# **Title of Project**

[Team name]: [List team members' names here in alphabetic order.]

University of Maryland Global Campus

CBR 600 *[section number]*

*[Professor's name]*

[Date project is due]

## **Executive Summary**

This should be a single, double-spaced page that highlights the key points covered in the sections that follow. It should be written after the rest of the technical report.

## **Title of Project**

This introductory section should provide basic information about the breach, what was compromised or damaged, and what the project will cover to arrive at your conclusion about this situation. It should consist of two or three focused paragraphs.

### **Organizational Profile for [Organization]**

This should include:

* a short introduction (about three sentences),
* a description and diagram of the organization and its critical missions, and
* information security needs to protect those critical missions.

### **Analysis of Threats to the Organization's Information Systems**

This section includes:

* a short introduction (about three sentences),
* a description of potential threats and vulnerabilities, and
* risks to the CIA triad.

### **Proposed Mitigation Strategy**

This section includes:

* a short introduction (about three sentences);
* your proposed identity management system;
* managing roles, accesses, restrictions, and conditions; and
* unknown risks and costs.

**Conclusion**

Your conclusion should summarize the key points you have made in the previous sections and why you think that your mitigation strategy will work (or where you have doubts), as well as where the challenges and unknowns remain. You can provide recommendations for further study or analysis, but avoid introducing any completely new ideas in this section.

## **References**

These should be in error-free APA format and listed in alphabetical order.