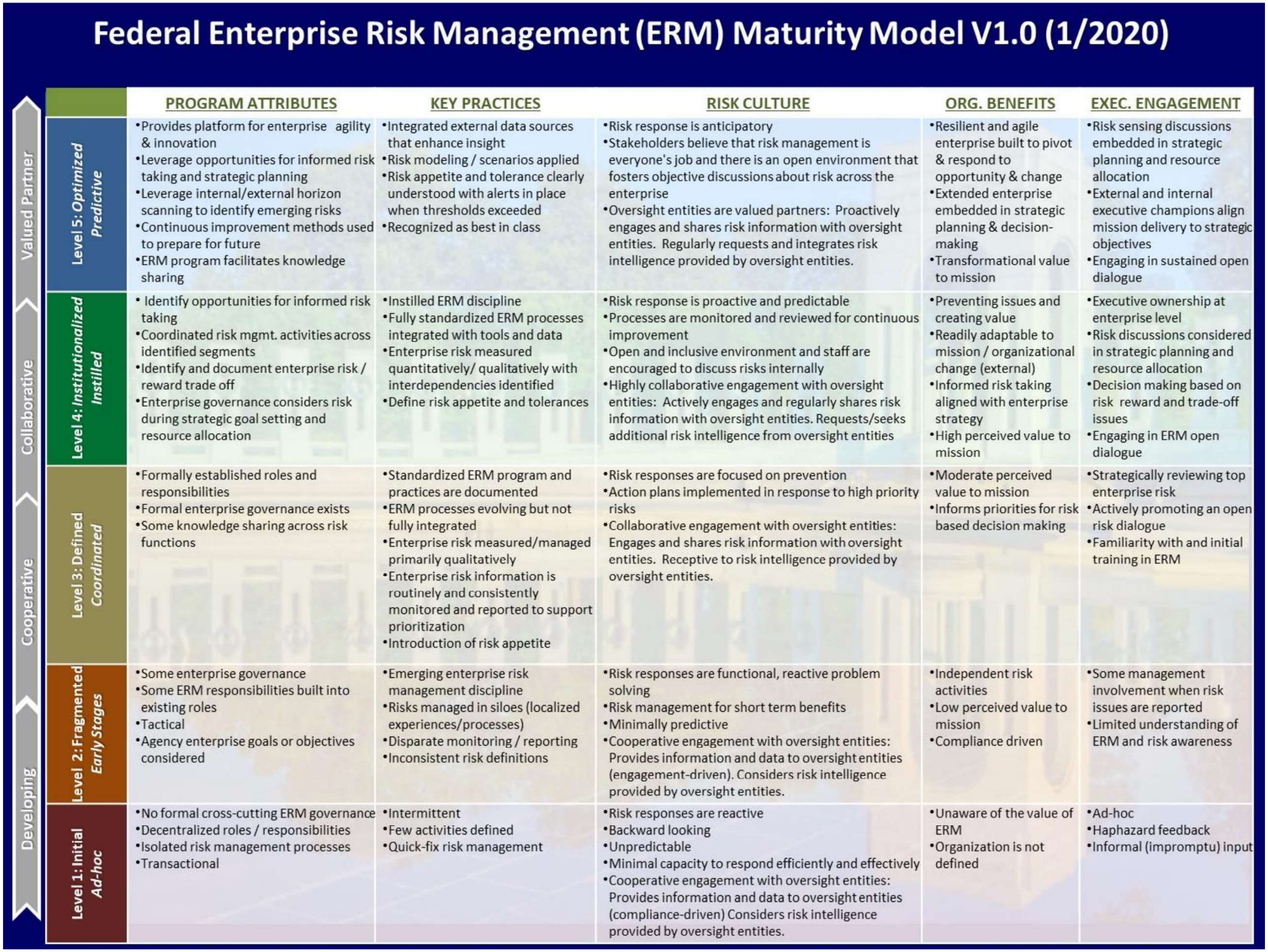

Federal Enterprise Risk Management (ERM) Maturity Model V1.0 (1/2020)

		PROGRAM ATTRIBUTES	KEY PRACTICES	RISK CULTURE	ORG. BENEFITS	EXEC. ENGAGEMENT
Valued Partner	Level 5: *Optimized* *Predictive*	•Provides platform for enterprise agility & innovation •Leverage opportunities for informed risk taking and strategic planning •Leverage internal/external horizon scanning to identify emerging risks •Continuous improvement methods used to prepare for future •ERM program facilitates knowledge sharing	•Integrated external data sources that enhance insight •Risk modeling / scenarios applied •Risk appetite and tolerance clearly understood with alerts in place when thresholds exceeded •Recognized as best in class	•Risk response is anticipatory •Stakeholders believe that risk management is everyone's job and there is an open environment that fosters objective discussions about risk across the enterprise •Oversight entities are valued partners: Proactively engages and shares risk information with oversight entities. Regularly requests and integrates risk intelligence provided by oversight entities.	•Resilient and agile enterprise built to pivot & respond to opportunity & change •Extended enterprise embedded in strategic planning & decision-making •Transformational value to mission	•Risk sensing discussions embedded in strategic planning and resource allocation •External and internal executive champions align mission delivery to strategic objectives •Engaging in sustained open dialogue
Collaborative	Level 4: *Institutionalized* *Instilled*	• Identify opportunities for informed risk taking •Coordinated risk mgmt. activities across identified segments •Identify and document enterprise risk / reward trade off •Enterprise governance considers risk during strategic goal setting and resource allocation	•Instilled ERM discipline •Fully standardized ERM processes integrated with tools and data •Enterprise risk measured quantitatively/ qualitatively with interdependencies identified •Define risk appetite and tolerances	•Risk response is proactive and predictable •Processes are monitored and reviewed for continuous improvement •Open and inclusive environment and staff are encouraged to discuss risks internally •Highly collaborative engagement with oversight entities: Actively engages and regularly shares risk information with oversight entities. Requests/seeks additional risk intelligence from oversight entities	•Preventing issues and creating value •Readily adaptable to mission / organizational change (external) •Informed risk taking aligned with enterprise strategy •High perceived value to mission	•Executive ownership at enterprise level •Risk discussions considered in strategic planning and resource allocation •Decision making based on risk reward and trade-off issues •Engaging in ERM open dialogue
