Kudler security report

Law, Security

Kudler Fine Foods IT Security Report and Presentation Security Considerations CMGT/400 Kudler Fine Foods IT Security Report and Presentation Security Considerations According to Whitman and Mattord (2010), The ISO 27000 series is one of the most widely referenced security models.

Referencing ISO/IEC 27002 (17799: 2005), the major process steps include: risk assessment and treatment, security policy, organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development, and maintenance, information security incident management, business continuity management, and compliance (Chapter 10, Security Management Models). 1.

Risk assessment and treatment 2. Security policy: Focuses mainly on information security policy 3. Organization of information security: For both the internal organization and external parties 4. Asset management: Includesresponsibilityfor assets and information classification 5. Human resources security: Ranges from controls prior to employment and during employment to termination or change of employment 6. Physical and environmental security: Includes secure areas and equipment security 7.

Communications and operations management: Incorporates operational procedures and responsibilities, third-party service delivery management, systems palnning and acceptance, protection against malicious and mobile code, backup, network security management, media handling, exchange of information, electronic commerce services and monitoring 8. Access control:

Focuses on business requirement for access control, user access management, user responsibilities, network access control, operating system access control, application and information access control, and mobile computing and teleworking 9.

Information systems acquisition, development, and maintenance: Includes security requirements of information systems, correct processing in applications, cryptographic controls, security of system files, security in development and support processes, and technical vulnerability management 10. Information security incident management: Addresses reporting information security events and weaknesses and management of information security incidents and improvements 11.

Business continuity management: Information security aspects of business continuity management 12. Compliance: Includes compliance with legal requirements, compliance with security policies and standards, and technical compliance and information systems audit considerations The “ SANS: SCORE” (2012) website provides a free audit checklist for organizations to verify if they comply with the ISO 27002. The following table represents the SANS audit checklist as it relates to Kudler FineFood’s frequent buyer program. Security policy: Focuses mainly on information security policy | | Section | Audit Question | Security Considerations | Security concern if | Mitigation | | | | | removed | | | Information security policy| Whether there exists an Information | A security policy is | Without a security policy | Define what needs to be | | document | security policy, which is approved by the | necessary to guide all | in place the restriction | protected in order to | | | management, published and communicated as | access or to block | of

information would be | develop a security policy. | | | appropriate to all employees. | access to information. | lost.

Uncontrolled access| The importance of the | | | | will result in the loss of| information should | | | Whether the policy states management | | company information. | determine the severity of | | | commitment and sets out the organizational| | | the security. | | | approach to managing information security. | | | | | Review of Informational | Whether the

Information Security Policy is| The security policy | Without the review of | Each policy should be | | Security Policy | reviewed at planned intervals, or if | should be reviewed as | security policies they | reviewed periodically to | | | significant changes occur to ensure its | business practices, | will most likely become | ensure its effectiveness. | | | continuing suitability, adequacy and | hardware, software, and | out dated and lose | | | | effectiveness. | the way in which | usefulness. Each policy owner will be | | | | information is shared | | responsible for the review | | | Whether the Information Security policy | change. | Without giving each | of the policy. | | | has an owner, who has approved management | | section of the policy an | | | | responsibility for development, review and| Each part of the policy | owner the policy will have| Each change will be brought| | | evaluation of the security policy. should have an owner who| no one responsible for its| before management before | | | | is responsible for | maintenance. | being brought into action. | | | Whether any defined Information Security | keeping it up to date. | | | | | Policy review procedures exist and do they| | A policy to review new | | | | include requirements for the management | A review procedure | policies or changes made | | | | review. should be in place, each| to current policies

should| | | | change made should be | be in place to discourage | | | | Whether the results of the management | reviewed by management. | unauthorized changes. | | | review are | | | | | taken into account. | | | | | | Whether management approval is obtained | | | | | for the revised policy. | | | | Organization of Information Security | | Section | Audit Question | Security | Security concern if | Mitigation | | | | Considerations | removed | | | Management commitment to| Whether management demonstrates active support for | An active role | Without the active support| A definition of the role | | information security | security measures within the organization.

