Mergers, Acquisitions and Information Security Aspects

ISM6100: Security Implementation Team Project

Authors: Andre Shori, ashori<at>mastersprogram.sans.edu
Ed Yuwono, ed.yuwono.msism<at>gmail.com

Advisor: Stephen Northcutt
Accepted: 3 March 2017

1. Executive summary

GIAC Fortune Cookie Company is in an early stage of a Merger and Acquisition of Ya Mon Fortunes, where we know little about the target company, and our team has been asked to provide a preliminary plan for the safe integration of Ya Mon Fortunes into GIAC Fortune Cookie operations.

The following report outlines a systematic and logical plan that will result in the safe integration of Ya Mon's existing processes, with minimal disruption to current and future business processes and in the shortest timeframe. We recommend utilizing the step by step phased approach in this report and categorizing business processes by their criticality and potential impact for better resource allocation to achieve a safe integration. Once the GIAC Acquisition Steering Committee approves this plan, efforts can begin immediately to gather information on Ya Mon's current structure and operations and begin detailed integration planning including appropriate cyber security measures.

2. Background

GIAC Fortune Cookie Company (GIAC), is in the process of merging and acquiring (M&A) Ya Mon Fortunes (Ya Mon). Our CIO asked our project team to develop a preliminary plan for the safe integration of Ya Mon's security architecture, operations and processes into GIAC as part of the broader business integration efforts. This plan and its recommendations are part of the overall integration plans of GIAC, which is owned and approved by the GIAC Acquisition Steering Committee (M&A Steering Committee)[1].

3. Initial Analysis

GIAC advocates to high standards in our operations and wherever possible, strive to obtain industry certification to that effect. GIAC also has wide-ranging corporate security

[1] It is also recommended that a member of GIAC's Cyber Security team be included on the M&A Steering Committee.

policies[2] and strong internal controls for business processes. GIAC's Cyber Security Team has adopted the ISO27001 standard as part of our security model.

In contrast, details of Ya Mon's geopolitical situation, physical environment, operations, maturity, threat landscape or technologies they currently utilize are unknown. This lack of knowledge presents a significant risk to the integration efforts. As a result, before being granted regulatory approval, GIAC is unlikely to be able to access detailed information or initiate any change to Ya Mon's environment.

4. Approach

The Cyber Security Team aims to support the business with their integration of Ya Mon while maintaining a high level of security. The following method provides an indication of Ya Mon's level of security maturity through evidence-based discovery and provides a high degree of safety for the M&A integration. Ya Mon's level of defense maturity also provides useful information when determining the correct valuation of Ya Mon.

5. Business Process Categorisation

Business Process Categorization provides information on where to focus integration efforts and forms the basis of security related decision making. Given the limited time and resources available for integration, prioritization is employed to ensure that business operations are integrated while minimizing disruption to profit generating business units. Categorization also provides the security team with an indication on resources allocation.

We propose that the following three primary categories for all business processes impacted by the integration:

1. **Business Critical** – These include GIAC core business processes where should an event compromise these processes; there is a high risk of GIAC no longer being able to function.

[2] GIAC Security Policies include Acceptable Use, Encryption, Passwords, Email Use, BCP/DRP, Security Response, Network Security and Server Security policy.

2. **Business Important** – These are non-critical but still significant business processes needed for day to day operations. Breaches of these systems would result in financial loss or cause disruption to operations but would still allow the company to operate.
3. **Business Strategic** – Business Strategic processes are those that do not necessarily fit into the above two categories or may be defined by the M&A Steering Committee as longer term integration targets.

Appendix B contains additional information and details of Business Process Categorization.

6. Phases

In conjunction with Business Process Categorization, our team recommends the following phased approach to the integration process. The segments comprise Reconnaissance, Pre-Planning, Audit, Final Planning, Integration, Validation, and Signoff. Stages follow a linear path, with one segment ending before the next begins. Each step serves to build on the previous stage and helps ensure completion of the integration in a secure manner.

Reconnaissance Phase	-> Pre Planning Phase	-> Audit Phase	-> Final Planning Phase	- > Integration Phase	- > Validation Phase	- > Signoff Phase

Figure 1: Phases presented in sequence

Appendix A contains additional information including timing and duration.

6.1 Reconnaissance Phase

Reconnaissance (Recon) provides GIAC with essential information relating to Ya Mon's environment. Our team recommends that an immediate recon of Ya Mon's end to end business processes and supporting infrastructure. We firmly recommend that requests for information be sent to Ya Mon immediately to capture key knowledge items[3]. Also, a team comprising appropriate members of GIAC's key verticals such as operations, legal, HR, Finance, IT (including a suitable member of the Cyber Security Team) should be dispatched onsite to gain

[3] Business processes and supporting technologies such as their current policies, past audit results, internal and external technologies, current security processes, user documentation, current policies, assets, design items like network and infrastructure and future strategic plans.

first-hand knowledge and insight into YaMon. We also recommend engaging an M&A consulting company with cyber security experience to act as advisors during the integration and engage them or a company specializing in business intelligence to conduct parallel research into Ya Mon. Ya Mon's "information snapshot" will include this research.

6.2 Pre-Planning Phase

Pre-Planning leverages the lead time pre-M&A approval to develop a preliminary implementation plan based on knowledge gathered during the Reconnaissance Phase. Planning utilizes information compiled from recon. Pre-Planning will complete once ownership of Ya Mon transfers to GIAC in six months' time. Conducting differential analysis will provide a better understanding of Ya Mon's business processes and interdependencies. Normalization of functions will determine similar capabilities and identify duplicate services. Business processes approved by the M&A Steering Committee for integration can then be classified based on Business Process Categories. Business Critical processes are aimed for operation before the organization's go live date (Day 0). Business Important processes are scheduled to complete near Day 0. Integration of Business Strategic processes will commence upon meeting necessary prerequisites. Go-live date (Day 0), and cost estimates will become available upon completion of the Pre-Planning phase.

Appendix C contains details of proposed security metrics by our team included in the Pre-Planning, Final Planning, Implementation and Validation Phases.

6.3 Audit Phase

The Audit Phase reconciles and validates information gathered and compiled during the earlier stages and provide confirmation to proceed with final planning. The Audit is scheduled to begin immediately once ownership of Ya Mon's assets transfers to GIAC. The Audit is estimated to take two months.

6.4 Final Planning Phase

The Final Planning Phase is final validation of earlier integration assumptions and plans against our new pool of information and allows for any last minute changes. Barring unforeseen

complications, Final Planning will take one month. The M&A Steering Committee will then approve finalized plans.

6.5 Implementation Phase

The Implementation Phase involves the actual execution of the approved integration plan.

6.6 Validation Phase

The Validation Phase ensures that integration is complete, according to business and security requirements. Business owners of systems will be required to perform appropriate analysis such as User Acceptance or Regression testing before final Signoff.

6.7 Signoff Phase

The Signoff Phase marks the end of each respective business processes integration as defined by the M&A Steering Committee and transfers the new shared systems to their respective owners. Business Critical and Business Important integration will be completed by Day 0, and Business Strategic integration will follow their timeline (long term integration).

7. Conclusion

As the integration progresses and information gathered about Ya Mon, the close examination and classification of its current business processes will allow us to validate their current environment and operations from a variety of perspectives including security. The sooner we begin the process of information gathering, the sooner we can start building an accurate picture of the current health of the target company. Classification of all the business processes included in the integration allows appropriate levels of resourcing and attention throughout the remainder of the merger of the two companies. By utilizing a planned, phased approach to the integration we establish a systematic process to follow that facilitates a smoother integration and the safe and secure creation of shared business processes and their supporting technologies.

Appendix A - Phases

In conjunction with Business Process Categorization, our team recommends a step-by-step approach be undertaken during the integration process to facilitate the safe and secure incorporation of Ya Mon's processes. These stages provide a methodology and insight into the overall progress of the integration and form the basis of performance measurement (Gates & Very, 2003, p. xx)[4] during the integration.

Each phase serves to build on the previous stage by enriching the information GIAC has gathered on Ya Mon. Implementing each step in a secure manner helps to ensure a complete integration. The steps comprise of Reconnaissance, Pre-Planning, Audit, Final Planning, Integration, Validation, and Signoff. Steps follow a linear path, with one period ending before the next begins. These steps are specially customized for Ya Mon's integration and are capable of encompassing a variety of business process modeling best practices that the M&A Steering Committee may ultimately select.

Reconnaissance Phase

Reconnaissance (Recon) provides GIAC with essential information relating to Ya Mon's environment. Gaining insight into Ya Mon's current structure is a necessary first step for our integration work as currently, little is known. Creating an "information snapshot" of Ya Mon's current business processes, structure, and security posture will help conduct a differential analysis between Ya Mon and GIAC, a necessary step during the next phase of our integration. Recon will also contribute to identifying key personnel and aid in mitigating any future risk of lost knowledge due to attrition or redundancy as a result of integration efforts. GIAC will have an opportunity to shorten the integration timeline by providing sufficient information to start integration planning. Recon is estimated to take two weeks to complete.

Our team recommends an urgent recon of Ya Mon's end to end business processes and supporting infrastructure (including cyber security controls, technologies, and related process). We firmly recommend that requests for information be sent to Ya Mon immediately to capture

[4] Gates, S., & Very, P. (2003). Measuring Performance During M&A Integration. *Long Range Planning*, *36*(2), 167-185. doi:10.1016/s0024-6301(03)00004-9

key knowledge items[5] with the aim of maximizing the available time for Pre-Planning. We advocate that a team comprising appropriate members of GIAC's key verticals such as Operations, Legal, HR, Finance, IT (including a suitable member of the Cyber Security Team) should be dispatched onsite for one week to gain firsthand knowledge and insight into Ya Mon. Ya Mon's current operations, systems, business controls, processes and related supporting technologies (and cyber security related items such as policies, processes, incident handling capabilities, past incident reports and so on) require examination. Estimated cost for the dispatch of one of our security engineer onsite for one week is USD9576.13 (Figure 2).

Estimated Travel Cost			
Arrives Monday 6 March 2017, leaves Friday 10 March 2017			
Flight[6]	business round trip	USD	$ 1,473.00
Hotel[7]	4 nights	USD	$ 2,288.00
Expenses[8]	100/day	USD	$ 500.00
Kidnap Insurance[9]		USD	$ 2,000.00
Travel Insurance[10]	$66.34 + 250 deductible	USD	$ 266.34
	subtotal	USD	$ 6,527.34
Labour Per hour		USD	$ 76.22
Man hours	40 hours	USD	$ 3,048.79
	Total estimate	USD	**$ 9,576.13**

Figure 2 Estimated Travel Cost for Security Engineer for one week to Montego Bay, Jamaica

We also recommend engaging our M&A advisors or a company specializing in business intelligence to conduct parallel research into Ya Mon and included in the "information

[5] Business processes and supporting technologies such as their current policies, past audit results, internal and external technologies, current security processes, user documentation, current policies, assets, design items like network and infrastructure and future strategic plans.

[6] Cheap flights from San Francisco International to Montego Bay at Skyscanner. (2017, March 1). Retrieved from https://www.skyscanner.com/transport/flights/sfo/mbj/170306/170310/airfares-from-san-francisco-international-to-montego-bay-in-march-2017.html?adult=1&child=0&infant=0&cabinclass=Business&rtn=1&lang=en#results

[7] Booking.com: 1,154,985 hotels worldwide. 114+ million hotel reviews. (2017, March 1). Retrieved from https://www.booking.com/

[8] Jamaica DoD Per Diem Rates for 2017. (2017). Retrieved from https://www.perdiem101.com/oconus/2016/jamaica

[9] A Guide To Kidnap & Ransom Insurance Coverage | Investopedia. (2015, July 29). Retrieved from http://www.investopedia.com/articles/personal-finance/062915/guide-kidnap-ransom-insurance-coverage.asp

[10] Visitors medical Insurance, Visitors Medical Insurance plans, USA Visitors Medical Insurance. (2017, March 1). Retrieved from https://www.americanvisitorinsurance.com/insurance/visitors-medical-summary.asp

snapshot." A business intelligence consultants estimated cost is USD25 per hour[11] and the M&A advisory for the duration of the integration process is approximately USD500 per day[12].

Pre-Planning Phase

Pre-Planning leverages the lead time pre-M&A approval to develop a preliminary implementation plan based on knowledge gathered during Recon. Analysis of the information gained from recon, even partial information, provides several advantages. Planning for the integration can begin sooner, utilizing the expected six-month period required for the M&A approval process. Business units can work with security teams to assess and plan the effort required to maintain business continuity.

A differential analysis provides a better understanding of Ya Mon's business processes and interdependencies. Normalization of functions will help to determine similar capabilities providing alignment that can be used to establish unnecessary services. A shared standard is then decided and will include which processes such as policies, processes, standards and technologies the combined companies will adopt (or keep).

One of the three primary Business Categories is used to classify all business processes for integration, as approved by the M&A Steering Committee. The security team will work with the business during the end to end integration planning, by recommending appropriate security controls based on the shared standard. Prioritization for the integration will be provided based on the Business Categories. The integration planning team will undertake business impact studies to minimize the impact on the organization during the migration. The team will explore various options aiming for the least disruption. Options include business continuity plans and rollback options to ensure continuous operations during integration. Other examples of options include re-education of staff to ensure business processes and upholding of policies.

For example, one method of minimizing impact may be a parallel run, where the existing process is used concurrently with the new one until switched over and eventually phased out. At

[11] Top 10 Osint Freelancers For Hire In March 2017 - Upwork. (2017, March 1). Retrieved from https://www.upwork.com/o/profiles/browse/?q=osint

[12] What are typical due diligence costs that a consulting firm charges for private equity due diligence? - Quora. (2014, October 21). Retrieved from https://www.quora.com/What-are-typical-due-diligence-costs-that-a-consulting-firm-charges-for-private-equity-due-diligence

the other end of the spectrum is a full cutover (changing immediately over to the new shared system) or any of a variety of approaches in between.

