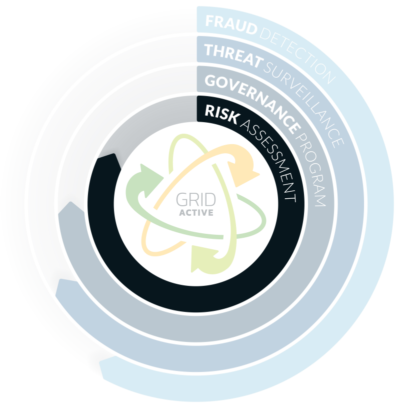
DEFENSESTORM
THE BEST OFFENSE.

GRID Active Risk Assessment

Real-time understanding of your cyber risk profile

Financial institutions have different requirements than other businesses using cybersecurity solutions. As regulated entities, FIs have regulations, guidance, best practices, and examiner expectations they must consider when building out cyber programs. Financial institutions must apply prudent risk management practices to cyber and information security risks and a key element of that is the risk assessment process. Risk assessments help institutions identify new and emerging risks, realize changes in risk levels, and make informed risk-based decisions for budgeting, resource allocation, and strategic planning. Where risk is elevated, mitigating controls must be well designed and effective.

DefenseStorm offers the only built for banking cyber risk management solution with integrated custom risk assessments. GRID Active Risk Assessment enables an FI to maintain and generate continuous risk assessments from the same place overall cyber risk is manage, since annual, check-the-box, risk assessments can open the door to elevated cyber risk if the mitigating controls aren't well designed or effective. Real-time understanding of the risk profiles enables an FI to be more proactive and have better insights that inform impactful action items and break down silos to identify and better manage risk interdependencies across the organization.



RISK ASSESSMENT

FEATURES

- Link risks to the register based on FI's unique audit and policy universe.
- Pre-built risk libraries
- Maintain integrated registers and generate risk assessments from the same platform where cyber risk is managed daily
- Quantitative scoring model

BENEFITS

- Demonstrate the FIs evolution of risk
- Ease of use to build out risk registers
- Proactive and timely insights for better informed decision making for strategic planning, budgets and resource allocation.
- Use aggregated risk score for each risk assessment based on population of risks

DEFENSESTORM
THE BEST OFFENSE.

DefenseStorm Risk Assessment

RISK ASSESSMENT FEATURES AND BENEFITS

- Ability to maintain custom risk, control registers and generate custom risk assessments based on each financial institution's unique risks and programs.
- Leverage prebuilt libraries of risks and controls to build out their registers. Library risks and controls are pre-mapped to each other (and the frameworks and self-assessments built into GRID Active Governance Program) making it even easier to prove adherence to industry and regulatory control frameworks.
- Risks and controls in the register can be linked to the institution's unique audit and policy universe to illustrate the full picture of the overall risk management program.
- Systematic evidence collection against controls in the register help support control effectiveness scores with security operations and governance activities happening daily within the GRID Active platform.
    - With supported and evidenced control scores, residual risk scores are more accurate and reliable.
- Risk assessments can be filtered based on the institution's unique needs to create multiple smaller risk assessments or one large Information Security Risk Assessment encompassing all risks in the register.
    - Demonstrate a clear picture of how risks and control systems have evolved over the course of your cybersecurity program
- An aggregate risk score is recommended for each risk assessment based on the population of risks within it using a quantitative scoring model.
    - Institutions may instead choose to select their own aggregate risk scores giving them the needed control over their risk management program.
    - Risk assessments are memorialized to provide a clear picture of how the risk profile has evolved over time.
- Maintain individual risk profiles for all systems and applications in use at the institution. Systems and applications are assessed based on the criticality of data they process or store and its impact to business operations.
    - Institutions can link inventory items to risks and controls in the registers to achieve a complete picture of cyber and information security risks and controls.