ACME

Center for Internet Cybersecurity Risk Assessment

Implementation Group X

Author Name:	Gern Blanstein
Version #:	Click here to enter text.
Project:	Cybersecurity Risk Assessment & Gap Analysis
Date:	6/1/2021

Legal Disclaimer

VERSION CONTROL

Version	Date	Author	Summary of Changes

TABLE OF CONTENTS

EXECUTIVE OVERVIEW

OneNeck IT Solutions LLC ("OneNeck") recently conducted a security risk assessment for Acme. The objective of the assessment was to determine whether the controls currently in place meet industry best practices, are compliant with corporate policies and regulatory controls, and allow the organization to sufficiently reduce risk to an acceptable level. This report details the information gathered, identifies weaknesses in the areas assessed, identifies areas of noncompliance with mapped frameworks and regulatory requirements, and provides recommendations for improvement.

The purpose of the assessment was to determine a baseline against the Center for Internet Security (CIS) Controls that could then be used for planning, budgeting, and resource allocation to guarantee the availability, confidentiality, and integrity of Acme's services.

Interviews, documentation reviews, and observations were utilized to examine Acme's information assets. OneNeck compiled all of the information obtained from these sources and conducted an in-depth analysis to arrive at the conclusions found in this report.

CIS Controls – Summary

The Center for Internet Security, Inc is a community-driven nonprofit and globally recognized best practices for securing IT systems and data. It is led by a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats.

The CIS Controls (formerly known as Critical Security Controls) version 8 was launched in May 2021. This reduced what was formerly a collection of the Top 20 controls in version 7.1 down to 18 carefully prioritized and well-vetted controls in version 8, each of which is supported by groupings of sub-controls that define security actions that organizations can take to assess and improve their current security state. However, this is not a one-size-fits-all solution in either content or priority. You must still understand what is critical to your business, data, systems, networks, and infrastructures, and you must consider the adversarial actions that could impact your ability to be successful in the business or operation. Even a relatively small number of Controls cannot be executed all at once, so you will need to develop a plan for assessment, implementation, and process management.

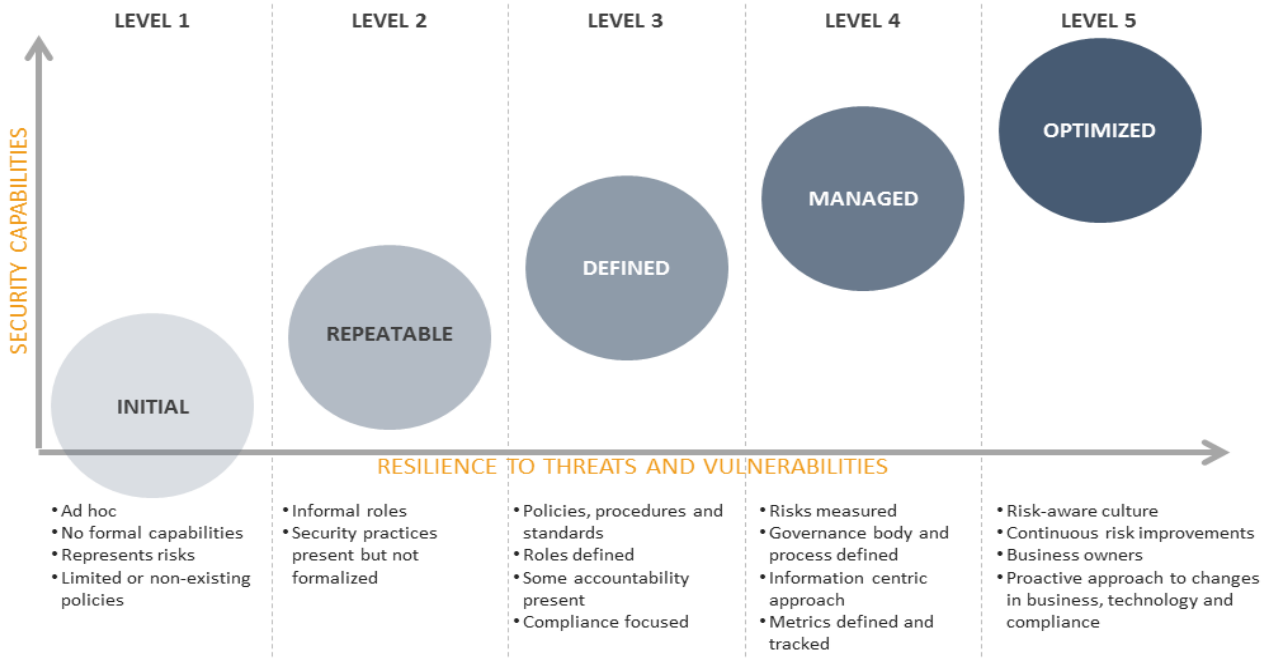
The CIS Controls Implementation Groups (IGs) are self-assessed categories for organizations based on relevant cybersecurity attributes Implementation Groups (IGs) are the recommended guidance to prioritize implementation of the CIS Controls. In an effort to assist enterprises of every size, IGs are divided into three groups. They are based on the risk profile and resources an enterprise has available to them to implement the CIS Controls.