Acceptance criteria for later phases will also be established to achieve final integration Signoff from the business. For example, if the decision is to utilize a shared web application for fortune cookie submission (as currently employed by GIAC's North America operations) then proper security measurements such as web penetration testing will be proposed as validation criteria. Business Strategic category items may not require the same level of attention during the actual integration and included at a later date.

Cybersecurity controls must be part of the Pre-Planning phase and appropriate specific security recommendations made to ensure adherence to proposed shared policies, standards, and processes. A quantified risk assessment on new systems across major cyber security domains is needed. Business process owners and the M&A Steering Committee must review the risk evaluation and mitigation recommendations. Should it be apparent that GIAC's security standard is the more mature, then that should be selected as the uniform standard across both sites. Analysis of Ya Mon's security posture by GIAC's Security team will assist in benchmarking Ya Mon's current level of security maturity. Past breaches and current active attacks disrupting operations may require major remedial work and could provide more information for Ya Mon's valuation (or devaluation). Estimated cost for allocating two security engineers @ 30% utilization for Pre-Planning is USD7317.12.

Audit Phase

The Audit Phase reconciles and validates information compiled during the earlier stages and provides confirmation for final planning. Upon M&A legal approval and transfer of ownership, we recommend that an immediate audit of Ya Mon be conducted to confirm all proposed integration plans. This review will also allow for end-to-end gap and threat identification, deeper analysis and assumption checking for later phases. The M&A Steering Committee, in turn, must be notified on any significant discrepancies. A long term benefit of the Audit Phase is that it will also aid in creating a long-term roadmap for bringing Ya Mon's operations to current GIAC standards (integration will be focused primarily on business

operations, not adherence to standards). An audit is estimated to take two months to complete and cost roughly 0.39 per USD1000 in revenue[13].

Final Planning Phase

The Final Planning Phase is the final validation of our integration assumptions and plans against our new pool of information and allows for any last minute changes. The Final Planning Phase will modify the integration plan with any variations identified in the Audit Phase. The Final Planning Phase will also include any other potential future change (such as pending loss of key staff). As ISO27001 serves as the security metric for integration, it is important that the integration plan has some evidence of alignment to ISO27001. Exceptions are then noted and approved by the appropriate stakeholder before commencing the Implementation Phase. In doing so, the evidence recorded could be incorporated into later long-term integration efforts or as evidence during ISO recertification. Final Planning duration is variable as all changes are subject to approval from the M&A Steering Committee.

Implementation Phase

The Implementation Phase involves the actual execution of the approved integration plan. Business Critical processes are likely to be aimed for operation before the organizations go live date (Day 0) and prioritized. Business Important processes are implementation methods feasibly scheduled to complete near Day 0. Business Strategic process integration would commence once necessary prerequisites are complete.

Integration will invoke mass changes and may introduce vulnerabilities into the organization. These vulnerabilities may be exploited by opportunists and may result in an adverse financial or operational impact. Vigilance is provided through security monitoring to ensure any vulnerabilities are detected. Vigilance also helps establish incident handling procedures and ensure minimal impact.

Deviations from the integration plan will require review by the integration team. Security metrics are to be used to align any proposed variations.

[13] Metric of the Month: Internal Audit Costs. (2015, November 3). Retrieved from http://ww2.cfo.com/auditing/2015/11/metric-month-internal-audit-costs/

Appendix C contains details of proposed security parameters by our team included in the Pre-Planning, Final Planning, Implementation and Validation Phases. Implementation Phase duration and costs are variable and dependent on earlier phases.

Validation Phase

The Validation Phase confirms that the integration is completed and done according to business and security requirements. Business owners of systems will be required to perform appropriate analysis such as User Acceptance or Regression testing before final Signoff.

From a security perspective, validation must provide sufficient detail needed for ISO27001 re-certification. Validation will also ensure that documentation reflects the implemented changes and provide evidence for future audits. As planned and agreed previously, appropriate security testing will take place in line with the security metrics. Testing may include validation of security controls, process audits or penetration testing on shared applications and services. The duration of this stage is dependent on the nature and type of validation testing approved by the M&A Steering Committee.

Signoff Phase

The Signoff Phase marks the end of each respective business processes integration as defined by the M&A Steering Committee and transfers the new shared systems to their respective owners. The security team will commence regular operational monitoring and adhere to standard incident response procedures for the service. After obtaining signoffs from all processes, the integration is considered complete.

Appendix B - Business Process Categorisation

Our team created custom Business Process Categorization specifically for the integration as we realized that current and traditional business process mapping would take too much time to complete. It is very likely for GIAC to want to finish the integration in the shortest period and return to full operations.

Utilizing a tailored Business Process Categorization provides the M&A team with information on where to focus integration efforts and forms the basis of the integration decision making process. Given the limited time and resources available for integration, prioritization is employed to ensure that business operations are integrated in a manner minimizing disruption to profit generating business units. Our M&A expert (J. Lam, personal communication, Feb 19, 2017) vetted these categories and deemed them viable for this project.

These categories are flexible, and business processes added or removed as the integration develops. They are also adaptable, capable of being tailored to changes in the integration timeline while maintaining an appropriate focus on the criticality and importance of those business processes. Categorization will also provide the team with an indication on where to allocate security resources during integration.

We propose that three Primary Business Process Categories be used to group all the business processes defined by the M&A steering committee (as part of the acquisition process or indirectly impacted). These groups comprise the following:

1. **Business Critical** – These include GIAC core business processes where should an event compromise these processes; there is a high risk of GIAC no longer being able to function. For example, an event that would have an adverse impact on GIAC's ability to buy and sell fortune cookie sayings. Business Critical processes will require the most focus and planning during the integration and are the first processes to be integrated before the go live (Day 0) date. These methods and systems require the highest levels of security given their criticality and sensitivity.
2. **Business Important** – These are non-critical but still significant business processes needed for day to day operations. Breaches of these systems would result in financial loss or cause disruption to operations but would still allow the company to operate. Examples

of Business Important systems might be Human Resource or Procurement. Business Important processes are those that will be integrated on Day 0 or shortly afterward and will require high levels of security, but not as high as Business Critical processes.

3. **Business Strategic** – Business Strategic processes are those that do not necessarily fit into the above two categories or may be defined by the M&A Steering Committee as longer term integration targets such as the amalgamation of software licensing and finalizing the minimisation of duplicative capabilities.

Appendix C – Security Metrics

Measuring security between two organizations is a challenge. Differences between the organization's culture, technology, processes and people present too many variables for a universal standard. However, company acquisitions and mergers necessitate the requirement for measuring the maturity of information security practices to reduce the risk of acquiring a bad investment. Organizations are required to demonstrate sound information security practices, similar to having to demonstrate sound financial practices.

Poor information security governance presents a significant transfer of liability to the purchaser during an M&A. The purchaser could inherit unrealized liabilities including and not limited to, outstanding legal obligations (file sharing within the organization resulting in DMCA requests), capital outlay for urgent infrastructure work (outdated/non-existent security infrastructure), required remediation work (undetected malware outbreak) or breach remediation (investigation and compensation costs)[14]. As seen with the Yahoo and Verizon acquisition, a violation could result in a devaluation of the organization[15].

As an M&A demands a fast-paced approach to merge two companies together, security vulnerabilities increase the exposure to risk for the purchaser. Due diligence is required to minimize risks to the buyer as early as possible during the M&A process.

This section provides insight into how GIAC Enterprises developed their security metric for the M&A of Ya Mon. Note that this would only uncover certain information security deficiencies and when used alone, would not be sufficient to determine Ya Mon's information security maturity. Other instruments such as and is not limited to, contractual clauses (e.g. limitation of liability, compensation for non-disclosure), staff interviews or the release of other system audit results (e.g. SOX or PCI-DSS) provides more due diligence.

[14] Yahoo Verizon: Titanic Data Breach Highlights Risk to M&A | Fortune.com. (2016, September 23). Retrieved from http://fortune.com/2016/09/23/yahoo-verizon-data-breach-ma/
[15] Verizon Demands New Deal Terms After Yahoo's Latest Hack | Fortune.com. (2016, December 16). Retrieved from http://fortune.com/2016/12/16/yahoo-hack-verizon-deal/

Establishing a Common Baseline

The GIAC Cyber Security Team needs to conduct due diligence to reduce the likelihood that their acquisition of Ya Mon did not result in the same way as Yahoo/Verizon.

As a start, they should adopt ISO 27001 as their security model allowing them to ensure that they follow industry best practices. They also decided to utilize this as the baseline and metric for Ya Mon's acquisition.

A common baseline is required to ensure that both organizations align to a security framework, and improvements can be measured (security metric). ISO27001 should be the comparison metric because:

- GIAC has adopted ISO27001 as their Cyber Security Management standard.
- It is a globally recognized standard for Information Security Management.
- It is an executive mandated initiative which indicates the organization's commitment to information security within the organization and is an indicator to determine Ya Mon's commitment to Information Security. The Executive Mandate is a mandatory requirement defined by the 27001 standards (Section 4.3).
- The standard is issued only after a successful independent audit. However, not all organizations seek to achieve full certification but adopt ISO27001 as part of security best practice.
- Its risk-based approach provides flexibility for organizations with varying security requirements. GIAC and Ya Mon could leverage this method to agree to a mutually acceptable security requirement.
- Third-party auditors are available globally to provide evidence for certification.
- Provides a level of assurance for external parties that the organization is practicing a level of due diligence on Cyber Security.
- Allows a common framework between two organizations (note this does not ensure the same degree of security as many factors such as certification scope will be different)

Conversely, there are negatives with ISO27001:

- The organization defines the scope of the certification. The organization may be ISO27001 compliant but not have all their systems within the scope. In an M&A, systems out of scope may require further examination.
- The standard is not prescriptive. While this provides flexibility with implementing solutions, results are individual and acceptable results disputable between both companies.

In the best case, Ya Mon has achieved full certification, allowing GIAC's security team to determine the scope of the certification, certificate validity dates and the Statement of Applicability (SoA)[16]. A request for information issued during the Reconnaissance Phase and a full Audit would provide GIAC's security team with an indication of their current security maturity level. ISO 27001 is also a good benchmark to use if Ya Mon has not reached full certification.

Security Metrics

The Security Metrics for the M&A will allow GIAC security staff to determine Ya Mon's level of security maturity.

For the M&A, the metrics aim to achieve the following goals:

- Establish Ya Mon's current level of security maturity.
- Identify deficiencies in Ya Mon's security.
- Determine the immediate remediation work required to bring Ya Mon on to the same degree of security maturity as GIAC.

As the time available to remediate before integration is limited, GIAC's M&A steering committee will prioritize work based on the Business categories. The security team will:

- Assess the request;
- Examine the application against ISO27001 domains;

[16] How can you validate a vendor that claims to have ISO 27001? – IT Governance Blog. (2016, September 19). Retrieved from https://www.itgovernance.co.uk/blog/how-can-you-validate-an-iso-27001-vendor/

- Determine if there is any extra security work required to comply with the domains;
- Prioritize the work: must the security work be completed urgently or can it be deferred to a later period as a strategic task or incorporated as an operational function;
- Provide the M&A Steering Committee with recommendations on how to proceed with the migration including the ISO domains and preliminary Red, Amber, Green status (RAG status).

As with all project based tasks, the M&A Steering Committee will be immediately informed of any issues regarding the scheduling or prioritization of tasks to allow time for the security team to assess and allocate the appropriate resources.

Applying the metric on a WBS level grants more accuracy. In the example below, each M&A business unit stream would consist of several subprojects containing WBS items. The security team would assess each WBS item against the ISO27001 standard for adequacy (Figure 3).

Task Name	Duration	Start	Finish	27001 Mapping	27001 Actions	27001 RAG
M&A Integration	**1 day?**	**Fri 24/02/17**	**Fri 24/02/17**			
Finance	**1 day?**	**Fri 24/02/17**	**Fri 24/02/17**			
Reconnaisance	**1 day?**	**Fri 24/02/17**	**Fri 24/02/17**			
Pre Planning	**1 day?**	**Fri 24/02/17**	**Fri 24/02/17**			
Audit	**1 day?**	**Fri 24/02/17**	**Fri 24/02/17**			
Final Planning	**1 day?**	**Fri 24/02/17**	**Fri 24/02/17**			
Implementation	**1 day?**	**Fri 24/02/17**	**Fri 24/02/17**			
Business Critical	**1 day?**	**Fri 24/02/17**	**Fri 24/02/17**			
Subproject: Migrate Financial system 1	**1 day?**	**Fri 24/02/17**	**Fri 24/02/17**			
Establish connectivity	**1 day?**	**Fri 24/02/17**	**Fri 24/02/17**	**A6.2.2, A8.1.1, A1**	**Determine current VPN product, establish encryption standards,...**	
Order VPN concentrator for Ya Mon				A15.1.2,...	Determine spec of VPN concentrator, determine 3rd party suppo	
Configure VPN Concentrator				A12.1.1,...	Configure VPN concentrator to GIAC spec, ...	
.						
.						
.						
Migrate data	**1 day?**	**Fri 24/02/17**	**Fri 24/02/17**	**A8.3....**	**Ensure data backups are operational, recent backup available,...**	
Subproject: Migrate Financial system 2	**1 day?**	**Fri 24/02/17**	**Fri 24/02/17**			
.						
.						
.						
HR	**1 day**	**Fri 24/02/17**	**Fri 24/02/17**			
Reconnaisance	**1 day**	**Fri 24/02/17**	**Fri 24/02/17**			

Figure 3: WBS containing references to ISO Sections

Items used for assessing that a task has met the ISO 27001 domain include:

- Existing documentation;
- Security data;
- Interviews;
- Audit reports.

