# Case Study #2: Technology & Product Review for Identity Governance & Administration

## Case Scenario:

For this case study, our focus shifts to technologies and products used to implement the Identity Governance & Administration (IGA) business process and related security controls.

IGA is used to manage and mitigate insider threat. Insiders, because of their access to information and information resources (e.g. workstations, servers, networks), potentially have the opportunity and the means by which to steal intellectual property, commit fraud, and perform other types of mischief and mayhem (ranging from pranks to deliberate sabotage).

For our focus firm, Sifers-Grayson, access control and identity management have not been a serious concern ... or so their executives and managers thought. The majority of employees and managers are from the local area where there is a strong sense of community. The founders of the company belong to families who were among the original settlers for the county. They contribute heavily to local charities and youth organizations. They rely upon these connections to family and community when hiring and have a strong tradition of promoting from within.

The problem is that Sifers-Grayson's operations and sales have taken them into the vast geographies of the Internet and cyberspace. There is an emerging awareness among the engineering staff of the potential for outsiders to attack the company through its Internet connections. The thought that an insider might cause trouble for the firm is still hard for them to accept.

The company can no longer afford to depend upon social mores (pronounced “more-rays”) and norms to protect it against the possibility of insider threats. The new contracts specifically require proper labeling of information ("data classification") and require control over access to government furnished information ("GFI"). This means that the company needs to change its culture and change its management processes.

The primary means for protecting against insider threats is to control insider access to information, information systems, and the information infrastructure. The two most basic processes used to protect against insider threat are (a) identity management and (b) access controls. Data classification is also an important protective process since it enables the use of the value or sensitivity of information when determining how and when to grant access. Privilege management is a third protective process, which is used to protect against the misuse of permissive access to software applications and operating system functions. The principle of *least privilege* is an important control over this permissive access. Finally, *separation of duties* is a key business process, which is used to prevent insiders from abusing access to information and information resources.

## Research:

1. Review the weekly readings.
2. Choose an Identity Governance & Administration product which was mentioned in the readings. Research your chosen product using the vendor’s website and product information brochures.
3. Find three or more additional sources which provide reviews for (a) your chosen product or (b) general information about the characteristics of Identity Governance & Administration Products.

## Write:

Write a 3 page summary of your research. At a minimum, your summary must include the following:

1. An introduction or overview for the security technology category (Identity Governance & Administration).
2. A review of the features, capabilities, and deficiencies for your selected vendor and product.
3. Discussion of how the selected product could be used by your client to support its cybersecurity objectives by reducing risk, increasing resistance to threats/attacks, decreasing vulnerabilities, etc.
4. A closing section in which you restate your recommendation for a product (include the three most important benefits).

As you write your review, make sure that you address security issues using standard cybersecurity terminology (e.g. protection, detection, prevention, “governance,” confidentiality, integrity, availability, nonrepudiation, assurance, etc.). See the ISACA glossary <https://www.isaca.org/pages/glossary.aspx> if you need a refresher on acceptable terms and definitions.

## Submit For Grading

Submit your case study in MS Word format (.docx or .doc file) using the *Case Study #2:IGA Technology & Product Review* assignment in your assignment folder. (Attach the file.)

## Additional Information

1. There is no penalty for writing more than 3 pages but, clarity and conciseness are valued. If your case study paper is shorter than 3 pages, you may not have sufficient content to meet the assignment requirements (see the rubric).
2. Your paper should use standard terms and definitions for cybersecurity. See Course Content > Week 1 > Cybersecurity Concepts Review for recommended resources.
3. You must include a cover page with the assignment title, your name, and the due date. Your reference list must be on a separate page at the end of your file. These pages do not count towards the assignment’s page count.
4. You are expected to write grammatically correct English in every assignment that you submit for grading. Do not turn in any work without (a) using spell check, (b) using grammar check, (c) verifying that your punctuation is correct and (d) reviewing your work for correct word usage and correctly structured sentences and paragraphs.
5. You are expected to credit your sources using in-text citations and reference list entries. Both your citations and your reference list entries must follow a consistent citation style (APA, MLA, etc.).
6. Consult the grading rubric for specific content and formatting requirements for this assignment.