This can be| by management | of management the security| management should play in | | | done via clear direction, demonstrated commitment, | is needed to | policy will lose its | the commitment to the | | | explicit assignment and acknowledgement of information| ensure the | effectiveness. | security policy should be | | | security responsibilities. | effectiveness | | stated in the security | | | | of the security| | policy. | | | | policy. | | | Information security | Whether information security activities are | Security | Information security | Ensure that the owner of | | coordination | coordinated by representatives from diverse parts of | activities need| activities need to be | each policy is responsible | | | the organization, with pertinent roles and | to be | organized by employees | for all activities | | | responsibilities. | coordinated by | with higher roles and | associated with the | | | | representatives| responsibilities. The | policies. | | | that carry | security policies protect | | | | | pertinent roles| the information and all | | | | | and | activities associated with| | | | responsibilitie| the security policy should| | | | s. | be made by responsible | | | | | parties. | | Allocation of | Whether

responsibilities for the protection of | The business | Without a clear set of | A clear set of instructions| | information security | individual assets, and for carrying out specific | will suffer a | rules governing the | will be provided to ensure | | responsibilities | security processes, were clearly identified and | great many | protection of individual | that each individual asset | | | defined. | losses due to | assets and security | and each security process | | | | unclear | processes the business | is clearly defined. | | | detentions of | will surely suffer a loss. | | | | | procedures. | | | | Authorization process | Whether management authorization process is defined | Authorization | Without the use of an | Any and all information | | for information | and implemented for any new information processing | processes need | authorization system a new| processing facilities need | | processing facilities | facility within the organization. to be clearly | information processing | to be given ownership to a | | | | stated in the | facility would be left | member of management. This| | | | security | vulnerable for attack. | member needs to ensure the | | | | policy. Any | | security policy is | | | | new information| | followed.

Using the proper| | | | processing | | authorization system is | | | | facility needs | | critical to securing the | | | | to have an | | information contained | | | | authorization | | within. | | | | process | | | | | | implemented. | | | Confidentiality | Whether the organization’s need for Confidentiality or| The NDA should | Without the use of an NDA | The NDA needs to be | | agreements | Non-Disclosure Agreement (NDA) for protection of | be clearly | the legal ramifications | reviewed periodically to | | | information is clearly defined and regularly reviewed. | defined. This | are greatly lessened. A | ensure that any changes in | | | will help to | business needs to protect | the

business are reflected | | | Does this address the requirement to protect the | ensure the | its data to the fullest | in it. | | | confidential information using legal enforceable terms| information is | extent of the law. | | | | not | | | | | | compromised. | | | | Contact with authorities| Whether there exists a procedure that describes when, | This is | The time it takes to act | A plan must be in place for| | | and by whom: relevant authorities such as Law | important to | in an emergency is crucial| different types of | | | enforcement, fire department etc. should be | the physical | to keeping employees and | emergencies involving any | | | contacted, and how the incident should be reported. | security of the| the business safe. A plan| outside authorities. This | | | | business and | must be in place to avoid | can help to prevent | | | | the employee | potential losses due to | injuries and harm done to | | | | within. | unforeseen events. | employees and the business. | Contact with special | Whether appropriate contacts with special interest | Contacts with | Allowing a third party | A policy needs to define | | interest groups | groups or other specialist security forums, and | third party | group access to any | the steps needed to apply | | | professional associations are maintained | groups need to | information can be a risk | for special interest groups| | | | be approved my | to the business. All | and how the relationship is| | | | management. third party associations | maintained. | | | | | should be approved in | | | | | | advance by management. | | | Independent review of | Whether the organization’s approach to managing | Security | The loss of strength to | To ensure the highest level| | information security | information security, and its implementation, is | management | the security of | of security a review should| | reviewed independently at planned intervals, or when | should be |