Any variations to this plan will be required to undertake a change control process.

Success criteria

The number of subprojects complied with the ISO27001 requirements could determine a successful migration. Subprojects would be rated using a Red, Amber, Green status (RAG status). Green indicates that it meets all ISO27001 criteria; Amber, some criteria was fulfilled; Red, no criteria was met or a serious issue discovered.

Note that the RAG status could also indicate that work may need to be deferred for later Phases thus, providing input for strategic planning. For example, a subproject with Amber tasks does not show that the activity is not secure, items not addressed may be vital elements such as user awareness or requires significantly more time and classified as a tactical function. The Cyber Security team would be expected to review the work before approving the amendment.

ISM6100 Assignment – Mergers and the Information Security aspects

Project Plan

Assignment Topic:

Mergers and the Information Security aspects

Assignment Scenario:

Your company, GIAC Enterprises, is a small to medium sized growing business (1,000 employees, two data centers, 200 people in central business and IT) and is the largest supplier of Fortune Cookie sayings in the world. They also have a large number of individual contractors, (in the US these are called 1099 based on their tax status), that submit fortune cookie sayings via a remote application. The CIO calls you in for a special tiger team project.

GIAC Enterprises employees are issued MacBook Pro Laptops. GIAC contractors have no standard, but from an analysis of web headers when they submit fortunes, they seem to be divided about equally between Mac and Windows. The goal of the project is to safely acquire another company.

The project focuses on the acquisition of another company, (Ya Mon Fortunes), by the GIAC Fortune Cookie Company. The acquisition has been approved by the boards of directors of both organizations and is currently proceeding through governmental and regulatory agencies for approval. The acquisition is expected to be approved and close[d] within the next two quarters. The assignment for the team would be to develop a plan for integration of the security architecture, operations, and processes acquired [of the] company into the infrastructure of the GIAC Fortune Cookie Company. The plan should focus on limiting the risk of introducing a breach into the GIAC infrastructure through the acquired company, while identifying and leveraging security best practices across both organizations, assessing and resolving vendor license agreement issues and minimizing duplicative capabilities, establishing connectivity between the two networks and facilitating the integration of business processes. Additionally the plan will include defining metrics to measure the success of the security integration efforts as a contributor to the broader business integration efforts.

Ya Mon Fortunes is located in Jamaica and there has been some unrest recently. Your team may need kidnap insurance.

Assignment Charter:

Develop a plan for integration of the security architecture, operations, and processes [of the] acquired company into the infrastructure of the GIAC Fortune Cookie Company.

Assignment Stakeholders:

- Andre Shori
  (project team member)
  <contact info redacted>
- Ed Yuwono
  (project team member)
  <contact info redacted>

- Dr. Stephen Northcutt
  Director Academic Advising
  The SANS Technology Institute
  (project advisor)
  <contact info redacted>

- Krysta Kurzynski
  (STI Advisor)
  <contact info redacted>

- Jason Lam
  (Sans Instructor/ Advisor)
  (project advisor)
  <contact info redacted>

Scope Management:

Assignment Requirements

- Safely acquire another company – Ya Mon Fortunes (Jamaica)

Scope (assignment)

- Develop a plan for integration of the security architecture, operations, and processes [of the] acquired company into the infrastructure of the GIAC Fortune Cookie Company.
- Focus on limiting the risk of introducing a breach into the GIAC infrastructure through the acquired company, while identifying and leveraging security best practices across both organizations, assessing and resolving vendor license agreement issues and minimizing duplicative capabilities, establishing connectivity between the two networks and facilitating the integration of business processes.
- Include defining metrics to measure the success of the security integration efforts as a contributor to the broader business integration efforts.
- Include an aspect of Physical Safety for the Project Team (kidnap insurance).

WBS (assignment)

Refer to Appendix A

Time Management:

Activities (assignment)

Sequence

- Project Plan – 10% of grade
- Project Labs (lab notebook) – 60% of grade
- Final Report – 20% of grade
- Reflections (individual) – 10% of grade

Resources

- Project Team - Andre Shori & Ed Yuwono
- Project advisors – Stephen Northcutt, Jason Lam
- STI advisor – Krysta Kurzynski
- External interviewees (planned) - Matthias <info redacted>, Jason Lam

Durations

- Project Plan - 5 days. Deadline - 7 Feb 2017 0000hrs UTC-7
- Project Labs/Research – 20 days. Deadline – 5 Mar 2017 0000hrs UTC-7
- Final Report – 5 days. Deadline – 5 Mar 2017 0000hrs UTC-7

Schedule (assignment)

Refer to Appendix B

Cost Management:

Costs/Budget

- Apart from course fees, there are no additional costs or budgetary requirements for the completion of this assignment.
- Any incidental costs will be borne out of pocket by project team members.

Quality Management:

Benchmarking

- Assignment will be benchmarked against existing samples on the STI group project webpage - https://www.sans.edu/cyber-research/group-projects

Project Plan (10% of grade)

- This document is the project plan and describes:
  - who is going to do what part of the work
  - how long are tasks expected to take
  - what is the schedule
  - The work breakdown structure

Lab Notebook (60% of grade)

- The lab notebook describes the technical approaches to the project. As described in the assignment document, "it will focus on the acquisition of another company by the GIAC Fortune Cookie Company. The key to a successful lab notebook is HOW, not ABOUT. There needs to be original research, interviews, surveys, tools etc, not just links found on the Internet."
  - "The problem/risk/vulnerability you were trying to solve/remediate".
  - "[O]ur thesis, why [we] thought it might work to solve the problem".
  - "[O]ur finding[s]".
- Lab notebook should capture all research, notes, interviews and other resources utilized during this assignment.
- Lab notebook can be submitted to Stephen Northcutt, cc'ing STI advisor, prior to final submission. Of particular focus will be the lab notebook format.

Final report (20% of grade)

- Final report will be benchmarked against existing examples on the STI group project webpage - https://www.sans.edu/cyber-research/group-projects
- Draft submissions can be submitted to Stephen Northcutt, cc'ing STI advisor, for comment prior to final submission

Reflections (10% of grade/individual)

- Team members are responsible for diarizing their own experiences and submitting individually.

- Draft submissions can be sent to Stephen Northcutt for comment prior to final submission

Quality Metrics

- Quality metrics will be largely assessed from feedback received from Project Advisors and integrated on an ongoing basis by project team members.
- Has GIAC enterprises, Ya Mon been through an M&A? If so, we can benchmark against that?

Change Requests

- Change requests to the assignment scope will be submitted to Stephen Northcutt, cc'ed to STI advisor and only implemented with written approval.

Human Resource Management:

- In the event of disputes or poor deliverables, mitigation actions are described in the risk management section of this project plan.
- Tools and software utilized by team members are free, off the shelf or licensed software already owned by team member. Examples of tools expected to be utilized on this project include Google Calendar, Skype. MS Project 2013, MS Office, Gmail. This list is non-exhaustive and can be expanded as required during the course of the assignment.

Communications Management:

Communications Management Plan (assignment)

Stakeholder	**Document**	**Format**	**Contact Person**	**Due**
Assignment Grading	Project Plan, Lab Notebook, Final Report, Reflections.	Word, Excel Word Word Word	Stephen Northcutt	**7 Feb 2017** **4 Mar 2017** **4 Mar 2017** **5 Mar 2017**
Project Advisors	Status Reports, Requests for information and advice Requests for information and advice	Emails Online Meetings Phone Emails Phone	Stephen Northcutt, Jason Lam	
STI Advisor	Project Plan, Lab Notebook, Final Report, Reflections.	Word, Excel Word Word Word	Krysta Kurzynski	**7 Feb 2017** **4 Mar 2017** **4 Mar 2017** **5 Mar 2017**

Risk Management:

Risks

- Time Management
- Time Zones
- Inaccessible resources particularly interviews
- Misunderstanding of assignment scope
- Misunderstanding the assignment deliverables
- Misunderstanding on deliverable ownership
- Missing deadlines
- Poor commitment by team member
- Poor deliverables by team member
- Disagreement regarding best approach to the assignment
- M&A skills are not present within the project team

Risk responses

- Time Management – team members have agreed to set all milestones as meeting requests in Google Calendar. Mandatory agendas for team meetings and calls will help to ensure better time management and keep us on track.
- Time Zones – team members have updated their Google calendars to reflect both time zones. Time zone difference between Sydney and Singapore is 4 hours and is not expected to have a major impact on team member's ability to deliver on their tasks.
- Inaccessible resources particularly interviews – Early identification of external assets and booking meetings/interviews early will mitigate much of the risks here. Fallback would be to look for alternate people to interview and if none are available, proceed with the assignment as best we can to fulfil all deadlines.
- Misunderstanding of assignment scope – constant checking and requests for feedback from project advisors will ensure clear and definite understanding of the assignment scope. Clear and constant communication between project team members will ensure that both team members clearly understand the scope.
- Misunderstanding the assignment deliverables - checking and requests for feedback before each project milestone from project advisors will ensure clear and definite understanding of the assignment scope. Clear and constant communication between

project team members will ensure that both team members clearly understand the deliverables.

- Misunderstanding on deliverable ownership – utilizing google calendars to document deliverable ownership and a clear project timeline will ensure that both team members have ownership of each task and milestone clearly defined.
- Missing deadlines- team members will again utilize google calendars as well as the project timeline and documentation to ensure that all deadlines are met. Open communication channels between team members will also aid in this effort. All project deadlines are at midnight of the due date (0000hrs of the following day).
- Poor commitment by team member – Open communication, documented deliverables and recorded submissions by each team member will help to ensure that both team members are delivering quality and meeting all deadlines. In the event of a dispute, a resolution will be requested by the offended team member from Stephen Northcutt, cc'ed to STI Advisor.
- Poor deliverables by team member – Open communication, documented deliverables and recorded submissions by each team member will help to ensure that both team members are delivering quality and meeting all deadlines. In the event of a dispute, a resolution will be requested by the offended team member(s) from Stephen Northcutt, cc'ed to STI advisor.
- Disagreement regarding best approach to the assignment – In the event of a dispute that cannot be settled between team members on the best approach to the assignment, the team members will consult with Stephen Northcutt, cc'ed to STI advisor, for resolution. The decision Stephen will be considered final.
- M&A skills are not present – Through research of white papers, examples and consulting with experienced professionals that have been through this process, it is the aim of this project team to be complete, thorough and as detailed as possible (particularly in the lab notes) to ensure that the recommendations we make to the CIO are the best possible ones.

Procurement Management

- No procurement is expected for this assignment
- The main project may require procurement

Stakeholder Management (assignment):

Stakeholder (name/role)	Importance (High/Med/Low)	Current Support Level	Desired Support Level	What's important to Stakeholder	What do we need from Stakeholder	Strategy to enhance support
Stephen Northcutt Project Advisor Grading	High	High	High	Project Deliverables Quality of deliverables Completeness	Advice Guidance Items that we may have missed	Engage Stephen through scheduled phone calls. Emails should be secondary or for quick answers.
Jason Lam Project Advisor	High	High	High	Quality of deliverables Completeness	Ideas Guidance Items that we may have missed	Introduce ourselves to Jason via email. Follow up with a phone call if possible. Keep asking relevant questions.
Krysta Kurzynski STI Advisor	Med	High	Med	Project Deliverables Project Final Grade Students GPA Students Engagement Level	Connections to resources within STI Project Submission	Keep updated, status report at each milestone. CC submission of all assignment deliverables to STI advisor.

