RECIPROCITY®

ENTERPRISE RISK MANAGEMENT AUDIT CHECKLIST

www.reciprocity.com

Enterprise organizations face risk daily. They must determine which risks present an opportunity to grow and which must be mitigated. Enterprise risk management (ERM) focuses on empowering these organizations to minimize loss while maximizing reward. Effective ERM incorporates corporate governance, risk assessment, and internal controls to align stakeholders, managers, employees, and third-party vendors for successful risk management.

But developing and executing an ERM program can be quite the undertaking for an organization. There are several complex steps and evaluations that must be done to ensure that all of the enterprise's bases are covered and that risk management is embedded across the organization.

This ERM Audit Checklist will provide a solid outline to help you establish the scope of your ERM program and take you step-by-step through assessing your risks, implementing training and awareness throughout the organization, assigning responsibility, mitigating risks, and monitoring your risk program.

SCOPE	✓	✗	***If no, Reciprocity's recommendation is to:***
Have you compiled all of your risks (operational, strategic, etc)?	○	○	***Spend more time on operational planning. Contact Reciprocity® for help if needed.***
Have you identified which risk management frameworks your organization is responsible for?	○	○	
Have you received approval of the overall ERM from your governing board?	○	○	
Do you have clear objectives that tie back to your respective risk management frameworks?	○	○	
Do you have business rules or protocols for identifying, communicating, recording, mitigating, and monitoring operational risks?	○	○	
Have you communicated those business rules to your staff?	○	○	

RISK ASSESSMENT	✓	✗	*If no, Reciprocity's recommendation is to:*
Do you have a comprehensive process for identifying risks?	○	○	*Spend more time on risk identification. Reciprocity can help. We also have a variety of resources on risk assessment and management.*
Have you executed your risk assessment?	○	○	
Were the appropriate management, staff, and stakeholders involved in identifying risks?	○	○	
For each risk:			
Have you assessed the severity of each risk depending on its potential impact and probability?	○	○	Assign an appropriate risk score (high, medium, low).
Have you collected enough information about the risk to make decisions? (e.g. source, cause, and potential outcomes)	○	○	Re-define your risk to identify these elements. It's important not to conflate risks. Each must be evaluated separately.
Has the risk category been allocated according to the cause of the risk?	○	○	Assign an appropriate risk category.
Has a risk owner been allocated to the risk?	○	○	*Assign an appropriate risk owner. Assign an appropriate authority to your risk owner.*
Does the risk owner have the appropriate level of authority and knowledge to manage the risk?	○	○	

RISK ANALYSIS	✓	✗	*If no, Reciprocity's recommendation is to:*
Has the risk level been assessed without controls in place?	○	○	Reciprocity can help. We also have a variety of resources on risk assessment and management.
Have you categorized which risks are acceptable and which are not?	○	○	Spend time identifying which risks are acceptable and which are not, and thus need controls to manage.
Were appropriate management, staff, and stakeholders involved in analyzing risks?	○	○	Seek input and advice from appropriate parties.
Have you identified the critical controls necessary to manage unacceptable risks?	○	○	Spend time considering the controls you have in place and whether they are effective. If they're not, you'll need to spend time improving the controls or adding new ones (see below).
Do all of the controls that you've listed already exist?	○	○	Controls that are not already in place need to be created.
Has someone who understands the risks and the controls assessed the effectiveness of the controls?	○	○	Assess the control effectiveness.
Do the controls address the cause of the risk? Are they working as intended?	○	○	Consider introducing additional risk controls.
Have you prioritized the controlled risks so that you know which risks to treat first?	○	○	Prioritize risks.

EDUCATION	✓	✗	*If no, Reciprocity's recommendation is to:*
Do staff understand the risk assessment criteria and acceptable risk levels?	○	○	Spend time training your staff on these topics.
Are staff equipped with the knowledge on lines of defense, skills, and capabilities to effectively manage risks?	○	○	Spend time training your staff on these topics.
Do staff understand their accountabilities, roles, and responsibilities as they relate to risk management?	○	○	Spend time training your staff on these topics.
Has a person in the division been identified to be responsible for supporting risk management?	○	○	Appoint a risk champion.

RISK MITIGATION	✓	✗	*If no, Reciprocity's recommendation is to:*
Have you developed a risk mitigation framework for identified controlled weaknesses including an approval process?	○	○	You will need to design a risk mitigation framework?
Do any uncontrolled risks have mitigation plans?	○	○	You will need to design risk mitigation plans.
Have stakeholders been consulted and involved in developing and evaluating mitigation plans?	○	○	Speak to your stakeholders.
Have you considered different treatment options for modifying the risk to an acceptable level?	○	○	Re-visit your mitigation plans.
Have you evaluated the options, including cost/ benefit analysis and stakeholder implications?	○	○	Re-visit your mitigation plans.
For complex plans: does the mitigation plan contain actions, resources, responsibilities, timing, monitoring, and reporting requirements?	○	○	*Make sure your mitigation plan is comprehensive and resourced.*
For complex plans: have these resources been included in relevant budgets?	○	○	
Has someone with the appropriate authority approved the mitigation plan?	○	○	
Has the treated risk been reassessed for risk level now that controls are in place?	○	○	Reassess the risk.
If the risk is above the department's tolerance, but no further treatment options are available has this been documented and escalated?	○	○	Record acceptance of risk and contingency arrangements. Escalate as required.

MONITORING			*If no, Reciprocity's recommendation is to:*
For each risk:			
Does your monitoring process included obtaining, compiling, and leveraging data from the identified risk areas?	○	○	Contact Reciprocity for help if needed.
Have you worked through the checklist?	○	○	Review the checklist to make sure that your answers still apply.
Has the risk level changed?	○	○	Use this information to inform your re-assessment of control and mitigation plan effectiveness.
Are there any new or emerging risks?	○	○	Analyze, evaluate and, if necessary, treat these as per the steps above.
Are identified risks still relevant?	○	○	Remove any risks that are now obsolete.
Did the risk turn into an incident? How effective were your treatments in addressing the consequences? What can you learn from that?	○	○	Use this information to inform your re-assessment of control and mitigation plan effectiveness.
Are risks being 'over controlled'?	○	○	Reduce or stop any controls that are excessive to eliminate unnecessary complications and waste.
Have lessons learned from the reassessment been identified and used to guide future risk management decisions?	○	○	Record and share lessons.
Is risk monitoring and review integrated with planning, performance management, budgeting, and other management processes?	○	○	Integrate these processes to improve long-term sustainability and growth.
Have your business rules been reviewed in consultation with staff and stakeholders?	○	○	
Are the business rules explicit, cohesive, and accessible?	○	○	

Make sure that you keep your documented business processes and rules up to date and accessible.

ABOUT RECIPROCITY

Reciprocity equips organizations with the fastest, easiest and most prescriptive information security solutions in the market. Our fully integrated and automated ZenGRC platform powers a full catalog of compliance, risk and other infosec applications. Supported by our award-winning customer service and industry-leading GRC expert teams, we help businesses realize the industry's fastest time to value while fostering in-house expertise.

Security builds trust. www.reciprocity.com