

Fraud management system and cyber security

Verona, 22 Febbraio 2018

Giuseppe Puleo: Senior Security and Privacy Consultant



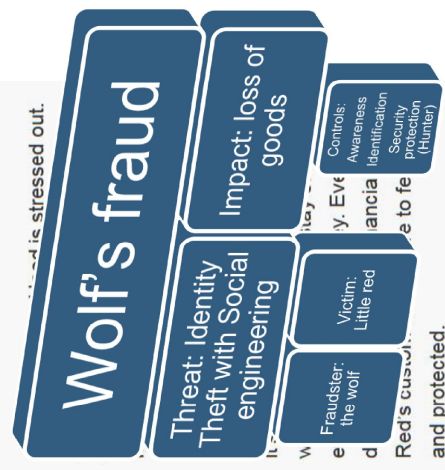
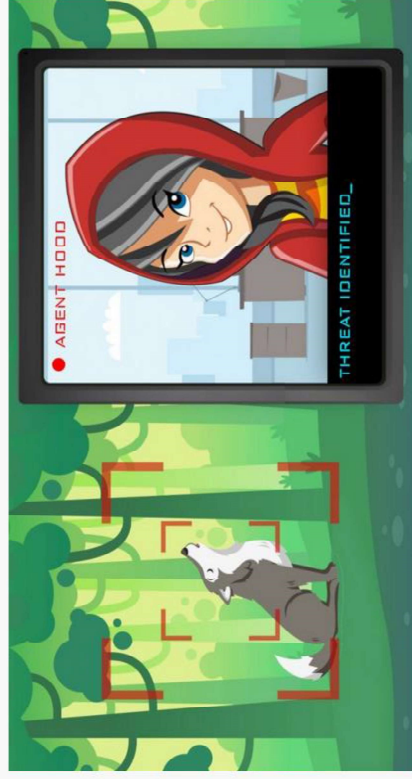
© 2018 IBM Corporation

A Wolf in Grandma's Clothes?

LESSONS IN SECURITY

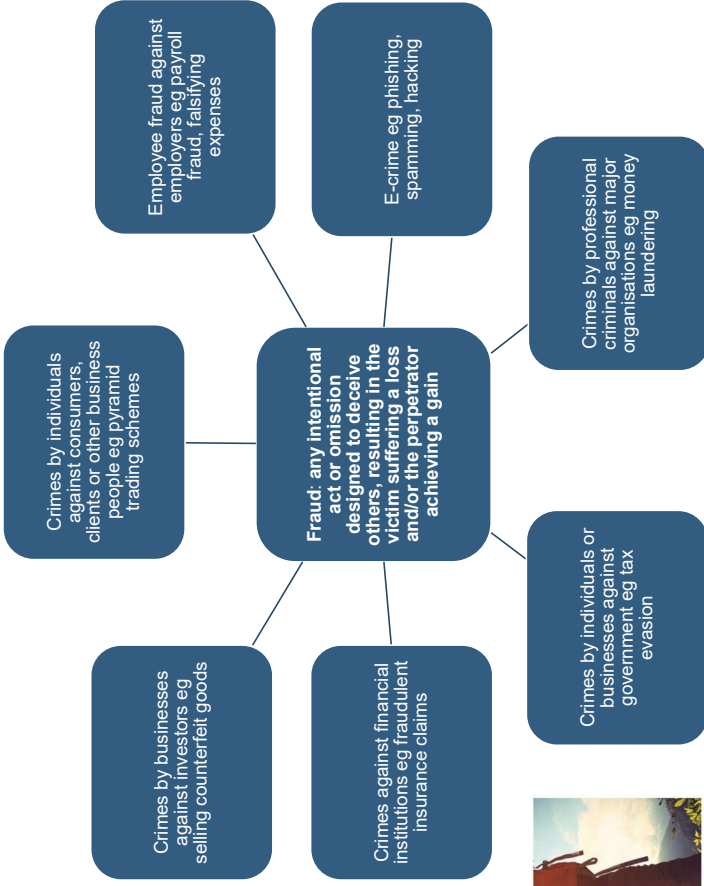
Grandma or the Wolf? Red Gets Smart About Fraud Protection

October 23, 2017 | By Aubre Andrus Co-authored by Eileen Turner | Brooks Miller



<https://securityintelligence.com/grandma-or-the-wolf-red-gets-smart-about-fraud-protection/>

Fraud definition



<https://www.cimaglobal.com/Research--Insight/Fraud-risk-management-A-guide-to-good-practice/>