Appendix A: WBS

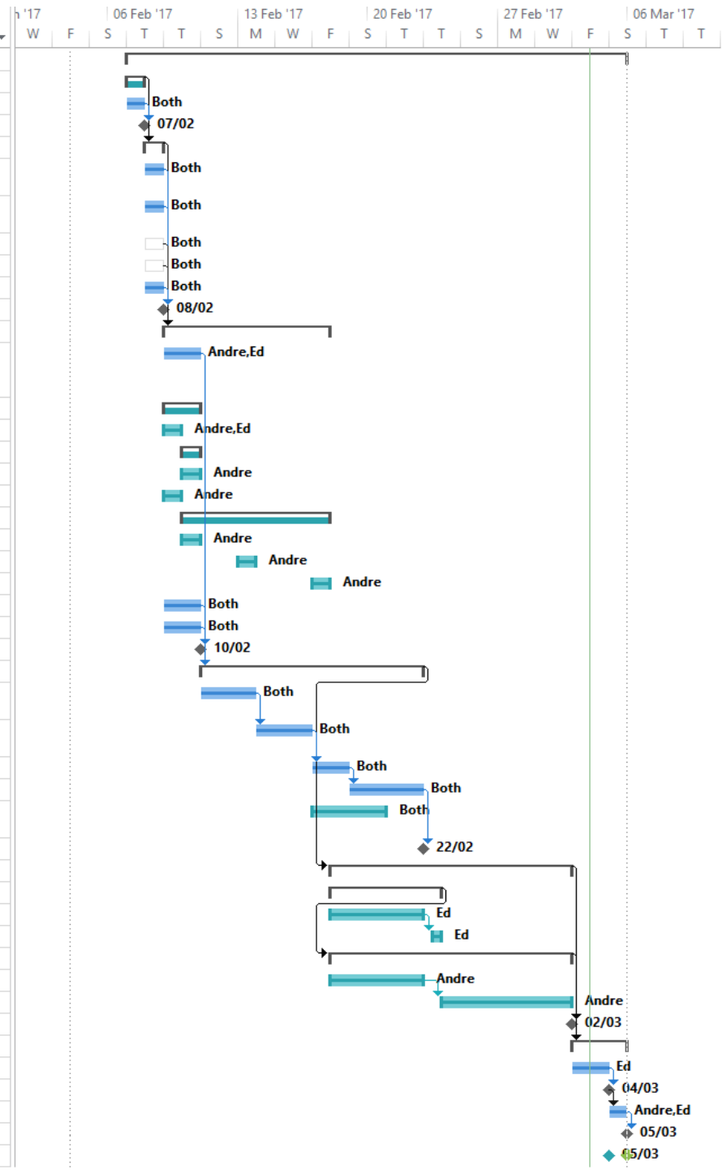
Task Name	Duration	Start	Finish	Predecessors	Notes	Resource Names	Milestone	WBS	% Complete	Detail
M & A Planning	**27 days**	**Tue 07/02/17**	**Sun 05/03/17**				**No**	**1**	**100%**	
Collect Assumptions	**1 day**	**Tue 07/02/17**	**Tue 07/02/17**		**Anything that hasn't been covered?**	**Both**	**No**	**1.1**	**100%**	
Collect Assumptions	1 day	Tue 07/02/17	Tue 07/02/17		Collect Business & Infosec assumptions	Both	No	1.1.1	100%	
Close Collect Assumptions	0 days	Tue 07/02/17	Tue 07/02/17	3	Close Collect Assumptions phase	Both	Yes	1.1.2	100%	
Check Assumptions	**1 day**	**Wed 08/02/17**	**Wed 08/02/17**	**2**	Gather information on previous M&As	**Both**	**No**	**1.2**	**100%**	
Stakeholder Analysis	1 day	Wed 08/02/17	Wed 08/02/17		Who has an interest in Yo Mon, any other M&A specialists	Both	No	1.2.1	100%	
Best Practice Identification	1 day	Wed 08/02/17	Wed 08/02/17		Identify industry, infosec best practice (standards, guidance, etc)	Both	No	1.2.2	100%	Adopting ISO 27001 as the base standard
~~Physical Asset Identification~~	~~1 day~~	~~Wed 08/02/17~~	~~Wed 08/02/17~~		~~Obtain information on physical assets~~	~~Both~~	~~No~~	~~1.2.3~~	~~0%~~	~~Removed due to change of approach~~
~~Technology Identification~~	~~1 day~~	~~Wed 08/02/17~~	~~Wed 08/02/17~~		~~Obtain information on technology assets~~	~~Both~~	~~No~~	~~1.2.4~~	~~0%~~	~~Removed due to change of approach~~
Risk Identification	1 day	Wed 08/02/17	Wed 08/02/17		Address the potential issues	Both	No	1.2.5	100%	
Close Check Assumptions	0 days	Wed 08/02/17	Wed 08/02/17	6,7,8,9,10	Close Check Assumptions phase	Both	Yes	1.2.6	100%	
Collect Requirements	**9 days**	**Thu 09/02/17**	**Fri 17/02/17**	**5**	**Collect Business & Infosec requirements**	**Both**	**No**	**1.3**	**100%**	
Interviews	2 days	Thu 09/02/17	Fri 10/02/17		Exact dates dependent on Interviewee availability but will be during this time period	Andre,Ed	No	1.3.1	100%	
Questionnaire	**2 days**	**Thu 09/02/17**	**Fri 10/02/17**			**Andre,Ed**	**No**	**1.3.2**	**100%**	
Devise	1 day	Thu 09/02/17	Thu 09/02/17			Andre,Ed	No	1.3.2.1	100%	
Distribute	**1 day**	**Fri 10/02/17**	**Fri 10/02/17**			Andre	**No**	**1.3.2.2**	**100%**	
Antonio	1 day	Fri 10/02/17	Fri 10/02/17		Provide questionnaire, email response	Andre	No	1.3.2.2.1	100%	
Identify Interviewees	1 day	Thu 09/02/17	Thu 09/02/17			Andre	No	1.3.3	100%	
Interviews	**8 days**	**Fri 10/02/17**	**Fri 17/02/17**			Andre	**No**	**1.3.4**	**100%**	
Jason	1 day	Fri 10/02/17	Fri 10/02/17		Interview over WebEx	Andre	No	1.3.4.1	100%	
Yee Ching	1 day	Mon 13/02/17	Mon 13/02/17		Face to face interview	Andre	No	1.3.4.2	100%	
Freddy	1 day	Fri 17/02/17	Fri 17/02/17		Face to face recorded interview	Andre	No	1.3.4.3	100%	
Articles	2 days	Thu 09/02/17	Fri 10/02/17		Research M&A lessons learned	Both	No	1.3.5	100%	
White papers	2 days	Thu 09/02/17	Fri 10/02/17		Research M&A checklists	Both	No	1.3.6	100%	
Close Collect Requirements	0 days	Fri 10/02/17	Fri 10/02/17	13,23,24	Close Collect Requirements phase	Both	Yes	1.3.7	100%	
Research Solution	**12 days**	**Sat 11/02/17**	**Wed 22/02/17**	**13**	**How will the integration be done?**	**Both**	**No**	**1.4**	**100%**	
Baseline functional requirements	3 days	Sat 11/02/17	Mon 13/02/17		What is required for the two orgs to function during M&A	Both	No	1.4.1	100%	
Baseline security requirements	3 days	Tue 14/02/17	Thu 16/02/17	27	What is required for the two orgs to be secure during M&A	Both	No	1.4.2	100%	Threats are listed and linked to the implementation WBS. Addressing each item in the WBS would combine to reduce the threat.
Priorise requirements	2 days	Fri 17/02/17	Sat 18/02/17	28	What is required for the M&A	Both	No	1.4.3	100%	
Devise Plan	4 days	Sun 19/02/17	Wed 22/02/17	29	Devise solution for M&A	Both	No	1.4.4	100%	
Revise Plan	4 days	Fri 17/02/17	Mon 20/02/17		Change of approach	Both	No	1.4.5	100%	Plan A did not work as planned, had to scrap and redo. Required after deliberation given that we're not going to go through the later phases (audit+) prior to approval. Rather than develop a detailed plan, we're developing a 'framework' for the impl. Team
Close Research Solution	0 days	Wed 22/02/17	Wed 22/02/17	30	Research Solution phase signoff/closure	Both	Yes	1.4.6	100%	
Propose Solution	**13 days**	**Sat 18/02/17**	**Thu 02/03/17**	**26**	**Report findings and compile solution documents**	**Both**	**No**	**1.5**	**100%**	
Implementation Framework	**6 days**	**Sat 18/02/17**	**Thu 23/02/17**		**Compile & Finalise implementation plan**	**Both**	**No**	**1.5.1**	**100%**	
Implementation F/w Draft	5 days	Sat 18/02/17	Wed 22/02/17		Compile 'C level' implementation plan	Ed	No	1.5.1.1	100%	
Implementation f/w Final	0.5 days	Thu 23/02/17	Thu 23/02/17	35	Finalise 'C level' implementation plan	Ed	No	1.5.1.2	100%	
Report	**13 days**	**Sat 18/02/17**	**Thu 02/03/17**	**34**	**Compile & Finalise report**	**Both**	**No**	**1.5.2**	**100%**	

Report Draft	5 days	Sat 18/02/17	Wed 22/02/17		Compile 'C level' report	Andre	No	1.5.2.1	100%	
Report Final	7 days	Fri 24/02/17	Thu 02/03/17	38	Finalise 'C level' report	Andre	No	1.5.2.2	100%	
Close Propose Solution	0 days	Thu 02/03/17	Thu 02/03/17	37	Propose Solution phase signoff/closure	Both	Yes	1.5.3	100%	
Close	**3 days**	**Fri 03/03/17**	**Sun 05/03/17**	**33**	**Project closing**	**Both**	**No**	**1.6**	**100%**	
Lab Notebook	2 days	Fri 03/03/17	Sat 04/03/17		Compile lab notebook	Ed	No	1.6.1	100%	
Final Submission	0 days	Sat 04/03/17	Sat 04/03/17	42	Submit all project documents	Both	Yes	1.6.2	100%	
Reflection Essay	1 day	Sun 05/03/17	Sun 05/03/17	43	Compile and submit reflection essay	Andre,Ed	No	1.6.3	100%	
Close Project	0 days	Sun 05/03/17	Sun 05/03/17	44	Close project phase signoff/closure	Both	Yes	1.6.4	100%	
Project Due	0 days	Sun 05/03/17	Sun 05/03/17		ISM 6100 Due date	Both	Yes	2	100%	

Andre Shori, ashori<at>mastersprogram.sans.edu
Ed Yuwono, Ed.Yuwono.MSISM<at>gmail.com

Appendix B: Schedule

Task Name	Duration	Start	Finish	Predec	Notes	Resource Names	Milestone	WBS	% Complete
M & A Planning	**27 days**	**Tue 07/02/17**	**Sun 05/03/17**				**No**	**1**	**100%**
Collect Assumptions	**1 day**	**Tue 07/02/17**	**Tue 07/02/17**		**Anything that hasn't been covered?**	**Both**	**No**	**1.1**	**100%**
Collect Assumptions	1 day	Tue 07/02/17	Tue 07/02/17		Collect Business & Infosec assumptions	Both	No	1.1.1	100%
Close Collect Assumptions	0 days	Tue 07/02/17	Tue 07/02/17	3	Close Collect Assumptions phase	Both	Yes	1.1.2	100%
Check Assumptions	**1 day**	**Wed 08/02/17**	**Wed 08/02/17**	**2**	Gather information on previous M&As	**Both**	**No**	**1.2**	**100%**
Stakeholder Analysis	1 day	Wed 08/02/17	Wed 08/02/17		Who has an interest in Yo Mon, any other M&A specialists	Both	No	1.2.1	100%
Best Practice Identification	1 day	Wed 08/02/17	Wed 08/02/17		Identify industry, infosec best practice (standards, guidance, etc)	Both	No	1.2.2	100%
~~Physical Asset Identification~~	~~1 day~~	~~Wed 08/02/17~~	~~Wed 08/02/17~~		~~Obtain information on physical assets~~	~~Both~~	~~No~~	~~1.2.3~~	~~0%~~
~~Technology Identification~~	~~1 day~~	~~Wed 08/02/17~~	~~Wed 08/02/17~~		~~Obtain information on technology assets~~	~~Both~~	~~No~~	~~1.2.4~~	~~0%~~
Risk Identification	1 day	Wed 08/02/17	Wed 08/02/17		Address the potential issues	Both	No	1.2.5	100%
Close Check Assumptions	0 days	Wed 08/02/17	Wed 08/02/17	6,7,8,9,10	Close Check Assumptions phase	Both	Yes	1.2.6	100%
Collect Requirements	**9 days**	**Thu 09/02/17**	**Fri 17/02/17**	**5**	**Collect Business & Infosec requirements**	**Both**	**No**	**1.3**	**100%**
Interviews	2 days	Thu 09/02/17	Fri 10/02/17		Exact dates dependent on Interviewee availability but will be during this time period	Andre,Ed	No	1.3.1	100%
Questionnaire	**2 days**	**Thu 09/02/17**	**Fri 10/02/17**			**Andre,Ed**	**No**	**1.3.2**	**100%**
Devise	1 day	Thu 09/02/17	Thu 09/02/17			Andre,Ed	No	1.3.2.1	100%
Distribute	**1 day**	**Fri 10/02/17**	**Fri 10/02/17**			Andre	**No**	**1.3.2.2**	**100%**
Antonio	1 day	Fri 10/02/17	Fri 10/02/17		Provide questionnaire, email response	Andre	No	1.3.2.2.1	100%
Identify Interviewees	1 day	Thu 09/02/17	Thu 09/02/17			Andre	No	1.3.3	100%
Interviews	**8 days**	**Fri 10/02/17**	**Fri 17/02/17**			Andre	**No**	**1.3.4**	**100%**
Jason	1 day	Fri 10/02/17	Fri 10/02/17		Interview over WebEx	Andre	No	1.3.4.1	100%
Yee Ching	1 day	Mon 13/02/17	Mon 13/02/17		Face to face interview	Andre	No	1.3.4.2	100%
Freddy	1 day	Fri 17/02/17	Fri 17/02/17		Face to face recorded interview	Andre	No	1.3.4.3	100%
Articles	2 days	Thu 09/02/17	Fri 10/02/17		Research M&A lessons learned	Both	No	1.3.5	100%
White papers	2 days	Thu 09/02/17	Fri 10/02/17		Research M&A checklists	Both	No	1.3.6	100%
Close Collect Requirements	0 days	Fri 10/02/17	Fri 10/02/17	13,23,24	Close Collect Requirements phase	Both	Yes	1.3.7	100%
Research Solution	**12 days**	**Sat 11/02/17**	**Wed 22/02/17**	**13**	**How will the integration be done?**	**Both**	**No**	**1.4**	**100%**
Baseline functional requirements	3 days	Sat 11/02/17	Mon 13/02/17		What is required for the two orgs to function during M&A	Both	No	1.4.1	100%
Baseline security requirements	3 days	Tue 14/02/17	Thu 16/02/17	27	What is required for the two orgs to be secure during M&A	Both	No	1.4.2	100%
Priorise requirements	2 days	Fri 17/02/17	Sat 18/02/17	28	What is required for the M&A	Both	No	1.4.3	100%
Devise Plan	4 days	Sun 19/02/17	Wed 22/02/17	29	Devise solution for M&A	Both	No	1.4.4	100%
Revise Plan	4 days	Fri 17/02/17	Mon 20/02/17		Change of approach	Both	No	1.4.5	100%
Close Research Solution	0 days	Wed 22/02/17	Wed 22/02/17	30	Research Solution phase signoff/closure	Both	Yes	1.4.6	100%
Propose Solution	**13 days**	**Sat 18/02/17**	**Thu 02/03/17**	**26**	**Report findings and compile solution documents**	**Both**	**No**	**1.5**	**100%**
Implementation Framework	**6 days**	**Sat 18/02/17**	**Thu 23/02/17**		**Compile & Finalise implementation plan**	**Both**	**No**	**1.5.1**	**100%**
Implementation F/w Draft	5 days	Sat 18/02/17	Wed 22/02/17		Compile 'C level' implementation plan	Ed	No	1.5.1.1	100%
Implementation f/w Final	0.5 days	Thu 23/02/17	Thu 23/02/17	35	Finalise 'C level' implementation plan	Ed	No	1.5.1.2	100%
Report	**13 days**	**Sat 18/02/17**	**Thu 02/03/17**	**34**	**Compile & Finalise report**	**Both**	**No**	**1.5.2**	**100%**
Report Draft	5 days	Sat 18/02/17	Wed 22/02/17		Compile 'C level' report	Andre	No	1.5.2.1	100%
Report Final	7 days	Fri 24/02/17	Thu 02/03/17	38	Finalise 'C level' report	Andre	No	1.5.2.2	100%
Close Propose Solution	0 days	Thu 02/03/17	Thu 02/03/17	37	Propose Solution phase signoff/closure	Both	Yes	1.5.3	100%
Close	**3 days**	**Fri 03/03/17**	**Sun 05/03/17**	**33**	**Project closing**	**Both**	**No**	**1.6**	**100%**
Lab Notebook	2 days	Fri 03/03/17	Sat 04/03/17		Compile lab notebook	Ed	No	1.6.1	100%
Final Submission	0 days	Sat 04/03/17	Sat 04/03/17	42	Submit all project documents	Both	Yes	1.6.2	100%
Reflection Essay	1 day	Sun 05/03/17	Sun 05/03/17	43	Compile and submit reflection essay	Andre,Ed	No	1.6.3	100%
Close Project	0 days	Sun 05/03/17	Sun 05/03/17	44	Close project phase signoff/closure	Both	Yes	1.6.4	100%
Project Due	0 days	Sun 05/03/17	Sun 05/03/17		ISM 6100 Due date	Both	Yes	2	100%