information can occur | be implemented periodically| | | major changes to security implementation occur. | reviewed at | through time (small | and whenever a major change| | | | planned | changes) or when a major | takes place. | | | | intervals and | change has taken place. | | | | | when major | | | | | | changes occur. | | | Identification of risks | Whether risks to the organization’s information and | Allowing third | Allowing third parties | Strict rules and an access | | related to external | information processing facility, from a process | parties access | access to the business | policy must be implemented | | parties | involving external party access, is identified and | to the network | network and the contents | to allow a third party | | | appropriate control measures implemented before | poses serious | of the business systems | access to any information | | | granting access. | risks to the | poses a serious threat to | in the business. | | | | integrity of | the integrity of the | | | | | the | system. | | | | information. | | | | Addressing security when| Whether all identified security requirements are | Allowing | Allowing customers access | Access to information by | | dealing with customers | fulfilled before granting customer access to the | customers with | to information in the | customers should be stated | | | organization’s information or assets. | the access to | business system poses a | in the security policy. | | | | certain | threat. Customers should only be | | | | information can| | allowed access to minimal | | | | help to | | information, a separate | | | | increase | | website or informational | | | | customer base | | address. | | | | and customer | | | | | | awareness. | | | Addressing Security in | Whether the agreement with third parties, involving | All third party| Agreeing with a third | Any third party contract | | third party agreements |

accessing, processing, communicating or managing the | agreements | party contract can hold | should be reviewed by the | | | organization’s information or information processing | should be | some legal ramifications. | legal department to ensure | | | facility, or introducing products or services to | reviewed before| | the contract agrees with | | | information processing facility, complies with all | implementation. | | all of the businesses | | | appropriate security requirements | | | security requirements. | Asset Management | | | | Section | Audit Question | Security Considerations | Security concern if | Mitigation | | | | | removed | | | Inventory of Assets | Whether all assets are identified and an | The businesses assets | Without a clear definition| Each new asset will be | | | inventory or register is maintained with | need to be registered to| of assets the business | registered and assigned an | | | all the important assets. | ensure their safety. | could suffer a loss or | owner. | | | | theft of assets. | | | Ownership of Assets | Whether each asset identified has an | The security policy must| The business could suffer | Each new asset should have | | | owner, a defined and agreed-upon security | include clearly defined | a loss without giving the | an owner and restrictions | | | classification, and access restrictions | parameters for | asset an owner and | to its access. | | | that are periodically reviewed. | registering assets. defining access | | | | | | restrictions. | | | Acceptable use of Assets | Whether regulations for acceptable use of | Legal issues and profits| Without regulations on the| Defineing all acceptable | | | information and assets associated with an | losses could occur from | use of assets the company | uses of business assets is | | | information processing facility were | the misuse of assets. | could suffer losses and | crucial. | | | identified,

documented and implemented | | legal issues. | | Classification guidelines | Whether the information is classified in | Classification of | By classifying information| All information should be | | | terms of its value, legal requirements, | information is crucial | is can be easier to | classified in terms of its | | | sensitivity and criticality to the | to the business. This | determine who has access | value, legal requirements, | | | organization. | will determine who has | to it. | and sensitivity to ensure | | | | access to the | | it is only accessible to | | | | information. | authorized users. | | Information Labeling and | Whether an appropriate set of procedures | A set of organizational | Unorganized information | All information should be | | handling | are defined for information labeling and | parameters should be | can result in the loss of | organized within a set of | | | handling, in accordance with the | devised to create a | the information. | parameters defined in the | | | classification scheme adopted by the | classification scheme. | | classification scheme. | | | organization. | | | | Human Resources Security | | Section | Audit Question | Security Considerations | Security concern if | Mitigation | | | | removed | | | Roles and responsibilities | Whether employee security roles and | All personnel authorized| Unauthorized access of | All confidential | | | responsibilities, contractors and third | to access confidential | this information could | information should be | | | party users were defined and documented in| information needs to be | result in identity theft. | handled by authorized | | | accordance with the organization’s | identified by management| | personnel only. | | information security policy. | team. | | | | | | | | | | Were the roles and responsibilities | | | | | defined and clearly communicated to job | | | | | candidates during the pre-employment | | | | |