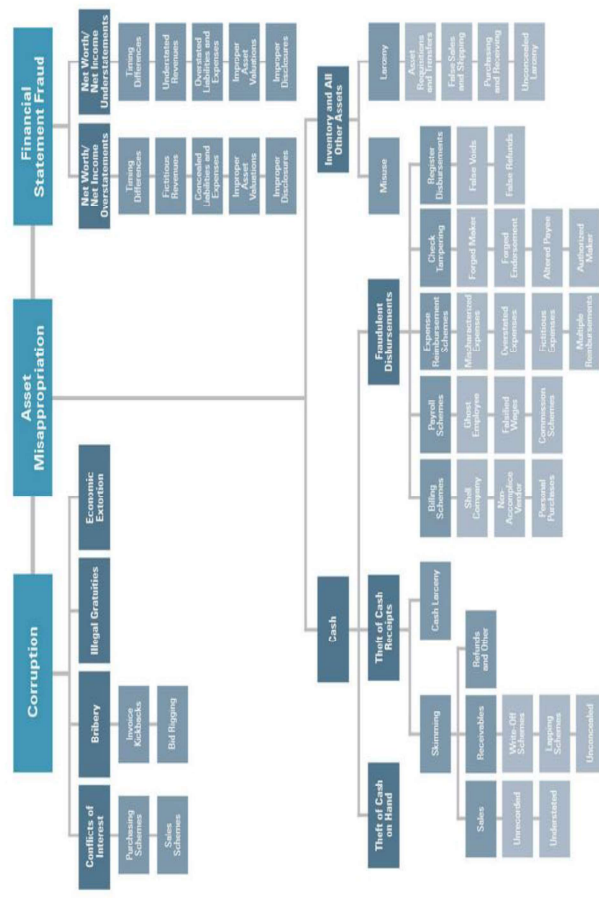
Internal Fraud

- Occupational frauds are those in which an employee, manager, officer, or owner of an organization commits fraud to the detriment of that organization.
- The three major types of occupational fraud are:
 - Corruption,
 - Asset Misappropriation,
 - and Fraudulent Statements.

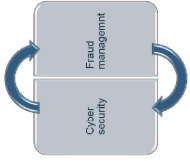
<http://www.acfe.com/fraud-tree.aspx>

THE FRAUD TREE

OCCUPATIONAL FRAUD AND ABUSE CLASSIFICATION SYSTEM



Cyber security and fraud management



Cybercrime Trends Are Shifting

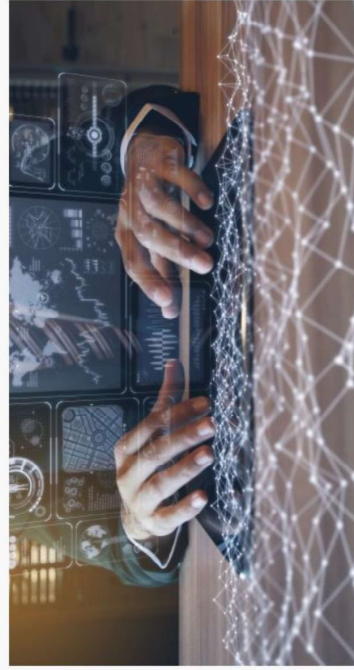
In its “[2016 Internet Crime Report](#),” the FBI’s Internet Crime Complaint Center (IC3) revealed that account takeover and identity theft claims had decreased by 23 percent since 2015, while the average loss per incident increased by 33 percent to \$3,491.

This change can be attributed to fraudsters’ efforts to optimize their ROI by focusing more on attacking commercial and treasury banking customers. These customers are attacked using more targeted, well-planned methodologies such as remote-access Trojans (RATs), business email compromise (BEC) and email account compromise (EAC). The FBI IC3 report showed a 53 percent increase in BEC/EAC attacks from 2015 to 2016 and a 46 percent increase in the monetary losses associated with these incidents, scaling up to more than \$360 million in 2016.

<https://securityintelligence.com/ransomware-trojans-and-fraud-oh-my-tracking-recent-cybercrime-trends-and-patterns/>

Cybersecurity, Fraud and Operational Risk: The Time for Cognitive Convergence Is Now

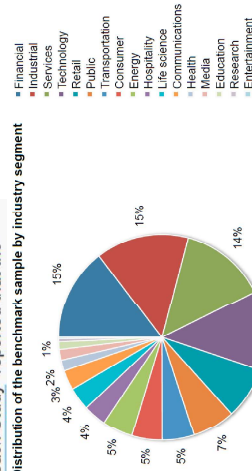
December 8, 2017 | By Indy Dhani



intricate and persistent. While technologies and processes have made advances in risk management, cybersecurity and fraud prevention, a recent IBM Institute for Business Value (IBV) report revealed that 42 percent of banking executives believe that their fraud operations are in need of an overhaul. Another IBV survey found that 61 percent of security leaders are significantly challenged to identify, assess and prioritize threats, due to insufficient resources.