Andre Shori, ashori<at>mastersprogram.sans.edu
Ed Yuwono, Ed.Yuwono.MSISM<at>gmail.com

GIAC Enterprises

SANS STI ISM6100 Logbook

GIAC Enterprises M&A of Ya Mon

Authors: Andre Shori, ashore<at>mastersprogram.sans.edu

Ed Yuwono, Ed.Yuwono.MSISM<at>gmail.com

Advisor: Dr. Stephen Northcutt

Revision: 0.1

Contents

1. Executive Summary

This assignment required team members to develop a plan to integrate the IT functions of a merger and acquisition (M&A) of a company (Ya Mon) into the parent company (GIAC Enterprises). While our initial plan was to develop an integration blueprint, the team later found that the absence of crucial detail makes this option unviable. The final result was to develop a framework in which the parent company with limited resources and time constraints could utilize with their integration. This notebook will provide details into the decision making process and the events that shaped the assignment's outcome.

1.1. Pre-assignment Organization

Given the geographical and time differences, the team agreed to communications protocols and leveraged Google Drive for collaboration and shared calendars to organize regular meetings over WhatsApp or Skype. These protocols provided us with the ability to collaborate, delegate and review work.

2. Plan AThe Problem

The problem we attempted to resolve was to provide an implementation plan ensuring information security best practices. We addressed these best practices during the integration process for GIAC Enterprises. Intended for the CIO, the plan would provide a recommendation, an overall approach backed up by research, and alternative recommendations should the organization not meet time or resource constraints. The successful delivery of the project was dependent on a reporting mechanism (metric) ensuring that we addressed information security concerns throughout the plan.

2.2. Method

The overall assignment was broken down into sections to provide team members with an indication of progress. These sections are: Collect Assumptions, Check Assumptions, Collect Requirements, Research Solution, Propose Solution and close. This document outlines each phase.

2.3. Collect Assumptions

The collection assumptions section is focused on establishing governance for the assignment, obtaining information regarding the general M&A process and determine the role that information security has in the M&A process.

The team was required to define the primary goal and objectives of the assignment. After reviewing the plan, the team agreed that the overall aim regarding the M&A between GIAC Enterprises and Ya Mon was to ensure that the business continued to function during the integration process. The team's task was to make sure that the integration was secure.

To achieve this, we had to:

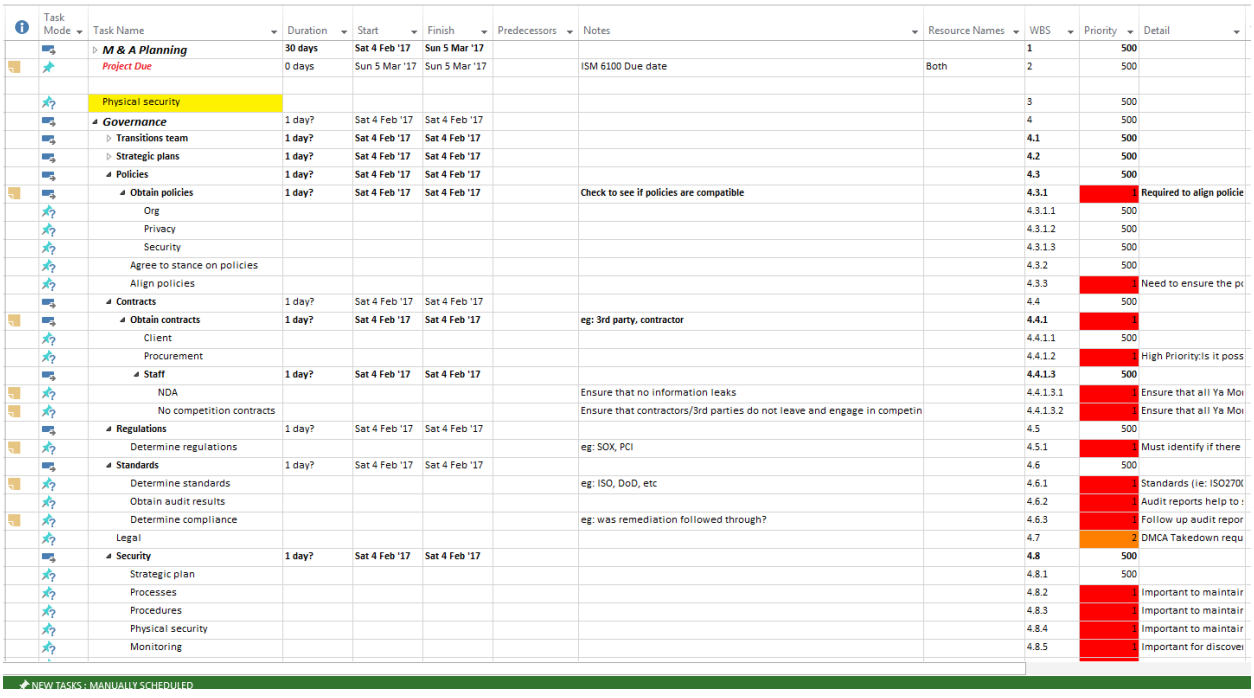
- Note the objectives provided for the assignment;
- Ensure that we addressed these during the integration process;
- Make sure that we conducted the integration process in a secure fashion by minimizing information security risks that could have resulted from the process.

To meet the objectives, the approach that the team adopted was to:

- Employ a project management approach to ensure management of resources for the assignment within the project's constraints;
- Produce the required project deliverables including a project plan, this notebook, a final report for attention of the CIO and personal reflections on the project;
- Assume that once the M&A Steering Committee granted approval; the timeframe provided for single operations would be short

With the team members not having managed an M&A process before, we conducted preliminary research to obtain an understanding of the effort involved. By carrying out internet research and white paper and case study reviews into the M&A process and their implications for information security, we devised a set of questions for the stakeholders and for professionals that have previously undertaken an M&A. The questions were designed to understand how the overall M&A process works, the board's expectations in the M&A process and lessons learned from their experiences (Appendix A).

A project plan along with a high-level work breakdown structure (WBS) was created (Figure 1) to provide governance for the integration. Given the limited information, an initial list of assumptions was generated for the team to progress through different phases. However, the success of each step depends on these assumptions being correct, and as a result, questions were devised and reviewed with the stakeholders to determine if the assumptions were true.



Task Mode	Task Name	Duration	Start	Finish	Predecessors	Notes	Resource Names	WBS	Priority	Detail
	M & A Planning	**30 days**	**Sat 4 Feb '17**	**Sun 5 Mar '17**				**1**	**500**	
	Project Due	0 days	Sun 5 Mar '17	Sun 5 Mar '17		ISM 6100 Due date	Both	2	500	
	Physical security							3	500	
	Governance	1 day?	Sat 4 Feb '17	Sat 4 Feb '17				4	500	
	Transitions team	**1 day?**	**Sat 4 Feb '17**	**Sat 4 Feb '17**				**4.1**	**500**	
	Strategic plans	**1 day?**	**Sat 4 Feb '17**	**Sat 4 Feb '17**				**4.2**	**500**	
	Policies	**1 day?**	**Sat 4 Feb '17**	**Sat 4 Feb '17**				**4.3**	**500**	
	Obtain policies	**1 day?**	**Sat 4 Feb '17**	**Sat 4 Feb '17**		**Check to see if policies are compatible**		**4.3.1**	**1**	**Required to align policie**
	Org							4.3.1.1	500	
	Privacy							4.3.1.2	500	
	Security							4.3.1.3	500	
	Agree to stance on policies							4.3.2	500	
	Align policies							4.3.3	1	Need to ensure the p
	Contracts	1 day?	Sat 4 Feb '17	Sat 4 Feb '17				4.4	500	
	Obtain contracts	**1 day?**	**Sat 4 Feb '17**	**Sat 4 Feb '17**		**eg: 3rd party, contractor**		**4.4.1**	**1**	
	Client							4.4.1.1	500	
	Procurement							4.4.1.2	1	High Priority:Is it poss
	Staff	**1 day?**	**Sat 4 Feb '17**	**Sat 4 Feb '17**				**4.4.1.3**	**500**	
	NDA					Ensure that no information leaks		4.4.1.3.1	1	Ensure that all Ya Mo
	No competition contracts					Ensure that contractors/3rd parties do not leave and engage in competin		4.4.1.3.2	1	Ensure that all Ya Mo
	Regulations	1 day?	Sat 4 Feb '17	Sat 4 Feb '17				4.5	500	
	Determine regulations					eg: SOX, PCI		4.5.1	1	Must identify if there
	Standards	1 day?	Sat 4 Feb '17	Sat 4 Feb '17				4.6	500	
	Determine standards					eg: ISO, DoD, etc		4.6.1	1	Standards (ie: ISO270
	Obtain audit results							4.6.2	1	Audit reports help to :
	Determine compliance					eg: was remediation followed through?		4.6.3	1	Follow up audit repor
	Legal							4.7	2	DMCA Takedown requ
	Security	**1 day?**	**Sat 4 Feb '17**	**Sat 4 Feb '17**				**4.8**	**500**	
	Strategic plan							4.8.1	500	
	Processes							4.8.2	1	Important to maintair
	Procedures							4.8.3	1	Important to maintair
	Physical security							4.8.4	1	Important to maintair
	Monitoring							4.8.5	1	Important for discover

NEW TASKS : MANUALLY SCHEDULED

Figure 1: Screenshot of WBS in MS Project

To ascertain the information security maturity level in which Ya Mon would be required to achieve, a comparison between both organizations is required. The baseline for the comparison is the security maturity level of GIAC Enterprises. Information about GIAC Enterprises was

obtained to determine the security maturity model. The team's approach was to create the initial assumptions and validate them during the check assumptions section. Assumptions include the potential size of the organization, their IT structure, information security capabilities and maturity. An example of this is in the next section.

Given the broad scope of information security disciplines possibly addressed in the assignment, it would have been tough to address them all. The approach taken by the team was to prioritize efforts based on the project brief, information gathered from interviews, along with any other areas being addressed based on our assertions.

Our first interview was with Jason Lam, who has completed several M&A implementations globally. During some of these M&A integrations, he assumed the role as interim CISO to provide information security guidance throughout the integration process. We believe that this experience provided the team with information on governing the information security aspect of the integration and an understanding of the overall M&A process.

After a constructive interview with Jason, the team discovered the importance of 'Day 0' - the date in which the two organizations would go live as one entity (Lam, 2017). Traditionally, most InfoSec projects would be dictated based on duration for the implementation of a particular project, whereas the go-live date has more impact during an M&A. As a result, we altered our thoughts on deployment to focus on Day 0 by working back from a go-live date (Day 0), focus on prioritization and emphasis on scope management. We scheduled high priority tasks required for continuous operation and items in the project brief previous to Day 0, with all other functions implemented after Day 0.

Jason provided an excellent overview of the M&A process and mindset. Utilizing the stories from the trenches that he provided, we have a much clearer understanding of the CIO and CEO's priorities. Clarity included the drivers and motivations during an M&A, which allowed us to prioritize more accurately. Some areas that were initially less important, such as legal considerations, were given more weight, and other tasks out of the IT department's control such as government approvals moved to a lower priority.

2.4. Check Assumptions

The objective for the Check Assumptions section was to confirm initial findings, establish boundaries for the assignment, address risks, and identify best practices that could be used to address the goals of our assignment.