Each IG identifies a set of Safeguards (previously referred to as CIS Sub-Controls), that they need to implement. There is a total of 153 Safeguards in CIS Controls v8.

Appendix A contains additional information about each Implementation Group.

Evaluation Scale (CMMI)

An adaptation of the Capability Maturity Model Integration (CMMI) index is used throughout the assessment report. The assessment is primarily based on a maturity rating from 1 to 5 that coincides with other common approaches for defining the maturity of an organization or specific operations. The idea was to evaluate the Client's effectiveness against an internationally recognized framework using the following scale:



For ease of recording, a numerical value was applied to the rating schema:

0. Nonexistent – Complete lack of recognizable applicable policy, procedure, control, etc.
1. Initial – ad hoc or chaotic state; security relies on the goodwill of employees
2. Repeatable/Limited – intuitive; processes are established, but there is a lack of policy structure
3. Defined – policies are defined, but the program lacks a risk-centric management approach
4. Managed – quantitative risk programs implemented, but lacking in continuous improvement efforts
5. Optimized – mature risk-focused organization with continuous improvement cycles

CIS – Control Overview

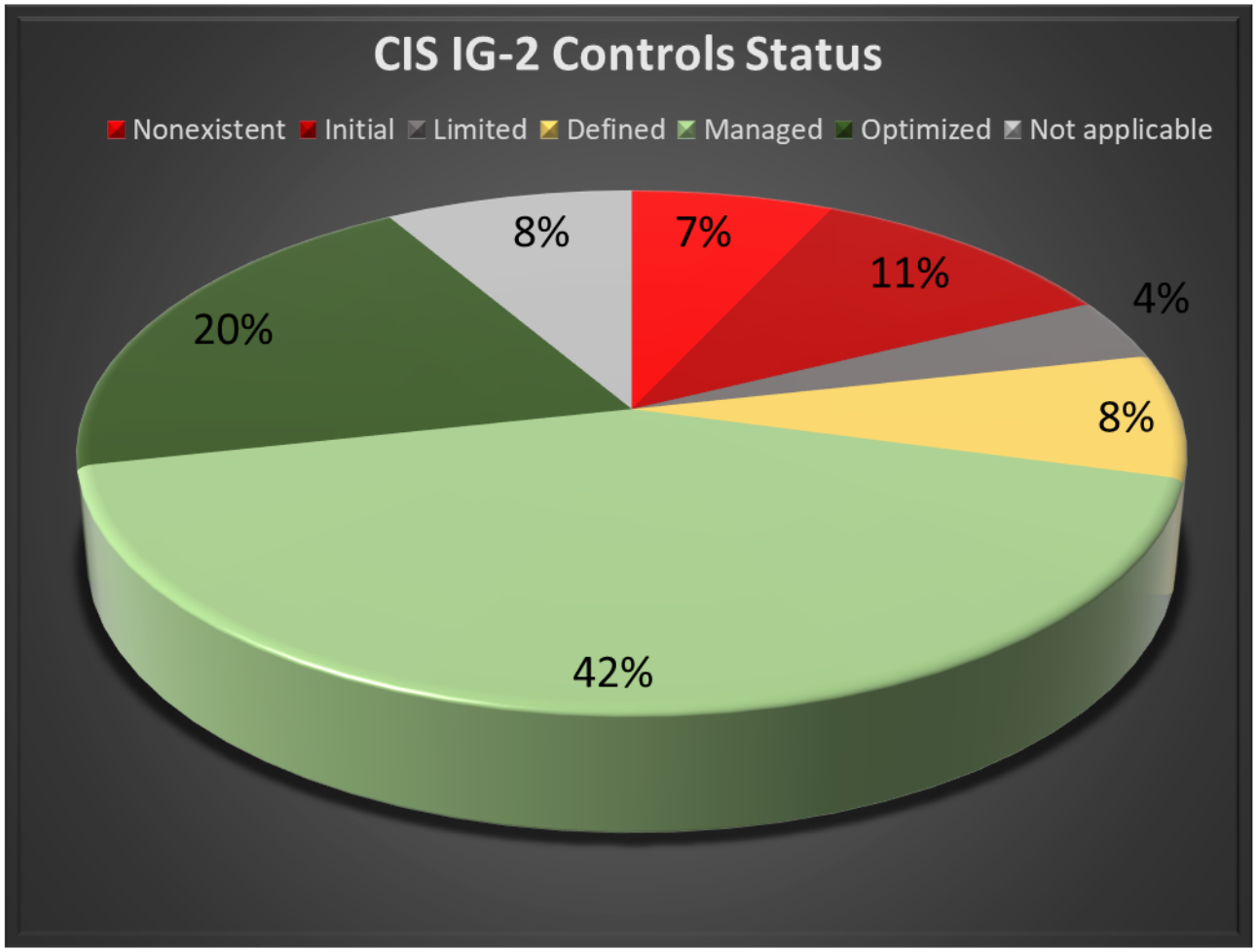
The following table provides an overall view of the controls reviewed and Acme's current Maturity and Risk. Maturity is calculated based on the CMMI index described above. Risk is assessed based on maturity score determined in the assessment, but also includes compensating controls and priority of the control as defined by the CIS Controls, and associated Implementation Group.