The Ponemon Institute’s “2017 Cost of Data Breach Study” reported that the

Pie Chart 3. Distribution of the benchmark sample by industry segment

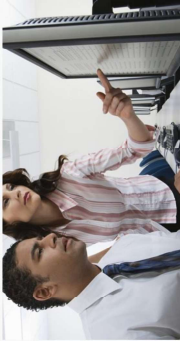


Cyberattacks, financial crime and fraud incidents are becoming more targeted,

<https://securityintelligence.com/cybersecurity-fraud-and-operational-risk-the-time-for-cognitive-convergence-is-now/>

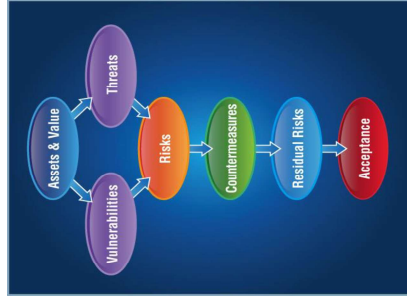
Fraud Management System

Management system
set of interrelated or
interacting elements of
an organization to
establish policies and
objectives and
processes to achieve
those objectives



Fraud Risk Assessment

- Fraud risk management program should be seen as a component of a larger enterprise risk management (ERM) and integrated with Information Security Risk Management.
- You should ask for following question:
 - How might a fraud perpetrator exploit weaknesses in the system of controls?
 - How could a perpetrator override or circumvent controls?
 - What could a perpetrator do to hide the fraud?
- Organizations should select and apply a framework to document their fraud risk assessment.
- Before conducting a risk assessment, management should identify a risk assessment team. This team should include individuals from throughout the organization with different knowledge, skills, and perspectives and should include a combination of internal and external resources (Accounting/finance, business unit and operations personnel, Risk management personnel, Legal and compliance personnel, Internal audit personnel, external consultants with expertise in Standard, KRI's, anti-fraud methodology,...)
- Team should present Risk Assessment Report to Top Management that will define best strategy to mitigate risk with a cost/benefit analysis.



Security Risk

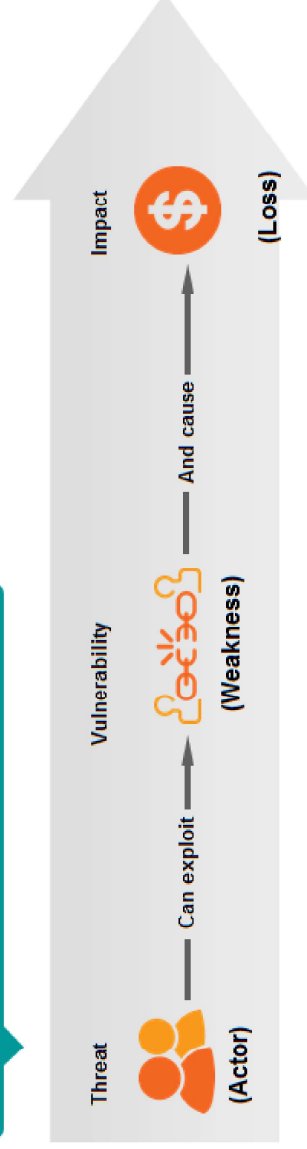
Security risk exists when ...



Security Risk Management is the application of **control** to detect and block the threat, to detect and fix a vulnerability, or to respond to incidents (impacts) when all else fails.

Fraud Risk

Fraud risk exists when ...



Fraud Risk Management is the application of **control** to detect and block the threat, to detect and fix a vulnerability, or to respond to incidents (impacts) when all else fails.