Given the initial information gathered about the organizations and information obtained from interviews, the team proceeded to delve further to fill the gaps in knowledge specific to the integration. The team devised a set of questions to establish the boundaries of the project. These questions allowed us to achieve focus and obtain a realistic scope for the integration. Insufficient information about both organization's management, operations, and IT infrastructure meant that organizational research was required. A decision was made to gather detailed information on both companies starting with GIAC Enterprises, where the team resorted to previous papers from the SANS reading room for technical information. With the limited information available on Ya Mon, assertions were made based on them being a small company with a target market focused solely in Jamaica such as:

- Jamaica is a small nation of close to 3 million people[1];
- The target market for the product (fortunes) would namely be fortune cookie manufacturers or the spiritual industry;
- With competition on a global scale, especially from large Asian communities, coupled with the fact that GIAC is the biggest supplier of fortunes in the world, Ya Mon would be smaller (perhaps significantly) than GIAC;
- Given the size of GIAC and the available resources, it is more likely that they are unable to promote themselves on a global scale effectively;
- All factors considered, their primary market would be Jamaica or the wider Caribbean region.

In response to our questions, Stephen provided the team with the opportunity to define GIAC's decision behind the M&A process (Northcutt, personal communication Feb 8, 2017).

[1] Jamaica Population (2017) - Worldometers. (2017, March 1). Retrieved from http://www.worldometers.info/world-population/jamaica-population/

The team made several high-level assertions to steer the C level's thought process and provide direction to the assignment. We based the statements below on interviews with M&A specialists, internet research, and white papers

- GIAC is in the growth phase;
- GIAC wants to enter the Caribbean market and recognize that Ya Mon provides an opportunity to do so;
- This M&A is not a buy then sell transaction, and selling Ya Mon shortly after was not the strategic goal.

Based on the assertions, the following recommendations were put forward to the board:

- GIAC does not have M&A experience, and it would be advisable that they engage a consultancy in an advisory capacity to provide guidance, especially given that GIAC may choose to pursue another acquisition in the future;
- Effort must be made to retain key staff within Ya Mon during the integration process to provide knowledge and input for the integration (Rouse & Frame, 2009). As Ya Mon staff possess intimate knowledge of their environment, it would be prudent for GIAC to utilize their expertise to maximize the potential of a successful delivery.
- Closer examination is required of the Jamaican regulatory landscape to avoid breaches of any local legislation.

The team set out to develop an integration plan using this information. Despite searching for a standard or case study to construct an M&A integration, the team could not find an appropriate framework. After speaking to Jason, each organization had specific requirements and made any textbook approach very challenging. As a result, the team decided to develop their own based on the information gathered.

The first step to the integration plan was to determine the order of operation during the M&A process. Each transaction would then be broken down into manageable work by the integration team. The team approached this by determining the priorities the board would expect from the integration process.

GIAC is committed to leveraging Ya Mon's acquisition as soon as possible, however, with limited resources, prioritization is essential to achieve this goal. Ya Mon's assets such as their cookie database, customer database, and sales teams are the focus of GIAC's acquisition and must be integrated by Day 0. To appropriately allocate resources for protection efforts, two initial actions were required. The first is the identification of assets and the prioritization of tasks associated with the handling of these assets. With the focus on business continuity, the second action was for the team to develop a tiered scheme for the classification prioritization of property as listed below.

Tier 1 classification centered on the protection of the core IP and any related property that, when compromised, would result in the complete loss of the company the next day (would cease to exist/operate and have zero chance of recovery). An example of which would be if GIAC lost its fortune cookie sayings database.

Tier 2 classification was for assets that would disrupt operations or have an adverse impact, but the organization will most likely be able to continue (for example, if our employee PII was leaked, the organization will be required to compensate for the loss. However, we could still operate).

We decided that Tier 3 classification would be any items/assets that did not fit the above criteria.

We then took a step back and reviewed our rating system from the boards' perspective. Given that we know the board will communicate in business process terms, we decided to map the business processes to our classification system (Figure 2).

Subcategory1	Subcategory2	Subcategory3	Priority	Notes	countermeasures	#Draft5	WBS Draft5	(ISC)2 domain	Duration
Background info	Type of business		Done	Manufacturing	already determined				
Background info	Physical location		Done	US, Indonesia, Jamaica	already determined			2. Asset Security 5. Identity and Access Management 7. Security Operations	
Security	Disgruntled Employees		Tier 1	Risk to IP	access controls, awareness training, behavioural analytics, physical security	180	9.2.1	1. Security and Risk Management 5. Identity and Access Management	3
Security	Disgruntled Employees		Tier 1	Risk to IP	access controls, awareness training, behavioural analytics, physical security	211	9.2.4.2.4	1. Security and Risk Management 5. Identity and Access Management	2
Security	Disgruntled Employees		Tier 1	Risk to IP	access controls, awareness training, behavioural analytics, physical security	203	9.2.4.1.4	1. Security and Risk Management 5. Identity and Access Management	3
Security	Disgruntled Employees		Tier 1	Risk to IP	access controls, awareness training, behavioural analytics, physical security	190	9.2.2.2.3	1. Security and Risk Management 5. Identity and Access Management	2
Security	Disgruntled Employees		Tier 1	Risk to IP	access controls, awareness training, behavioural analytics, physical security	186	9.2.2.1.3	1. Security and Risk Management 5. Identity and Access Management	1
Security	Disgruntled Employees		Tier 1	Risk to IP	access controls, awareness training, behavioural analytics, physical security	155	8.6.2	1. Security and Risk Management 5. Identity and Access Management	1
Security	Disgruntled Employees		Tier 1	Risk to IP	access controls, awareness training, behavioural analytics, physical security	107	5.1.5	1. Security and Risk Management 5. Identity and Access Management	2
Security	Disgruntled Employees		Tier 1	Risk to IP	access controls, awareness training, behavioural analytics, physical security	82	4.4.1.3.1	1. Security and Risk Management 5. Identity and Access Management	1
Security	Disgruntled Employees		Tier 1	Risk to IP	access controls, awareness training, behavioural analytics, physical security	83	4.4.1.3.2	1. Security and Risk Management 5. Identity and Access Management	3
Security	Redundant Employees		Tier 1	Don't fire the people we need to complete the M&A, especially the audit	access controls, awareness training, behavioural analytics, physical security	180	9.2.1	1. Security and Risk Management 5. Identity and Access Management	1
Security	Redundant Employees		Tier 1	Don't fire the people we need to complete the M&A, especially the audit	access controls, awareness training, behavioural analytics, physical security	211	9.2.4.2.4	1. Security and Risk Management 5. Identity and Access Management	3
Security	Redundant Employees		Tier 1	Don't fire the people we need to complete the M&A, especially the audit	access controls, awareness training, behavioural analytics, physical security	203	9.2.4.1.4	1. Security and Risk Management 5. Identity and Access Management	1
Security	Redundant Employees		Tier 1	Don't fire the people we need to complete the M&A, especially the audit	access controls, awareness training, behavioural analytics, physical security	190	9.2.2.2.3	1. Security and Risk Management 5. Identity and Access Management	3
Security	Redundant Employees		Tier 1	Don't fire the people we need to complete the M&A, especially the audit	access controls, awareness training, behavioural analytics, physical security	186	9.2.2.1.3	1. Security and Risk Management 5. Identity and Access Management	2
Security	Redundant Employees		Tier 1	Don't fire the people we need to complete the M&A, especially the audit	access controls, awareness training, behavioural analytics, physical security	155	8.6.2	1. Security and Risk Management 5. Identity and Access Management	2
Security	Redundant Employees		Tier 1	Don't fire the people we need to complete the M&A, especially the audit	access controls, awareness training, behavioural analytics, physical security	107	5.1.5	1. Security and Risk Management 5. Identity and Access Management	1
Security	Redundant Employees		Tier 1	Don't fire the people we need to complete the M&A, especially the audit	access controls, awareness training, behavioural analytics, physical security	82	4.4.1.3.1	1. Security and Risk Management 5. Identity and Access Management	3
Security	Redundant Employees		Tier 1	Don't fire the people we need to complete the M&A, especially the audit	access controls, awareness training, behavioural analytics, physical security	83	4.4.1.3.2	1. Security and Risk Management 5. Identity and Access Management	3
Security	Disgruntled Employees	Relocated Employees	Tier 1		access controls, awareness training, behavioural analytics, physical security	180	9.2.1	1. Security and Risk Management 5. Identity and Access Management	1
Security	Disgruntled Employees	Relocated Employees	Tier 1		access controls, awareness training, behavioural analytics, physical security	211	9.2.4.2.4	1. Security and Risk Management 5. Identity and Access Management	3
Security	Disgruntled Employees	Relocated Employees	Tier 1		access controls, awareness training, behavioural analytics, physical security	203	9.2.4.1.4	1. Security and Risk Management 5. Identity and Access Management	1
Security	Disgruntled Employees	Relocated Employees	Tier 1		access controls, awareness training, behavioural analytics, physical security	190	9.2.2.2.3	1. Security and Risk Management 5. Identity and Access Management	1
Security	Disgruntled Employees	Relocated Employees	Tier 1		access controls, awareness training, behavioural analytics, physical security	186	9.2.2.1.3	1. Security and Risk Management 5. Identity and Access Management	1
Security	Disgruntled Employees	Relocated Employees	Tier 1		access controls, awareness training, behavioural analytics, physical security	155	8.6.2	1. Security and Risk Management 5. Identity and Access Management	1

Figure 2: WBS with Tier Mappings

Brainstorming techniques allowed the team to categorize WBS tasks according to business impact. We changed the names of the classification scheme from "Tiers" to "Business Critical," "Business Important" and "Business Strategic" to provide clarity for the stakeholders.

We divided the implementation into several phases: Reconnaissance, audit, planning, integration, validation and signoff. The phases are as follows:

- Reconnaissance provided necessary information about Ya Mon to allow the integration team to determine the state of Ya Mon.
- Audit verifies Ya Mon against the state defined in the Reconnaissance phase.
- Planning develops a plan for integration
- Validation tests the integration from an operational point of view
- Signoff is the official business acceptance of the integration

Despite the vast amount of unknowns at this stage of the M&A, we checked our system to ensure that it was flexible and robust enough to withstand potential changes. For example, integration resources will initially focus on critical IP such as the fortune sayings database, should the board redirect their priority to sales, will the plan work? With one of us playing

devil's advocate, we put our plan through some Q&A and concluded that it did still fulfill the scope of our assignment.

During this phase, the team set out to identify risks that could derail the project. The biggest risk was that many details were missing for the project. The team approach to addressing this risk is to interview M&A professionals and create a profile for Ya Mon based on the gathered information.

As stakeholders are one of the biggest influences on the outcome of a project, we also discussed, expanded and finalized our stakeholders for the integration project. This discussion allowed us to prepare a RACI chart to aid in stakeholder management and communication (Figure 3). Subsequently, however, we ended up not using the RACI chart in the CIO report as it did not fit into the high-level strategy that we proposed. We also created a stakeholder communications plan to help us ensure that all stakeholders would be updated and the best methods for communicating with them during the integration. The communications plan (Figure 4) was also subsequently not used for final assignment submission.

RACI For GIAC Enterprises M&A

	recon															
Stakeholders	Strategic plans	Policies	Contracts	Regulations	Standards	Legal	Staff vetting/capabilities	Access control	asset mgt	physical sec (layout)	design diagrams	ops processes	procurement	security processes	bcp/drp processes	crypto
Project Manager	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
PMO	C,I	C, I	I	I	C,I	I	I	I	I	I	I	I	I	I	I	I
M&A Steering Committee	C,I	C,I	C,I	C,I	C,I	C,I	C,I	C,I	C,I	C,I	C,I	C,I	C,I	C,I	C,I	C,I
GIAC Enterprises Board	C,I	C, I	C,I	C, I	C, I	C, I	C, I	I	I	I	I	I	I	I	I	I
Ya Mon Fortunes Board	C, I	C, I	C,I	C,I	C,I	C,I	C,I	I	I	I	I	I	I	I	I	I
GIAC Enterprises Risk Management team (includes audit team)	R, I	R, I	R, I	R, I	R, I	R, I	R, I	R, I	R, I	R, I	R, I	R, I	R, I	R, I	R, I	R, I
Ya Mon Fortunes Risk Management team (includes audit team)	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C
GIAC Enterprises Infrastructure team	-	-	-	-	I	-	-	C	I	I	I	I	I	I	I	-
Ya Mon Fortunes Infrastructure team	-	C	-	-	C	-	-	C	C	C	C	C	C	C	C	-
GIAC Enterprises Operations team	I	-	-	-	I	-	-	C	I	I	I	I	I	I	I	-
Ya Mon Fortunes Operations team	C	C	-	-	C	-	-	C	C	C	C	I	C	C	C	-
GIAC Enterprises Application team	I	-	-	-	I	-	-	C	C	-	I	C	-	I	I	I
Ya Mon Application Team	C	C	-	-	C	-	-	C	C	-	C	-	-	C	C	C
GIAC Enterprises Cybersecurity team	I	I	I	I	I	I	I	R	I	I	I	I	I	I	I	I
Ya Mon Fortunes Cybersecurity team	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C
Employees (both)	-	C	-	-	-	-	-	-	-	-	-	C	-	C	-	-
GIAC Enterprises Individual Contractors (fortune cookie sayings)	-	-	-	-	-	-	-	-	C	-	-	-	-	C	-	-
Ya Mon Individual Contractors (fortune cookie sayings)	-	C	-	-	C	-	-	-	C	-	-	-	-	C	-	-
GIAC Change Management Board	I	-	-	-	-	-	-	-	I	-	-	I	I	-	-	-
Ya Mon Change Management Board	C	C	-	-	C	-	-	-	C	-	-	C	C	-	C	-
Legal Team	C,I	C, I	C, I	C, I	C, I	R, C, I	C, I	C	C, I	C, I	-	-	C, I	C, I	C, I	C, I
Integration Project Team	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R
Finance (both)	C,I	C	-	C, I	C	C, I	-	C	C	-	-	C, I	C,I	C,I	C, I	-
Ya Mon HR	-	C	-	C	C	C, I	C	C	C	-	-	-	-	C,I	-	-
GIAC HR	-	-	-	I	I	I	C	C	I	-	-	-	-	I	-	-
Customer Support	-	C	-	C	C, I	C, I	-	C	C	-	C	C	-	C	C	C
GIAC Customers	-	-	-	-		-	-	-	-	-	-	-	-	-	-	-
Ya Mon Customers	-	-	-	-	C	-	-	-	-	-	-	-	-	C	-	-
Production (both)	-	C	-	C	C	C	-	C	C	-	-	C	-	C,I	C	-

Responsible (also Recommender)
Those who do the work to achieve the task.[7] There is at least one role with a participation type of responsible, although others can be delegated to assist in the work required.

