GRA's Security Assurance Services assist organizations to identify and review their information security to verify that the PHI and other sensitive information is adequately protected.

Our offering includes:

- Threat and Risk Assessments (TRA) is a formal risk management tool designed to identify potential administrative, technical and physical weaknesses in your Information Systems' infrastructure as well as recommended changes or additional safeguards that reduce identified risks to an acceptable level.

- Privacy Impact Assessments (PIA) is another formal risk management tool used to identify the actual or potential effects that a proposed, or existing, information system, technology or program may have on individuals' privacy. Our privacy consultants use a methodology based on the Privacy Impact Assessment Guidelines published by the Federal Treasury Board of Canada, adapted to conform with the requirements of the Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act published by the Information and Privacy Commissioner for Ontario.

- Our Privacy and Security Architecture (PSA) development service identifies and documents existing or planned controls (people, process, technology, facility) that are required to safeguard the confidentiality, integrity and availability of sensitive assets such as PHI. A services-oriented architecture is employed to document the various safeguards that address the required and recommended controls.

- Our vulnerability and penetration testing service provides the ultimate assurance that the privacy and security program leverages sound technical and administrative security safeguards. Our offering is customized to the organization's goals and requirements and our consulting team and associates are qualified to review and identify vulnerabilities associated with the configuration of Windows or UNIX hosts, databases, applications and network components. In many cases, our consulting team is engaged to perform vulnerability testing, as well as the optional penetration of identified vulnerabilities. GRA also offers application code review to identify exploitable software coding weaknesses.

GRA's business continuance planning service identifies the realistic risks and threats that may limit the survivability of your organization's infrastructure and assists you in developing an effectiveness plan to minimize the negative impact and resumption timelines of key services. GRA's business continuance consulting services include our Survivability Assessment and Disaster Recovery Planning services.

Achieving Survivability:

- Resistance to Events
- Recognition of Events
- Recovery from Events
- Adaptation or Learning

Resistance/Protection

Recognition/Detection

Recovery

Adapt
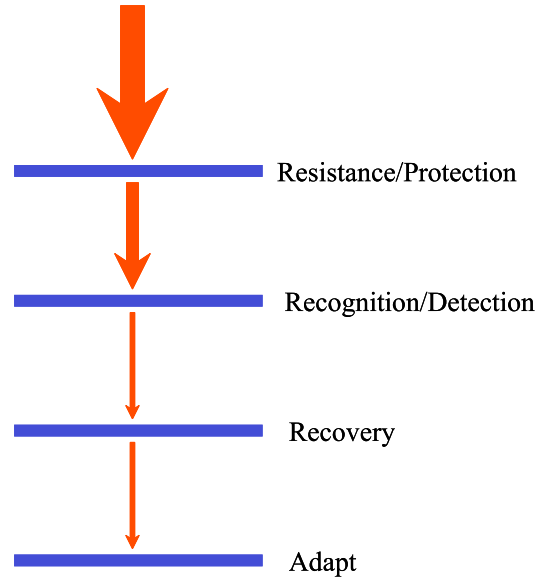
The GRA team will work with you to develop a recovery plan tailored to your facility. Our DR Planning services walks you through the process of building a plan to address realistic exposures and utilize resources at hand.

Phil Kretzmar at SCO Health Services said:

> *"GRA was the catalyst that caused us to start thinking about what is likely to happen and what we need to do. There were many issues that surfaced that we would have easily missed."*

Our GRA Survivability Assessment (GSA) is fast becoming a de facto standard for hospitals to evaluate their recovery readiness and choices. Your customized report will include a list of recovery options, pricing, recovery times and data loss exposure, as well as internal risks associated with each option.