process | | | | Screening | Whether background verification checks for| All applicants | If not performed, persons | All employees should be | | | all candidates for employment, | considered for | with a history of theft | free of any criminal | | | contractors, and third party users were | employment have to | could be hired. | history that may cause | | | carried out in accordance to the relevant | undergo a criminal | | concern to the company. | | | regulations. | background check prior | | | | | to a job offer being | | | | | Does the check include character | made. | | | | reference, confirmation of claimed | | | | | | academicand professional qualifications | | | | | | and independent identity checks | | | | | Terms and conditions of | Whether employee, contractors and third | Management must define | Unauthorized access of | To prevent confidential | | employment | party users are asked to sign | what information is | this information could be | information to be disclosed| | | confidentiality or non-disclosure | confidential in | used for personal use. | to unauthorized persons. | | | agreement as a part of their initial terms| accordance to existing | | | | | and conditions of the employment contract. | laws and company policy. | | | | | | | | | Whether this agreement overs the | | | | | information security responsibility of the| | | | | | organization and the employee, third party| | | | | | users and contractors. | | | | | Management responsibilities| Whether the management requires employees,| Management must define | Unauthorized access could | To prevent confidential | | | contractors and third party users to apply| which users have to have| be used for personal gain. | information to be disclosed| | | security in accordance with the | this access. | | to unauthorized persons. | | established policies and procedures of the| | | | | | organization. | | | | |

Information security | Whether all employees in the organization,| Management and Loss | Private information could | To educate all personal | | awareness, educationand | and where relevant, contractors and third | Prevention must develop | be disclosed to | about privacy policy. | | training | party users, receive appropriate security | a training program and | unauthorized persons for | | | | awareness training and regular updates in | establish how often it | personal use. | | | organizational policies and procedures as | needs to be | | | | it pertains to their job function. | administered. | | | | Disciplinary process | Whether there is a formal disciplinary | Management must | Private information could | To advise employees what | | | process for the employees who have | establish corrective | be disclosed to | recourse their actions will| | | committed a security breach. | action measures if there| unauthorized persons for | have. | | | | | is a security breach. | personal use. | | Termination | Whether responsibilities for performing | Management must advise | If an employee was not | To define the procedures of| | responsibilities | employment termination, or change of | what actions will | properly terminated could | terminating employment. | | | employment, are clearly defined and | terminate employment and| result in a lawsuit. | | | | assigned | what procedures are | | | | | involved in the | | | | | termination process. | | | Return of assets | Whether there is a process in place that | Management must define | If not returned, certain | To ensure that all | | | ensures all employees, contractors and | what materials employees| company items could be | appropriate company | | | third party users surrender all of the | must return upon | used for personal use. | materials are returned. | | |

organization’s assets in their possession | employment. | | | | | upon termination of their employment, | | | | | | contract or agreement. | | | | Removal of access rights | Whether access rights of all employees, | Management will define a| If not defined, it is | To prevent unauthorized | | | contractors and third party users, to | timeframe in which a | possible that a terminated| personnel from accessing | | | information and information processing | terminate employee | employee could still | company information. | | | facilities, will be removed upon | access is removed | access company | | | | termination of their employment, contract | | information. | | | | or agreement, or will be adjusted upon | | | | | | change. | | | | Physical and Environmental Security | | Section | Audit Question | Security Considerations | Security concern if | Mitigation | | | | | removed | | | Physical security perimeter| Whether a physical border security | | | | | | facility has been implemented to protect | | | | | | the information processing service. | | | | | | | | | | | | Some examples of such security facilities | | | | | | are card control entry gates, walls, | | | | | | manned reception, etc. | | | | Physical entry controls | Whether entry controls are in place to | Physical access to | potential for security | server room should be | | | allow only authorized personnel into | system | breach through | locked with access | | | various areas within the organization. | | unauthorized access to | restricted to authorized | | | | | physical equipment. | personnel.

Sophistication | | | | | | of restraint would be | | | | | | dependent upon importance | | | | | | of information and budget. | | Securing offices, rooms, | Whether the rooms, which have the | | | | | and facilities | information processing service, are locked| | | | | | or have lockable cabinets or safes. | | |