Cooperative	Level 3: Defined *Coordinated*	•Formally established roles and responsibilities •Formal enterprise governance exists •Some knowledge sharing across risk functions	•Standardized ERM program and practices are documented •ERM processes evolving but not fully integrated •Enterprise risk measured/managed primarily qualitatively •Enterprise risk information is routinely and consistently monitored and reported to support prioritization •Introduction of risk appetite	•Risk responses are focused on prevention •Action plans implemented in response to high priority risks •Collaborative engagement with oversight entities: Engages and shares risk information with oversight entities. Receptive to risk intelligence provided by oversight entities.	•Moderate perceived value to mission •Informs priorities for risk based decision making	•Strategically reviewing top enterprise risk •Actively promoting an open risk dialogue •Familiarity with and initial training in ERM
Developing	Level 2: Fragmented *Early Stages*	•Some enterprise governance •Some ERM responsibilities built into existing roles •Tactical •Agency enterprise goals or objectives considered	•Emerging enterprise risk management discipline •Risks managed in siloes (localized experiences/processes) •Disparate monitoring / reporting •Inconsistent risk definitions	•Risk responses are functional, reactive problem solving •Risk management for short term benefits •Minimally predictive •Cooperative engagement with oversight entities: Provides information and data to oversight entities (engagement-driven). Considers risk intelligence provided by oversight entities.	•Independent risk activities •Low perceived value to mission •Compliance driven	•Some management involvement when risk issues are reported •Limited understanding of ERM and risk awareness
	Level 1: Initial *Ad-hoc*	•No formal cross-cutting ERM governance •Decentralized roles / responsibilities •Isolated risk management processes •Transactional	•Intermittent •Few activities defined •Quick-fix risk management	•Risk responses are reactive •Backward looking •Unpredictable •Minimal capacity to respond efficiently and effectively •Cooperative engagement with oversight entities: Provides information and data to oversight entities (compliance-driven) Considers risk intelligence provided by oversight entities.	•Unaware of the value of ERM •Organization is not defined	•Ad-hoc •Haphazard feedback •Informal (impromptu) input