Figure 3: GIAC M&A RACI Chart

Communications Management:

Communications Management Plan (Project)

Note: Communications to any Ya Mon employees only after NDA and written permission from GIAC Enterprise CTO

Stakeholder	Document	Format	Contact Person	Due
GIAC Enterprises Board	Monthly Project Status Report	Word PowerPoint Phone F2F/ Video Conference	GIAC Enterprise CEO Admin	Monthly
GIAC Enterprises CIO	Weekly Project Status Report	Word PowerPoint Email Phone F2F/ Video Conference	GIAC Enterprises CIO	Weekly
Ya Mon Fortunes Board	Monthly Project Status Report	Word PowerPoint Email Phone Video Conference	To be determined	Monthly
GIAC Enterprises Risk Management team	Weekly Project Status Report Weekly Project Meeting	Word PowerPoint Email Phone F2F/ Video Conference	GIAC Risk Manager	Weekly On Demand
Ya Mon Fortunes Risk Management team	Weekly Project Status Report Weekly Project Meeting	Word PowerPoint Email Phone F2F/ Video Conference	Ya Mon Risk Manager	Weekly On demand
GIAC Enterprises Infrastructure team	Weekly Project Status Report Weekly Project Meeting	Word PowerPoint Email Phone F2F/ Video Conference	GIAC Infrastructure Manager	Weekly On Demand
Ya Mon Fortunes Infrastructure team	Weekly Project Status Report Weekly Project Meeting	Word PowerPoint Email Phone Video	Ya Mon Infrastructure Manager	Weekly On Demand

Figure 4: Communications plan for GIAC's M&A

2.5. Collect Requirements

The Collect Requirements section will aim to provide structure for the project by conducting interviews to confirm the approach, address potential issues and ensure that the proposed plan was sound.

Our leading M&A person dropped out (Matthias), and as a result, we resorted to industry contacts and the advisory board in search of professionals with M&A experience. We received a few responses from different sources and decided on choosing face to face interviews where possible.

We arranged an interview with a technical specialist to gain perspective on technological aspects of our M&A. Yee Ching was a technical lead for an M&A between two medium sized security companies in Singapore. The meeting provided several suggestions such as conducting a SWOT analysis before the merger, however, due to time constraints for the integration, this was not feasible.

Yee Ching also suggested that a 1000 employee company is a medium sized enterprise, with enough budget to handle much of the M&A activities (Tok, 2017). Sending a ten person team to Jamaica for a week or two would be realistic (Tok, 2017). Based on this information, the team decided that for this scenario it would be plausible to send a security engineer, an auditor, a few members from various operations verticals and some support staff over to Jamaica to conduct due diligence.

Based on the conversation with Yee Ching, we proposed utilizing a scorecard metric for the CIO. One that is simplified with a red/yellow/green color scheme but would be grounded in the various criteria/KPI's/tests before we would declare the asset “appropriately protected” (Tok, 2017). The scorecard would serve as a very high-level milestone chart. The board could use this scorecard to authorize proceeding to the next stage of the M&A.

After the interview, a group discussion was held to review the content of the C-level report. On a high level, the C level report should include an executive summary, business goals, metrics, issues/show stoppers, explored alternatives and a conclusion. The parameters provided a measurement to support each recommendation.

The goal of the report was to provide the board with an assurance that the organization will be operating throughout the integration by:

- Identifying all critical business operations;
- Working with respective business units to ensure operations.

The metric would provide a measurement of countermeasures against threats to operations by:

- Identifying threats against business operations;
- Developing a mitigation strategy to threats against operations;

- Measuring that the combined effect of the mitigation plan serves to reduce risks.

Given the information provided, we proceeded to draft up a high-level plan based on the assertions on Ya Mon to date. However, we hit a stumbling block. A Day 0 is required, the day when both companies operated as one entity. We requested a Day 0 from Stephen N, and he responded with 'up to us,' indicating that we should recommend or define a Day 0 (Northcutt, personal communication Feb 14, 2017). We discussed and decided that in the real world, the board would establish a Day 0. As a result, the plan would need to be flexible enough to work around the board's decision, and any metric will need to highlight any security shortfalls based on the board's decision.

2.5.1. Subsection: Dynamic Metrics

In short, a list of threats to the organization was mapped to individual controls while each WBS had one or more controls assigned to it. The metric worked on the premise that a combined collection of WBS would reduce the potential of an exploitable threat. Completion of WBS tasks would minimize all the identifiable threats. The board would be able to visualize this with a sliding scale which determines Day 0. Should the board request that Day 0 would be very soon, there is a high probability that risk would remain before integration. Conversely, a longer Day 0 would provide an opportunity to implement controls to mitigate these risks. Appendix B presents an illustration of our security metrics.

However, circumstances prevented us from employing this technique. Firstly, a change in direction later in the assignment meant that we did not have the detail required to demonstrate it is effectiveness. Secondly, correspondence with Stephen N hinted that some focus should be made to prevent a 'tiny Yahoo.' This hint was concerning the Yahoo/Verizon M&A where Yahoo was breached and did not disclose these violations to Verizon (Northcutt, personal communication Feb 20, 2017; Northcutt, Security: Yahoo Verizon Breach Impact on Future M&A, 2016). Finally, we were over-engineering a metric when there was a simpler method.

2.6. Research Solution

The Research Solution phase combines the all the requirements obtained and devise a plan.

Comparing the replies from our M&A questionnaires, we noted that the approaches people took, and the mindset towards prioritization were all quite different. Given the stage of the assignment we were at, having finalized the approach we are taking, we did not expect to change our strategy at that point. We did note that there was much room for knowledge capture and exchange on this topic within our industry and that this area might be a good presentation topic.

Freddy Tan's interview proved to be immensely helpful for our project. Freddy is a very senior Cybersecurity figure in Singapore, a former ISC2 Global President and was in the cyber security industry before it was even called cyber security. Currently, the Director of Enterprise Security at Singtel, Freddy works in close collaboration with senior management. He also did his Master's thesis on M&A at the London School of Economics.

Freddy gave us the CIO's point of view in an M&A. What's relevant to a CIO? How would one approach an M&A from a strategic perspective? We came away from the interview feeling like we finally "got it."

After the interview, it was now clear to us that our approach was not achievable. We were focused on a full end to end integration plan for the integration of Ya Mon into GIAC. What we now clearly realized was that there would already be an integration plan put together by the various verticals and a steering committee would be making the decisions on how to do the integration. Business owners and the integration team would put forward recommendations and business cases. The M&A Steering Committee would then approve or deny and the result would be the "bigger integration effort."

Given the number of possibilities that the M&A Steering Committee could decide combined with a great many unknowns, it would not be prudent for the team to provide a

detailed implementation plan. The team should be developing a framework which the committee could utilize to complete the integration. In light of the events that has transpired, the team decided to start again and devise a framework.

3. Plan B

The revised problem was to provide an implementation framework ensuring addressing of information security best practices during the integration process for GIAC Enterprises. Intended for the CIO, the framework would provide an end to end structure for the M&A committee to follow and we embedded security best practices within the framework to minimize the risk of a breach.

3.1. Research Solution

What the team was required to do was propose to the CIO how the team would fit into the bigger plan. How do we come up with a working plan that would be flexible enough given that we know nothing about Ya Mon right now, but would allow us to remain safe and secure? What we needed to do, in essence, was to write a car manual for a car that didn't exist yet.

The best way to do that is to outline how one would write the manual as the car slowly came into existence. Instead of the complete handbook (the full integration plan for Ya Mon), we needed to write how to create a car manual (a guide on how to build a safe integration plan for Ya Mon).

This understanding represented a significant change in strategy. We realized that we had gone too far and into too much detail in our earlier plan. Furthermore, the team did not provide stakeholders with the opportunity to give input into the project. This flaw became evident as we compiled the draft CIO report. Initially, we had the business classifications and the phases lined up (from our WBS), and as we wrote the first draft, we outlined the strategy for creating the M&A integration plan. Halfway through, we took stock, realized that again we were attempting to create something that would be a company-wide effort and not led by the cyber security team.

The challenge we were now facing was how to write a cyber security strategy for an integration plan that still did not exist yet. Turning the problem on its head, we then asked ourselves, how would we add cybersecurity to the integration project as the integration team created it?

The relevant question at that stage was then how would an integration plan be created? What would GIAC likely do, given its size and capabilities, to create a plan? After talking to Freddy and Jason, we already knew that they would have a steering committee that will make the final decisions for the integration but currently, nothing of the sort existed.

The team then decided that we would propose a framework, employing the primary phases from our original plan, use that framework to highlight security concerns and provide the business with recommendations. We would also be able to illustrate on a high level where the team would focus resources and what would be considered important from a cyber security perspective.

The business processes would dictate how technology and security would support these processes. From the interviews, the team is aware that one of the first things both companies needed to do was to come to an agreement on what policies and standards would emerge from the integration. Obtaining information from both organizations is necessary. After that a comparison of standards and policies before alignment is possible.

Several methods can be used to achieve this goal. From Jason's interview, he had mentioned "parachuting in" and doing a covert audit of a target company. Freddy had suggested a formal request for information (RFI) process as an alternative (Tan, 2017). Our team suggested that conducting business intelligence would be another method to get more information. Finally, GIAC would have compiled information about Ya Mon before obtaining approval; this information would also be of value (if made available).

The team recommended that recon remains the first phase of our integration. This stage of the merger requires facts. Following recon, the other steps would follow. The Audit Phase would validate the recon (however that would likely have to wait for M&A approval, and Ya Mon was handed over).

Mapping the phases into a model, and the team realized that there is a significant time gap between these phases as the merger underwent regulatory approval. Through the pre-planning phase, this gap allows all stakeholders involved with the M&A, to start planning. After the first round of planning and validating our reconnaissance data against the audit, we would then validate and improve the integration plans and when ready, propose them to the M&A steering committee for final approval and a go/no-go decision.

The M&A steering committee would consult the business units and obtain the tasks required to for the integration process. The categories mentioned in Plan A: Business Critical, Business Important, and Business Strategic, help prioritized the tasks. The information security team would then assign the controls as noted in the section ‘revised metric’ below. Once approved, we converted these duties into a subproject for implementation.

The assignment lists several objectives for completion during the integration. Business Critical tasks nominated by the M&A steering committee would include establishing connectivity between the two networks to allow continuity of operations. Under guidance from the information security team, controls taken from the ISO2700x standards applied as part of the implementation of the subproject.

Business Important tasks would include assessing and resolving vendor license agreement issues as it would serve to reduce long-term costs as various systems have completed integration. Business Strategic would include minimizing duplicative capabilities as staff would be required for most of the integration process to retain inside knowledge while HR processes and union policies may need a plan of action should mass layoffs occur.

The M&A integration team would adopt Freddy's approach and issue a request for information on information about any prior breaches or significant incidents that the organization has experienced to minimize the chance that a 'small Yahoo' would occur (Tan, 2017). The sooner this information is obtained, the sooner that compensatory action could be taken such as requesting a lower offer for Ya Mon, reimbursement for remediation or compensation efforts.

3.2. Revised Metric

The absence of detail around the business functions meant that the metric did not 'hold up' and a new one was required. As GIAC has adopted ISO 27001 as their standard, we decided that these specifications would form the basis for the new shared metric. The standard was used as a baseline to compare security initiatives between the two organizations. The fact that ISO 27001 is an established global standard meant that organizations globally could employ the norm and have a common protocol to assess their security maturity.

As ISO27001 is risk-based and not prescriptive, organizations could employ measures to meet each criterion. While the measures may be subject to debate, there is a shared understanding between both companies on what the objective of the measure would achieve.

Implementing the metric was similar to plan A. Each WBS object had one or more ISO27001 controls assigned to it. Assuming all the WBS tasks were completed, the associated ISO27001 controls would also be implemented. The combined controls would contribute to the compliance of ISO27001 and success achieved with the achievement of ISO27001 certification for the combined GIAC/Ya Mon entity.

As a working example from the assignment, establishing connectivity between the two networks is one task that would require controls such as, ensuring that the asset is recorded (ISO 27001 section 8), apply access control to the device (section 9) and so on (IsecT, n.d.).

A note on employing ISO27001 as a comparative metric. The assignment pointed out that due to the conditions in Jamaica, Kidnap Insurance was relevant. We address Kidnap Insurance

as an extension to ISO 27001 Human Resource Security section 7.2 (IsecT, n.d.). Staff would be expected to follow protocol to ensure that they are safe.

3.3. Solution Revision

Acting on feedback from Stephen N for our final draft of the report, we decided to include more information regarding the proposed timelines and costing for our integration. As later steps depend on the previous phases, we were only able to give some cost estimates up till the Audit Phase. Information from the recon phase or which processes approved for integration or which system would act as a baseline and which were to be integrated and so on, would impact subsequent charges.