| Protecting against external| Whether the physical protection against | corruption and/or loss | loss of critical data. | Data and system redundancy,| | and environmental threats | damage from fire, flood, earthquake, | of information due to | | off-site storage and/or | | | explosion, civil unrest and other forms of| environmental conditions| | multiple servers at | | | natural or man-made disaster should be | | | different locations. | | | designed and applied. | | | | | | | | | | Whether there is any potential threat from| | | | | | neighboring premises. | | | | | Working in secure areas | Whether physical protection and guidelines| | | | | for working in secure areas is designed | | | | | | and implemented. | | | | | Public access delivery and Whether the delivery, loading, and other | | | | | loading areas | areas where unauthorized persons may enter| | | | | | the premises are controlled, and | | | | | | information processing facilities are | | | | | | isolated, to avoid unauthorized access | | | | | Equipment sitting | Whether the equipment is protected to | | | | | protection | reduce the risks from environmental | | | | | | threats and hazards, and opportunities for| | | | | | unauthorized access | | | | | Supporting utilities | Whether the equipment is protected from | | | | | | power failures and other disruptions | | | | | | caused by failures in supporting | | | | | | utilities. | | | | | | | | | | | | Whether permanence of power supplies, such| | | | | | as a multiple feed, an Uninterruptible | | | | | | Power Supply (ups), a backup generator, | | | | | | etc. are being utilized. | | | | | Cabling security | Whether the power and telecommunications | | | | | | cable, carrying data or supporting | | | | | | information services, is protected from | | | | | | interception or damage. | | | | | | | | | | | | | | Whether there are any additional security | | | | | | controls in place for sensitive or | | | | | | critical information. | | | | | Equipment Maintenance |

Whether the equipment is correctly | | | | | maintained to ensure its continued | | | | | availability and integrity. | | | | | | | | | | Whether the equipment is maintained, as | | | | | per the supplier’s recommended service | | | | | | intervals and specifications. | | | | | | | | | | Whether the maintenance is carried out | | | | | only by authorized personnel. | | | | | | | | | | Whether logs are maintained with all | | | | | suspected or actual faults and all | | | | | preventive and corrective measures. | | | | | | | | | | Whether appropriate controls are | | | | | implemented while sending equipment off | | | | | premises. | | | | | | | | | | Are the equipment covered by insurance and| | | | | the insurance requirements satisfied | | | | | Securing of equipment | Whether risks were assessed with regards | off-site data storage | off-site data may be | proper security measures in| | off-premises | to any equipment usage outside an | centers provide a level | compromised or otherwise | place to ensure integrity | | | organization’s premises, and mitigation | of redundancy to | corrupted due to | of data. | | | controls implemented. maintain integrity in | insufficient security | | | | the event of a local | measures | | | | Whether the usage of an information | breach | | | | processing facility outside the | | | | | organization has been authorized by the | | | | | | management. | | | | Secure disposal or re-use | Whether all equipment, containing storage | | | | of equipment | media, is checked to ensure that any | | | | | sensitive information or licensed software| | | | | is physically destroyed, or securely | | | | | | over-written, prior to disposal or reuse. | | | | | Removal of property | Whether any controls are in place so that | | | | | | equipment, information and software is not| | | | | taken off-site without prior | | | | | | authorization. | | | | Communications and Operations

Management | | Section | Audit Question | Security Considerations | Security concern if | Mitigation | | | | | removed | | | Documented Operation | Whether the operating procedure is | Management should set | Without direction, | To establish how the | | Procedures | documented, maintained and available to | guideline about how each| employees would not know | company is to operate on a | | | all users who need it. | function should operate | what to do throughout the | daily basis. | | | | in the company. | day. | | | Whether such procedures are treated as | | | | | | formal documents, and therefore any | | | | | changes made need management | | | | | authorization. | | | | | Change Management | Whether all changes to information | | | | | processing facilities and systems are | | | | | | controlled. | | | | Segregation of duties | Whether duties and areas of responsibility| Management is | No one would be | To establishaccountability| | | are separated, in order to reduce | responsible for | responsible for ensuring | for task performed in each | | | opportunities for unauthorized | assigning area of | tasks are completed. | area. | | | modification or misuse of information, or | responsibility. | | | | | services. | | | | Separation of development, | Whether the development and testing | Management needs to | Incorrect information | To prevent incorrect | | test, and operational | facilities are isolated from operational | establish a separate | could cause a delay in | information is not given to| | facilities | facilities. For example, development and | network. | production or development. | incorrect personnel. | | | production software should be run on | | | | | | different computers.

