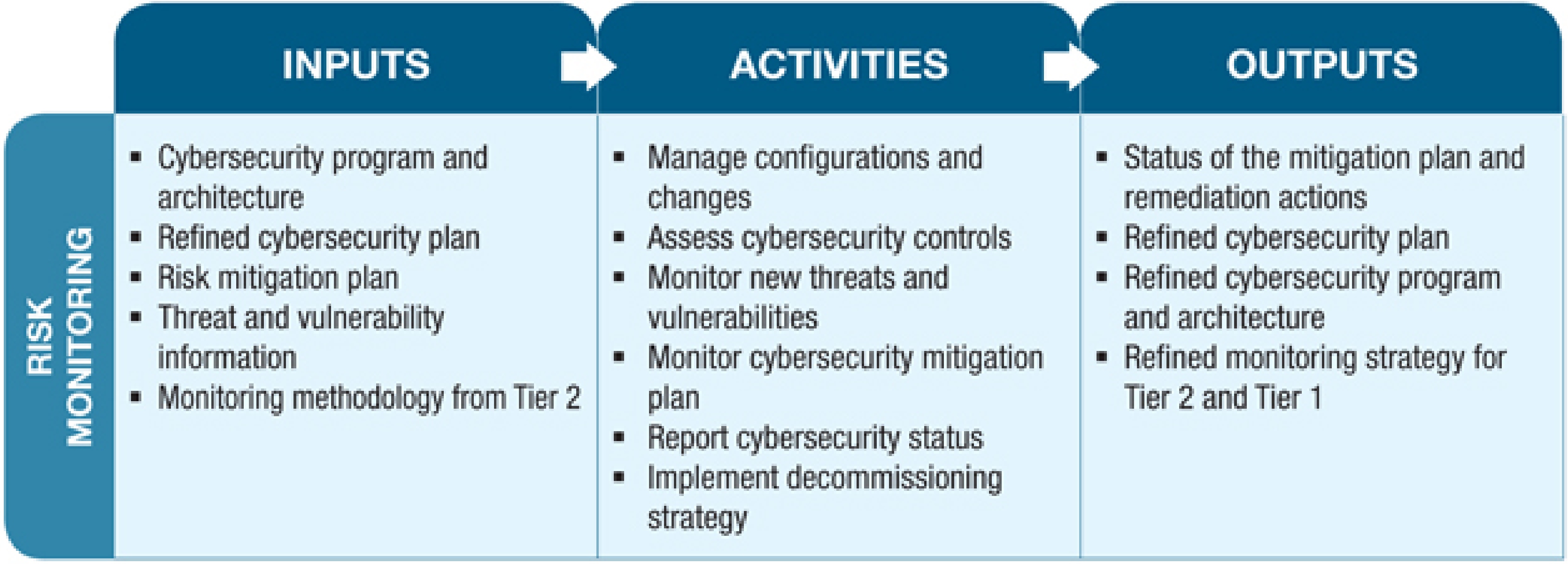
	INPUTS	ACTIVITIES	OUTPUTS
RISK ASSESSMENT	▪ Cybersecurity plan ▪ Assessment methodology from Tier 2	▪ Perform cybersecurity risk assessment ▪ Develop cybersecurity risk assessment report	▪ Cybersecurity risk assessment report with findings and recommendations