We recommended sending a recon team to Ya Mon and costing for our portion of the group was derived as follows. To price the flight, we needed to determine the starting point. After discussion, we decided that San Francisco would make the most sense for GIAC headquarters, as it is known for innovative, trendy tech companies and has a large Asian community (which would support the fortune cookie market). We then researched the cost of the flight from San Francisco to Montego Bay, Jamaica, We looked up a suitable hotel rate and added in a per diem (daily expense) for the engineer. We also were able to estimate and add in kidnap insurance[2] (based on a detail in our assignment spec) and travel insurance[3] (medical).
Our team also did check into the actual situation on the ground in Jamaica and were able to find a report from the US Department of State listing Jamaica's overall crime and safety situation as "critical." We felt that this certainly justified our decision to include kidnap and travel insurance, as well as ensure that our engineer would stay at the Hilton (a reputable hotel) and have enough of an expense account to get reliable transport to and from Ya Mon's operations. If necessary, we could also arrange secure transport via the hotel. However, we left this option open for now.

[2] A Guide To Kidnap & Ransom Insurance Coverage | Investopedia. (2015, July 29). Retrieved from http://www.investopedia.com/articles/personal-finance/062915/guide-kidnap-ransom-insurance-coverage.asp
[3] Visitors medical Insurance, Visitors Medical Insurance plans, USA Visitors Medical Insurance. (2017, March 1). Retrieved from https://www.americanvisitorinsurance.com/insurance/visitors-medical-summary.asp

Estimated Travel Cost			
Arrives Monday 6 March 2017, leaves Friday 10 March 2017			
Flight[4]	business round trip	USD	$ 1,473.00
Hotel[5]	4 nights	USD	$ 2,288.00
Expenses[6]	100/day	USD	$ 500.00
Kidnap Insurance[7]		USD	$ 2,000.00
Travel Insurance[8]	$66.34 + 250 deductible	USD	$ 266.34
	subtotal	USD	$ 6,527.34
Labour Per hour		USD	$ 76.22
Man hours	40 hours	USD	$ 3,048.79
	Total estimate	USD	**$ 9,576.13**

We also looked into approximate M&A consultant and business intelligence consultant rates. A business intelligence consultants estimated cost was USD25 per hour[9] and the M&A advisory for the duration of the integration process was approximately USD500 per day[10].

Our team felt that one week (5 working days) would be sufficient for a decent initial recon of Ya Mon's operations. The primary goal for the team would be to gain as much understanding and insight into Ya Mon's operations as possible. Our engineer's specific goals would be to understand the security maturity of the organization, to understand the security processes, technologies, metrics, standards and policies of Ya Mon, as well as to meet the security team

[4] Cheap flights from San Francisco International to Montego Bay at Skyscanner. (2017, March 1). Retrieved from https://www.skyscanner.com/transport/flights/sfo/mbj/170306/170310/airfares-from-san-francisco-international-to-montego-bay-in-march-2017.html?adult=1&child=0&infant=0&cabinclass=Business&rtn=1&lang=en#results

[5] Booking.com: 1,154,985 hotels worldwide. 114+ million hotel reviews. (2017, March 1). Retrieved from https://www.booking.com/

[6] Jamaica DoD Per Diem Rates for 2017. (2017). Retrieved from https://www.perdiem101.com/oconus/2016/jamaica

[7] A Guide To Kidnap & Ransom Insurance Coverage | Investopedia. (2015, July 29). Retrieved from http://www.investopedia.com/articles/personal-finance/062915/guide-kidnap-ransom-insurance-coverage.asp

[8] Visitors medical Insurance, Visitors Medical Insurance plans, USA Visitors Medical Insurance. (2017, March 1). Retrieved from https://www.americanvisitorinsurance.com/insurance/visitors-medical-summary.asp

[9] Top 10 Osint Freelancers For Hire In March 2017 - Upwork. (2017, March 1). Retrieved from https://www.upwork.com/o/profiles/browse/?q=osint

[10] What are typical due diligence costs that a consulting firm charges for private equity due diligence? - Quora. (2014, October 21). Retrieved from https://www.quora.com/What-are-typical-due-diligence-costs-that-a-consulting-firm-charges-for-private-equity-due-diligence

there (and identify key personnel). Any missing information from the recon could be supplemented by RFI's to Ya Mon (or vice versa) with the primary goal being that we want to gain as much accurate insight as possible about Ya Mon so that we could proceed to the next phase, namely the Pre-Planning stage.

We know from the assignment guidelines that Legal approvals would take six months to completed and our team felt that this time should be for Recon (estimated at one month total time) and Pre-Planning (the remainder of the time until approvals). Given that the Pre-Planning effort would be intensive we decided to allocate two security engineers to Pre-Planning for that period. Given that we are acting primarily as consultants to the overall integration effort, we felt that 30% utilization of our engineers' time would be sufficient. Using the same labor rate as used in the travel cost, we then estimated the cost of allocating two security engineers @ 30% utilization would be USD7317.12.

The Audit Phase, while dependent on the recon and Pre-Planning phase, would take roughly two months to complete. Based on research, on average an internal audit takes three months. One month for planning, one for execution and one for review. Given that we would have already completed the planning portion during Pre-Planning, we felt that two months would be sufficient and cost roughly 0.39 per USD1000 in revenue[11].
Costs and durations for subsequent phases were not able to be estimated with any accuracy and given the professional nature of the report; we felt it best to leave out any guestimates.

4. Final Report

We compiled the CIO report, and the team found that the report did not address all the requirements in the assignment. The cause was related to insufficient information about the target company. As the team has proposed a framework, it was difficult for the team to provide a firm recommendation apart from GIAC completing the reconnaissance and audit phases.

[11] Metric of the Month: Internal Audit Costs. (2015, November 3). Retrieved from http://ww2.cfo.com/auditing/2015/11/metric-month-internal-audit-costs/

We decided to send the draft report to Jason for his perspective. His review mentioned that we needed more technical details in the second half of the CIO report.

After his feedback, one long discussion our team had was whether to include all the potential solutions for integration of various business processes. Being Engineers, we were both drawn to wanting to propose problem/solutions ranging from a “big bang” approach to a parallel system. In the report, however, we felt that the CIO would be more focused on the bigger strategy we were taking vs. the specific solutions to every scenario.

5. Conclusion

Despite the issues encountered during the first iteration of the assignment, the revised implementation addressed the assignment requirements. We delivered a plan for integration, ensured risks were measured against best practices, provided a metric to evaluate the effectiveness of information security measures taken throughout the project and provided short, medium and long-term options for integration tasks.

References

BSI Group. (n.d.). *ISO/IEC 27001:2013 Self-assessment questionnaire.* Retrieved from Standards, Training, Testing, Assessment and Certification | BSI Group:: https://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/ISO-27001-self-assessment-checklist.pdf

BSI Group. (n.d.). *ISO/IEC 27001:2013 Your implementation guide.* Retrieved from Standards, Training, Testing, Assessment and Certification | BSI Group:: https://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/ISO-27001-implementation-guide.pdf

Ieranò, A. (2017, February 15). Email Interview with Antonio Ieranò.

IsecT. (n.d.). *ISO/IEC 27001 certification standard*. Retrieved from ISO27k infosec management standards: http://www.iso27001security.com/html/27001.html

IsecT. (n.d.). *ISO/IEC 27002 code of practice*. Retrieved from ISO27k infosec management standards: http://www.iso27001security.com/html/27002.html

Lam, J. (2017, February 10). M&A Interview with Jason Lam. (A. Shori, & E. Yuwono, Interviewers)

Northcutt, S. (2016, November 10). *Security: Yahoo Verizon Breach Impact on Future M&A*. Retrieved from Stephen Northcutt's blog: https://securitywa.blogspot.com.au/2016/09/yahoo-verizon-breach-impact-on-future-m.html

Northcutt, S. (2017, February 14). personal communication Feb 14.

Northcutt, S. (2017, February 20). personal communication Feb 20.

Northcutt, S. (2017, February 8). personal communication Feb 8.

Pelnekar, C. (n.d.). *Planning for and Implementing ISO 27001*. Retrieved from ISACA: https://www.isaca.org/Journal/archives/2011/Volume-4/Pages/Planning-for-and-Implementing-ISO27001.aspx

Rouse, T., & Frame, T. (2009, November 4). *The 10 steps to successful M&A integration*. Retrieved from Bain & Company: http://www.bain.com/publications/articles/10-steps-to-successful-ma-integration.aspx

Tan, F. (2017, February 17). M&A Interview with Freddy Tan. (A. Shori, Interviewer)

Tok, Y. C. (2017, February 13). M&A Interview with Yee Ching Tok. (A. Shori, Interviewer)

Appendix A: Sample interview questions

Have you done something similar to our assignment in the past? What's your experience with M&A, particularly with the cyber security portion?

1. What kind of industry vertical did the M&A reside in? Do you have any examples from the manufacturing sector?
2. What would be the top things you had to protect for your M&A?
3. Who are the biggest stakeholders during an M&A?
4. In your opinion, from the CIO's perspective (our target audience) what are they likely to be focused on? Is it a step by step plan or would a "these are the key areas to focus on as we go through the acquisition" document be better?
    a. What are the top 5 cybersecurity things you would ensure are included in the plan?
    b. What are the five biggest mistakes you encounter during M&A?
    c. What are some of the things that you might change if you could go back and do it again?
5. From your experience, should the report be more technically oriented or business focused?
    a. Would you suggest the focus be primarily on risk mitigation?
    b. Would the cost be a higher priority?
    c. Would operations be a top priority? (dumb question I know, trying to understand a CIO's priorities hence I had to ask)
6. Would there be any material that you might consider sharing with us?
7. Are there any tools that you would recommend that would be useful for cyber security during M&A?
    a. Have you used the MS threat modeling tool before? Would you recommend we use it?

Appendix B: Security Metric version 1

1. The team brainstormed on assets belonging to the organization (Table B1)
2. The team brainstormed on threats that could have an adverse impact on those assets (Table B1)
3. The team then prioritized these threats into 'Tiers' (Table B1)
4. Each asset also had a risk assigned to it
5. A model WBS was created to demonstrate the tasks required to achieve integration (Table B2)
6. Each threat had a control allocated in the form of a WBS
7. Each WBS would be assigned to an integration subproject as agreed by the business
8. The total duration of the WBS is noted for each subproject
9. We considered tasks that have a duration < day 0 as addressing the security issue assigned to the WBS.

Category	Tier	Countermeasures	WBS
Disgruntled Employees	Tier 1	access controls, awareness training, behavioral analytics, physical security	9.2.1, 9.2.4.2.4, 9.2.4.1.4, 9.2.2.2.3, 9.2.2.1.3, 8.6.2, 5.1.5, 4.4.1.3.1, 4.4.1.3.2
Redundant Employees	Tier 1	access controls, awareness training, behavioral analytics, physical security	9.2.1, 9.2.4.2.4, 9.2.4.1.4, 9.2.2.2.3, 9.2.2.1.3, 8.6.2, 5.1.5, 4.4.1.3.1, 4.4.1.3.2

Table B1

	Operations	**9**
	Processes	**9.1**
	Procurement	**9.1.1**
	Servers	9.1.1.1
	Networks	9.1.1.2
	Workstations	9.1.1.3
	Mobile phones	9.1.1.4
	Licenses	9.1.1.5
	Physical security	**9.2**
	Staff	9.2.1
	Access control	**9.2.2**
	Onboarding	**9.2.2.1**
	Administrators	9.2.2.1.1
	Applications	9.2.2.1.2
	Normal staff	9.2.2.1.3
	Offboarding	**9.2.2.2**
	Administrators	9.2.2.2.1
	Applications	9.2.2.2.2
	Normal staff	9.2.2.2.3
	Support	**9.2.3**
	During Hours	9.2.3.1

Table B2

Appendix C: Security Metric version 2

1. The M&A integration team would collate the integration tasks.
2. The M&A team along with stakeholders would convene to determine the prioritization of the tasks.
3. Once prioritized, the information security team would work with the stakeholder to assess the risks, assign appropriate ISO 27001 controls and actions to the tasks (27001 Mapping).
4. The tasks would be approved and converted into a sub-project (prefixed in Task Name).
5. Assuming no deviations from the plan, the completion of each sub-project would indicate compliance with ISO 27001 shown as green in the RAG status (27001 RAG). Amber or Red would reflect deviations.

Task Name	Duration	Start	Finish	27001 Mapping	27001 Actions	27001 RAG
M&A Integration	1 day?	Fri 24/02/17	Fri 24/02/17			
Finance	1 day?	Fri 24/02/17	Fri 24/02/17			
Reconnaisance	1 day?	Fri 24/02/17	Fri 24/02/17			
Pre Planning	1 day?	Fri 24/02/17	Fri 24/02/17			
Audit	1 day?	Fri 24/02/17	Fri 24/02/17			
Final Planning	1 day?	Fri 24/02/17	Fri 24/02/17			
Implementation	1 day?	Fri 24/02/17	Fri 24/02/17			
Business Critical	1 day?	Fri 24/02/17	Fri 24/02/17			
Subproject: Migrate Financial system 1	1 day?	Fri 24/02/17	Fri 24/02/17			
Establish connectivity	1 day?	Fri 24/02/17	Fri 24/02/17	A6.2.2, A8.1.1, A1	Determine current VPN product, establish encryption standards,...	
Order VPN concentrator for Ya Mon				A15.1.2,...	Determine spec of VPN concentrator, determine 3rd party suppo	
Configure VPN Concentrator				A12.1.1,...	Configure VPN concentrator to GIAC spec, ...	
.						
.						
.						
Migrate data	1 day?	Fri 24/02/17	Fri 24/02/17	A8.3....	Ensure data backups are operational, recent backup available,...	
Subproject: Migrate Financial system 2	1 day?	Fri 24/02/17	Fri 24/02/17			
.						
.						
.						
HR	1 day	Fri 24/02/17	Fri 24/02/17			
Reconnaisance	1 day	Fri 24/02/17	Fri 24/02/17			

Figure C1: Integration plan with information security metrics.