Where necessary, | | | | | development and production networks should| | | | | be kept separate from each other. | | | | | Service delivery | Whether

measures are taken to ensure that | Define what measures are| Goods and services will | To ensure that service | | | the security controls, service definitions| needed and establish who| not be done in a timely | level is established and | | | and delivery levels, included in the third| to monitor. | manner. | maintained. | | party service delivery agreement, are | | | | | | implemented, operated and maintained by a | | | | | | third party | | | | | Monitoring and review of | Whether the services, reports and records | Define what measures are| Goods and services will | To ensure that service | | third party services | provided by third party are regularly | needed and establish who| not be done in a timely | level is established and | | | monitored and reviewed. | to monitor. | manner. | maintained. | | | | | | | Whether audits are conducted on the above | | | | | third party services, reports and records,| | | | | | on regular interval. | | | | | Managing changes to third | Whether changes to provision of services, | Define what measures are| Goods and services will | To ensure that service | | party services | including maintaining and improving | needed and establish who| not be done in a timely | level is established and | | | existing information security policies, | to monitor. | manner. | maintained. | | | procedures and controls, are managed. | | | | | | | | | | Does this take into account criticality of| | | | | business systems, processes involved and | | | | | | re-assessment of risks | | | | | Capacity management | Whether the capacity demands are monitored| Management must decide | Systems will not be able | To establish who will | | | and projections of future capacity | if a third party will be| to process information | monitor computer systems. | | | requirements are made, to ensure that | needed to assist with | needed in a timely manner. | | | adequate processing

power and storage are | their IT needs. | | | | available. | | | | | | | | | | Example: Monitoring hard disk space, RAM | | | | | and CPU on critical servers. | | | | System acceptance | Whether system acceptance criteria are | Management must decide | Systems will not be able | To establish who will | | | established for new information systems, | if a third party will be| to process information | monitor computer systems. | | | upgrades and new versions. | needed to assist with | needed in a timely manner. | | | | their IT needs. | | | | Whether suitable tests were carried out | | | | | prior to acceptance | | | | Controls against malicious | Whether detection, prevention and recovery| IT personnel must ensure| Unauthorized access could | Establish measures to | | code | controls, to protect against malicious | proper measures are in | lead to system shut down. | protect from virus and | | | code and appropriate user awareness | place. | | malware. | | | procedures, were developed and | | | | | implemented. | | | | | Controls against mobile | Whether only authorized mobile code is | | | | | code | used. | | | | | | | | | | Whether the configuration ensures that | | | | | authorized mobile code operates according | | | | | to security policy. | | | | | | | | | | Whether execution of unauthorized mobile | | | | | code is prevented. | | | | | | | | | | (Mobile code is software code that | | | | | transfers from one computer to another | | | | | | computer and then executes automatically. | | | | | | It performs a specific function with | | | | | little or no user intervention. Mobile | | | | | | code is associated with a number of | | | | | middleware services. | | | | | Information backup | Whether back-ups of information and | IT personnel will ensure| If not properly manage | To establish back up and | | | software is taken and tested regularly in | that system is properly | could result in loss of

| recover of data procedures. | | | accordance with the agreed backup policy. | working. | data. | | | | | | | | | Whether all essential information and | | | | | | software can be recovered following a | | | | | disaster or mediafailure. | | | | Network Controls | Whether the network is adequately managed | IT personnel must ensure| Unauthorized access could | Establish measures to | | | and controlled, to protect from threats, | proper measures are in | lead to system shut down. | protect from virus and | | | and to maintain security for the systems | place. | | malware. | | | and applications using the network, | | | | | | including the information in transit. | | | | | | | | | Whether controls were implemented to | | | | | | ensure the security of the information in | | | | | networks, and the protection of the | | | | | | connected services from threats, such as | | | | | | unauthorized access. | | | | Security of network | Whether security features, service levels | IT/Third party will | The company may not be | To establish what security | | services | and management requirements, of all | advise management the | aware of what is needed to| features of needed to | | | network services, are identified and | necessary requirements | secure the network and the| maintain the network. | | | included in any network services | needed for the network. | system is broken into | | | | agreement. | | compromising information. | | | | | | | | Whether the ability of the network service|