Tier 3: IT and ICS Risk Response



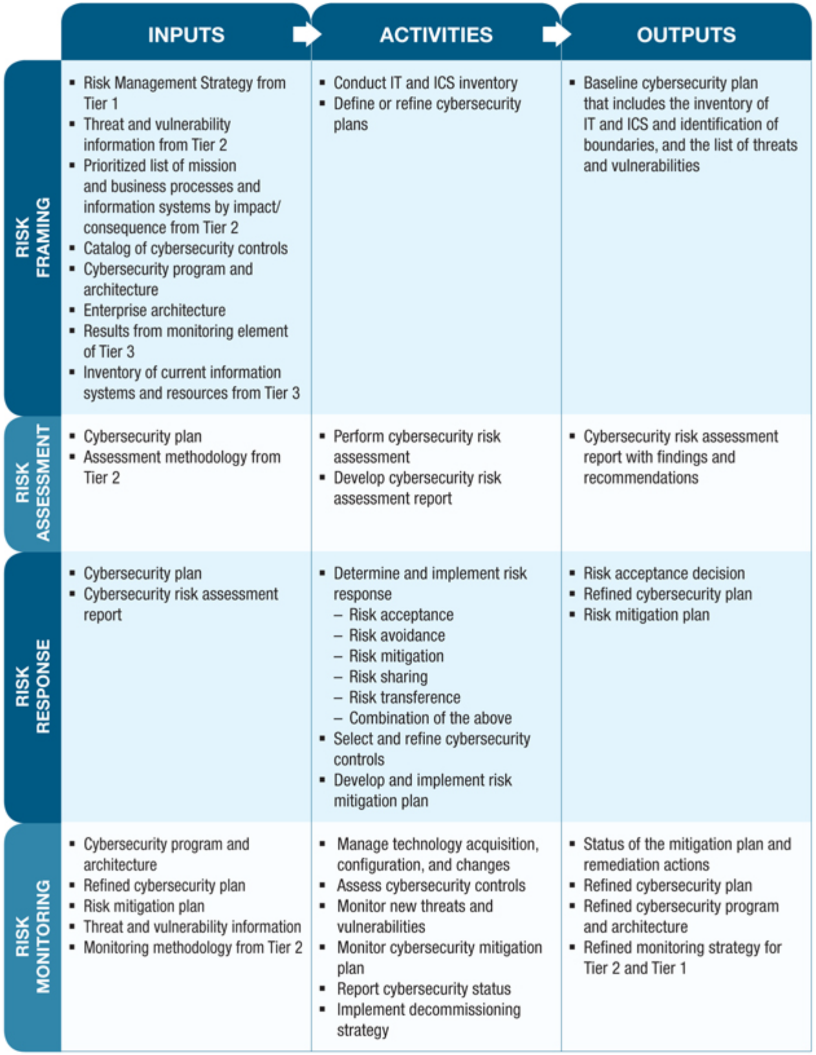
	INPUTS	ACTIVITIES	OUTPUTS
RISK RESPONSE	▪ Cybersecurity plan ▪ Cybersecurity risk assessment report	▪ Determine and implement risk response – Risk acceptance – Risk avoidance – Risk mitigation – Risk sharing – Risk transference – Combination of the above ▪ Select and refine cybersecurity controls ▪ Accept cybersecurity plan ▪ Develop and implement risk mitigation plan	▪ Risk acceptance decision ▪ Refined cybersecurity plan ▪ Risk mitigation plan

Tier 3: IT and ICS Risk Monitoring



	INPUTS	ACTIVITIES	OUTPUTS
RISK MONITORING	▪ Cybersecurity program and architecture ▪ Refined cybersecurity plan ▪ Risk mitigation plan ▪ Threat and vulnerability information ▪ Monitoring methodology from Tier 2	▪ Manage configurations and changes ▪ Assess cybersecurity controls ▪ Monitor new threats and vulnerabilities ▪ Monitor cybersecurity mitigation plan ▪ Report cybersecurity status ▪ Implement decommissioning strategy	▪ Status of the mitigation plan and remediation actions ▪ Refined cybersecurity plan ▪ Refined cybersecurity program and architecture ▪ Refined monitoring strategy for Tier 2 and Tier 1