	Control	Maturity Score	Risk
CSC-1	Inventory & Control of **Enterprise Assets**	1.50	Medium/ High
CSC-2	Inventory & Control of **Software Assets**	2.67	Medium
CSC-3	**Data Protection**	3.80	Low
CSC-4	**Secure Configuration** of Enterprise Assets & Software	3.44	Medium/ Low
CSC-5	**Account Management**	4.17	Low
CSC-6	**Access Control Management**	4.14	Low
CSC-7	**Continuous Vulnerability Management**	3.00	Medium
CSC-8	**Audit Log Management**	4.25	Low
CSC-9	**Email and Web Browser Protections**	5.00	Low
CSC-10	**Malware Defenses**	4.60	Low
CSC-11	**Data Recovery**	4.00	Low
CSC-12	**Network Infrastructure Management**	3.43	Medium
CSC-13	**Network Monitoring & Defense**	2.50	Medium
CSC-14	**Security Awareness & Skills Training**	4.00	Low
CSC-15	**Service Provider Management**	1.50	Medium/ High
CSC-16	**Application Software Security**	N/A	Low
CSC-17	**Incident Response Management**	1.00	High
CSC-18	**Penetration Testing**	2.33	Low

Score
0 Nonexistant
1 Initial
2 Limited
3 Defined
4 Managed
5 Optimized

The following pie chart provides an overview of Acme's current Maturity.

- Nonexistent – Complete lack of recognizable applicable policy, procedure, control, etc.
- Initial – ad hoc or chaotic state; security relies on the goodwill of employees
- Repeatable/Limited – intuitive; processes are established, but there is a lack of policy structure
- Defined – policies are defined, but the program lacks a risk-centric management approach
- Managed – quantitative risk programs implemented, but lacking in continuous improvement efforts
- Optimized – mature risk-focused organization with continuous improvement cycles



Determining Priorities

In determining the priorities of remediating the risk in your environment it is important to consider:

- The three Implementation Groups (IGs) provide a roadmap for prioritizing implementation of the CIS Controls. Implementation Group 1 (IG1) represents a baseline, or minimum standard of security that can be considered as "basic cyber hygiene" for all enterprises, no matter their size or scope of business. IG2 and IG3 sequentially build upon the foundation of IG1.
- IT environments can be very expansive, and implementing strong security controls requires investments in people, process, and tools. Therefore, it's recommended to understand what the critical data (sensitive/regulated) and services (mission critical) are for your business and ensure those areas are segmented and have the most security possible.
- The right toolsets, combined with the necessary skill sets are critical not only for actively managing operational security, but also for ensuring continuous insight and timely alerting keep you constantly informed about the state of security in your environment. Our recommendations may include options for new tools and technologies that could require investment, but we will also look for opportunities to better leverage tools and resources that already exist in your environment.
- Cyber-attacks happen around the clock and the bad actors behind them often prefer late night hours and holidays. When making any investment in a security tool make sure you have the processes and people required to run the tool and respond whenever necessary, and the proper support in place to ensure your tool always performs to expectations.
- Be opportunistic:
    - If you have an active project try to consider what controls you could start implementing as part of the project for example establishing a standard and secure configuration, ensuring access to the new system/service requires Multi-Factor Authentication (MFA), or that you have appropriate logging and monitoring to ensure the security and availability of the server/service.
    - If you have an investment in a tool, make sure you maximize its usage by knowing/using the features that it provides.
- Importance of policies & procedures:
    - Policies and procedures are essential for all businesses but are often looked at as a rulebook full of restrictions. Create your library of policies and procedures so that it functions more as an encyclopedia or knowledge repository. Keep your policies simple but focused. Clearly explain the policy's position but save the 'how-to' information for a supporting procedure document. Procedures should be written with enough detail to serve as a reference manual to ensure business operations can run efficiently even in situations such as unexpected staffing changes.
    - Review all your policies and procedures annually at minimum to keep them current and store them in a globally accessible centralized repository. Because policy topics can sometimes overlap, it is important to ensure you are delivering the same message consistently in all documents wherever that message is used.
    - Incorporate policies into company culture and demonstrate management support through frequent socialization activities (e.g., periodic security awareness bulletins, anti-phishing drills, etc.). Balance policies so that security concerns are properly addressed, but in the least restrictive manner possible by looking for compensating controls that promote operational efficiency without compromising security.

Recommended Priorities

As determined from the assessment there are areas that have been determined to have a higher risk in your environment due to current abilities in those areas, which includes:

#15 SERVICE PROVIDER MANAGEMENT

Maturity: 1.00 **Risk: High**

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Existing Environment
Example Findings may be: Vendor information is collected and stored, however, there is not a policy or process that offers guidance to how this is done. All actions are manual and ad-hoc. Vendor information can be found in several location across different technology solutions.

Action to Improve
Suggested Improvements may be: Implement a vendor risk classification system based on characteristics such as data sensitivity handling, data volume, availability, regulatory concerns, and other relevant areas critical to the enterprise's security posture.

#3 DATA PROTECTION

Maturity: 1.50 **Risk: Medium/High**

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Existing Environment
Example Findings may be: Data is not classified, or segmented. There is no policy documentation to support this control.

Action to Improve
Suggested Improvements may be: Develop a Data Encryption policy based on industry standards that defines requirements for encryption of data in transit and at rest, and document encrypted data flows by classification.

#17 INCIDENT RESPONSE MANAGEMENT

Maturity: 1.50 **Risk: Medium/High**

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Existing Environment

Example Findings may be: A formal incident response plan does not exist. Incidents are handled reactively. There is not a communication plan in place. Communications are done ad-hoc as needed using internal knowledge of who may be needed to help resolve any issues.

Action to Improve

Suggested Improvements may be: Formalize an incident reporting policy/process that will capture all the relevant information including incident details, response and escalation activities, and remediation plans/outcomes.

End of Executive Summary

CIS CATEGORY OBSERVATIONS AND RECOMMENDATIONS

In the following section, each category of the CIS Controls is given a rating based on the interviews and analysis conducted during the assessment. Each cell begins with a high-level description of the category followed by a summary of the current state of the observed environmental conditions that directly impact the organization's ability to align with the category and satisfy the requirements of each Sub-Control.

#	Control Review	Rating
1	**INVENTORY & CONTROL OF ENTERPRISE ASSETS** Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate. **Existing Environment** *Fairly robust management of hardware asset inventory. The ability to quickly identify current assets exists through actively implemented technologies. However, there is a lack of documentation around policy.* **Action to Improve** *Develop and publish a policy that provides guidelines and requirements for the inventory and control of enterprise assets.*	4.00

INVENTORY & CONTROL OF SOFTWARE ASSETS

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Existing Environment

2

Technology exists in the environment that will allow for the inventory of installed software and OS's. However, the technology is not being leveraged to it's full potential and does not encompass all devices, leading to an inaccurate listing of installed software.