Tier 3: IT and ICS Summary



	INPUTS	ACTIVITIES	OUTPUTS
RISK FRAMING	▪ Risk Management Strategy from Tier 1 ▪ Threat and vulnerability information from Tier 2 ▪ Prioritized list of mission and business processes and information systems by impact/ consequence from Tier 2 ▪ Catalog of cybersecurity controls ▪ Cybersecurity program and architecture ▪ Enterprise architecture ▪ Results from monitoring element of Tier 3 ▪ Inventory of current information systems and resources from Tier 3	▪ Conduct IT and ICS inventory ▪ Define or refine cybersecurity plans	▪ Baseline cybersecurity plan that includes the inventory of IT and ICS and identification of boundaries, and the list of threats and vulnerabilities
RISK ASSESSMENT	▪ Cybersecurity plan ▪ Assessment methodology from Tier 2	▪ Perform cybersecurity risk assessment ▪ Develop cybersecurity risk assessment report	▪ Cybersecurity risk assessment report with findings and recommendations
RISK RESPONSE	▪ Cybersecurity plan ▪ Cybersecurity risk assessment report	▪ Determine and implement risk response – Risk acceptance – Risk avoidance – Risk mitigation – Risk sharing – Risk transference – Combination of the above ▪ Select and refine cybersecurity controls ▪ Develop and implement risk mitigation plan	▪ Risk acceptance decision ▪ Refined cybersecurity plan ▪ Risk mitigation plan
RISK MONITORING	▪ Cybersecurity program and architecture ▪ Refined cybersecurity plan ▪ Risk mitigation plan ▪ Threat and vulnerability information ▪ Monitoring methodology from Tier 2	▪ Manage technology acquisition, configuration, and changes ▪ Assess cybersecurity controls ▪ Monitor new threats and vulnerabilities ▪ Monitor cybersecurity mitigation plan ▪ Report cybersecurity status ▪ Implement decommissioning strategy	▪ Status of the mitigation plan and remediation actions ▪ Refined cybersecurity plan ▪ Refined cybersecurity program and architecture ▪ Refined monitoring strategy for Tier 2 and Tier 1

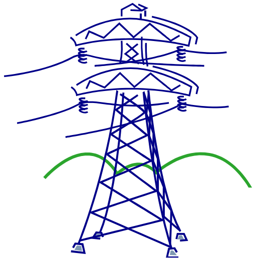
RMP: A Case Study

Scott Saunders, CISSP, CISM, MSISA

Sacramento Municipal Utility District (SMUD)

Why a Case Study

- Transition theoretical ideas into real world
- Create a real word implementation framework
- Validate the RMP
- Provide a “Starting point” for a utility
- Able to highlight opportunities
- Able to highlight struggles



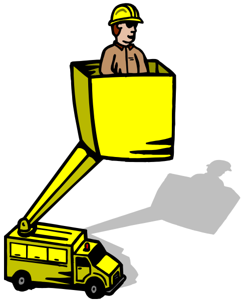
Papaya Power

Case Study Directives

- Primary Directive: under 40 pages

- Secondary Directive: fun to read

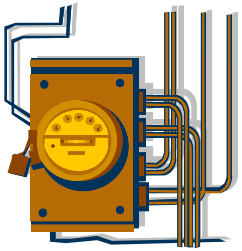
- Tertiary Directive: weave realism into story



Papaya
Power

Case Study Characteristics

- Use casual conversation storytelling
- Create characters seen in real utilities
- Create same angst seen in real utilities
- Cover major activities of the RMP
- Reference existing related bodies of work
- Provide example inputs and outputs
- Provides drafting teams own Lessons Learned



Papaya
Power

Tier 1: Organization Business Impact Assessment

Priority	At-Risk Business Functions and Processes	Threats	Vulnerabilities	Impact	Probability	Constraints	Tolerances	Mitigation Action	Next Review Date
1	Power Operations	Anything that would impact reliability	*Remote access to grid control systems *Disruption or corruption of communications	* High impact * Outages * Fines	High	Need to have remote access to systems	We do not want to put reliability of the grid or our delivery of electricity to customers at risk.	Invest in robust protection to make sure that only our staff can get remote access, and are appropriately trained avoid mistakes.	
1	Metering-to-Cash	Disruption of systems used to perform fiscal operations or management	*Web site failure	* High impact *Loss of money, time, and resources to replacement/repair	High	Budget and financial constraints – how much money can be devoted to this effort this year… or future years?	We have to manage our current resources most efficiently. There isn't more money or more people.	Make sure there are adequate testing of the cybersecurity controls so the websites are resistive to hacking.	
1	Customer Services	*Negative press *Hacking customer information	*Escalation to regulators	*High impact * Fines * Loss of board confidence	High	State data/PII breach laws	We do not want to have any security breaches that put us in the news or gives the company negative press		

Papaya Power

Tier 2: Mission and Business Process Application Inventory

Application Inventory		Business Process Supported	Policy / Documentation	Priority	Rank (tier1/ tier2)	Impact	Prob.	Risk	Mitigations	Next Review Date
EMS in the POC	OT – Systems	Power Operations - Energy Mgmt	Partial	1	High/ high	High	High	Documentation and security policy	Complete documentation, set policy (Bill_S, Al_K)	July
Accounting	IT- Corp Systems	Metering to Cash - Accounting	Yes - policy	1	High/ med	High	High	Testing and access control		July
Billing	IT- Corp Systems	Metering to Cash - Billing	Yes - policy	1	High/ med	High	High	Missing incident controls		July
Remote Access Services	OT – Systems	Power Operations - Energy Mgmt	Partial	1	High/ high	High	High	Documentation and security policy	Complete documentation, set policy (Bill_S, Al_K)	July
Meters - Head in (outsourced)	IT- Corp Systems	Metering to Cash - Smart Meters	Outsourced?	2	High/ med	High	Med	Controls at contractor * review contracts		July
IT Access Control / RSA Type / VPN	IT- Corp Systems	Corporate Services	Yes - policy	2	/high	High	Med	Critical service, RSA incident?		July
SCADA Network	OT – Systems	Power Operations - Energy Mgmt	Partial	2	High/ med	High	Med	NERC CIP coverage		July

Papaya Power

Tier 3: IT and ICS Systems Inventory

Asset Name	Location	Serial Number	MAC Address	IP Address - Network ID - VLAN	System Association	Constraints	Threats / Vulns	Mitigations	Next Review Date
GE EMS 100 / UNIX Server	Building 2 POC Server Room	492992-0001	N/A	PineOpsNetwork A0023:9000:1	EMS	GE Proprietary			
GE EMS 100-A / Controller System / Data Feeds	Building 2 POC Server Room	5600923-2992-0001	N/A	PineOpsNetwork A0023:8567:61	EMS	GE Proprietary			
GE DMS Module	Building 2 POC Server Room	A9456-492992-0009	N/A	PineOpsNetwork A0023:6755:12	EMS	GE Proprietary			
GE Outage Management Controller	Building 2 POC Server Room	99-854777	N/A	PineOpsNetwork A0023:6928:70	Relay Protection System	GE Proprietary			
Terminal Services Module	Building 2 POC Server Room	45-78880	N/A	PineOpsNetwork A0023:6999:54	Relay Protection System	GE Proprietary			
Monitor Concentrator	Substations (all)	Varies	N/A	PineOpsNetwork vary	Relay Protection System	GE Proprietary			

Papaya Power

POAM

Risk Item	Date	Action Prescribed	Milestone	Assigned to	Completed	Notes (instructions)
EMS in the POC	4-Apr	Complete documentation, set security policy and standards		(Bill_S, Al_K)		Executives: Invest in robust protection to make sure that only our staff can get remote access, and are appropriately trained avoid mistakes
Relays & Protected	4-Apr	Complete documentation, set security policy and standards		(Bill_S, Al_K)		
Remote Access Services	4-Apr	Complete documentation, set security policy and standards		(Bill_S, Al_K)		
Billing	4-Apr	Update policy to address missing incident controls		Monet		Executives: Priority is Metering to Cash
Accounting	4-Apr	Update policy to address security testing and access control		Monet		Executives: Priority is Metering to Cash

Papaya Power

What Case Study does not do…

- Cover all business processes in the first implementation
- Prescribe specific methods to perform analysis
- Illustrate all communication issues
- Account for all utility corporate structures
- Include every step and activity in the RMP

Papaya Power

RMP: Next Steps

- Publish RMP Case Study
  - Fictional story
  - Illustrates how an organization may implement the RMP
- RMP Pilot
  - Work with 1-3 organizations to implement the RMP
  - Approx. 1 year engagement
  - Capture lessons learned and best practices
- RMP Website
  - Develop a resource center for the RMP
  - Provide additional content

RMP Information

Energy.gov: Office of Electricity Delivery and Energy Reliability

http://energy.gov/oe/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012

Contact Info:

Matt Light
DOE
matthew.light@hq.doe.gov

Marianne Swanson
NIST
marianne.swanson@nist.gov

Scott Saunders
SMUD
scott.saunders@smud.org