1.83

Action to Improve

Expand tool use to leverage their full potential (e.g., by performing recurring scans to report on all existing OS/software installations within the environment) and document in a policy.

DATA PROTECTION

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Existing Environment

3

<Finding>

3.80

Action to Improve

<Improvement>

SECURE CONFIGURATION OF ENTERPRISE ASSETS & SOFTWARE

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

Existing Environment

4 <Finding> 3.44

Action to Improve

<Improvement>

ACCOUNT MANAGEMENT

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

Existing Environment

<Finding>

5 4.17

Action to Improve

<Improvement>

6 ACCESS CONTROL MANAGEMENT

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

Existing Environment

<Finding>

4.14

Action to Improve

<Improvement>

7 CONTINUOUS VULNERABILITY MANAGEMENT

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Existing Environment

<Finding>

3.00

Action to Improve

<Improvement>

AUDIT LOG MANAGEMENT

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

Existing Environment

8 <Finding> 4.25

Action to Improve

<Improvement>

EMAIL & WEB BROWSER PROTECTIONS

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

Existing Environment

9 <Finding> 5.00

Action to Improve

<Improvement>

MALWARE DEFENSES

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Existing Environment

10 <Finding> 4.60

Action to Improve

<Improvement>

DATA RECOVERY

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

Existing Environment

11 <Finding> 4.00

Action to Improve

<Improvement>

NETWORK INFRASTRUCTURE MANAGEMENT

Establish, implement, and actively manage (track, report, correct) network devices, to prevent attackers from exploiting vulnerable network services and access points.

Existing Environment

<Finding>

12 3.43

Action to Improve

<Improvement>

NETWORK MONITORING & DEFENSE

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

Existing Environment

13

There are several efforts being undertaken to improve the network defense infrastructure. There is a lack of Network Intrusion Detection Systems (NIDS) and network segmentation.

2.50

Action to Improve

<Improvement>

SECURITY AWARENESS & SKILLS TRAINING

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

Existing Environment

14

<Finding>

4.00

Action to Improve

<Improvement>

SERVICE PROVIDER MANAGEMENT

Develop a process to evaluate service providers who hold sensitive data or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

15	**Existing Environment** <Finding> **Action to Improve** <Improvement>	1.50

APPLICATION SOFTWARE SECURITY

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

16	**Existing Environment** <Finding> **Action to Improve** <Improvement>	N/A

INCIDENT RESPONSE MANAGEMENT

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Existing Environment

17

<Finding>

1.00

Action to Improve

<Improvement>

PENETRATION TESTING

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

Existing Environment

18

<Finding>

2.33

Action to Improve

<Improvement>

APPENDIX A: CIS IMPLEMENTATION GROUPS

Implementation Group 1:

Implementation Groups (IGs) are the recommended guidance to prioritize implementation of the CIS Controls. CIS Controls v8 defines Implementation Group 1 (IG1) as basic cyber hygiene and represents an emerging minimum standard of information security for all enterprises. IG1 is the on ramp to the CIS Controls and consists of a foundational set of 56 cyber defense Safeguards. The Safeguards included in IG1 are what every enterprise should apply to defend against the most common attacks.

In most cases, an IG1 enterprise is typically small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. A common concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime.

The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information. Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.

Implementation Group 2:

IG2 is comprised 74 additional Safeguards and builds upon the 56 Safeguards identified in IG1.

The 74 Safeguards selected for IG2 can help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.

An IG2 enterprise employs individual who are responsible for managing and protecting IT infrastructure. These enterprises typically support multiple departments with differing risk profiles based on job function and mission. Small enterprise units may have regulatory compliance burdens. IG2 enterprises often store and process sensitive client or enterprise information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs.

Implementation Group 3:

IG3 is comprised of an additional 23 Safeguards. It builds upon the Safeguards identified in IG1 (56) and IG2 (74) totaling the 153 Safeguards in CIS Controls v8.

An IG3 enterprise commonly employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare.

Safeguards selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

APPENDIX B: CIS CONTROLS & SUB-CONTROLS DETAILS

See provided XLS