Fraud Risk Assessment

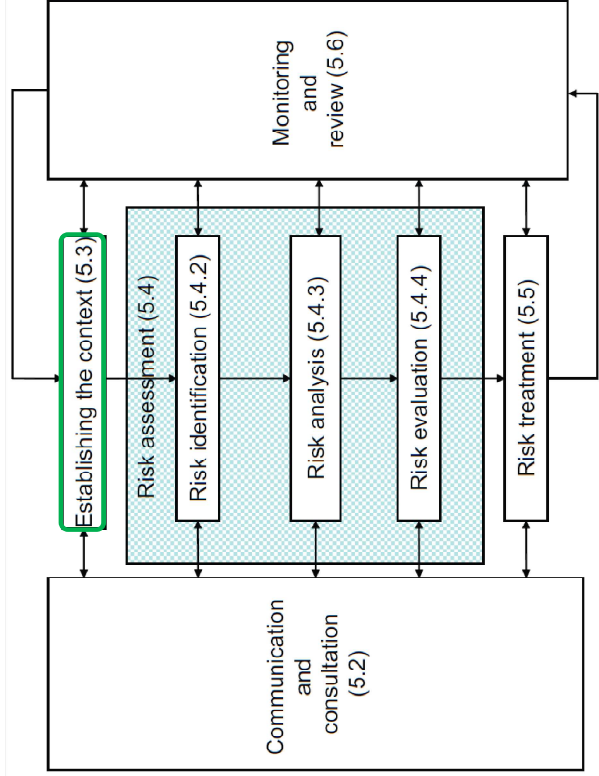


Figure 3 — Risk management process

ISO 31000



- Establishing the context
 - The organization's main purpose
 - Its business, its mission, its values
 - Structure of organization
 - Stakeholder analysis
 - List of constraints
 - legislative and regulatory,
 - technical,
 - financial,
 - organizational,
 - ...

Fraud Risk Assessment

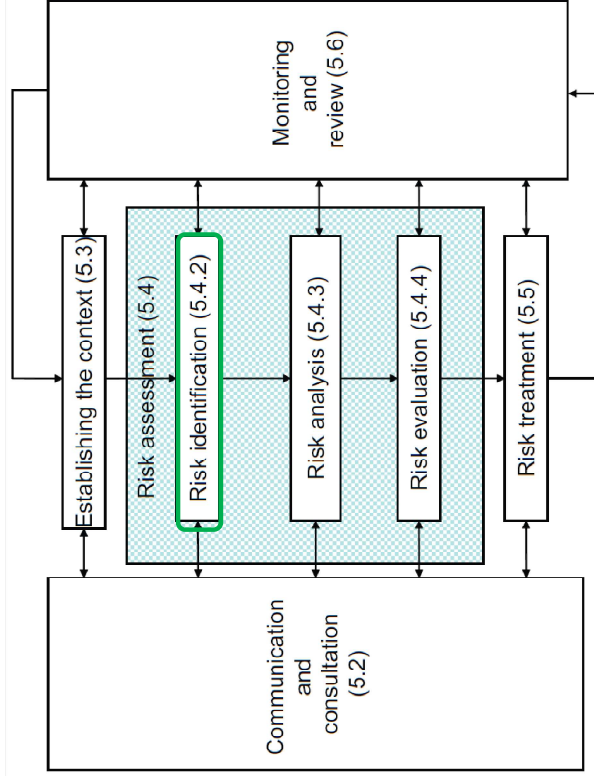


Figure 3 — Risk management process

ISO 31000

- Risk Identification
 - Asset Identification (Processes, Information, Resources,...)
 - Asset valuation (Impact analysis and classification)
 - Threat identification from a selection of Fraud risk catalogue: considering any situation applicable, potential fraudsters and motivation
 - Vulnerabilities and Threats analysis
 - Which controls you need (using standard)
 - Threats and Controls matrix

Fraud Risk Assessment

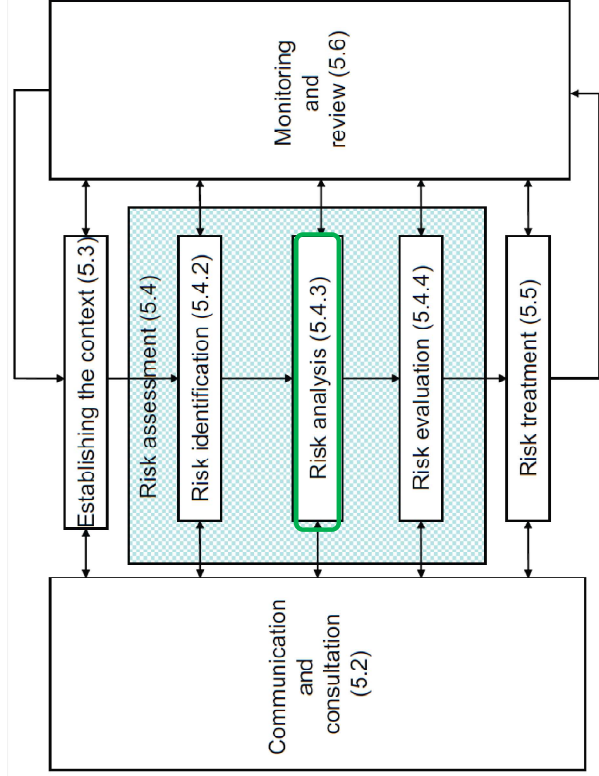
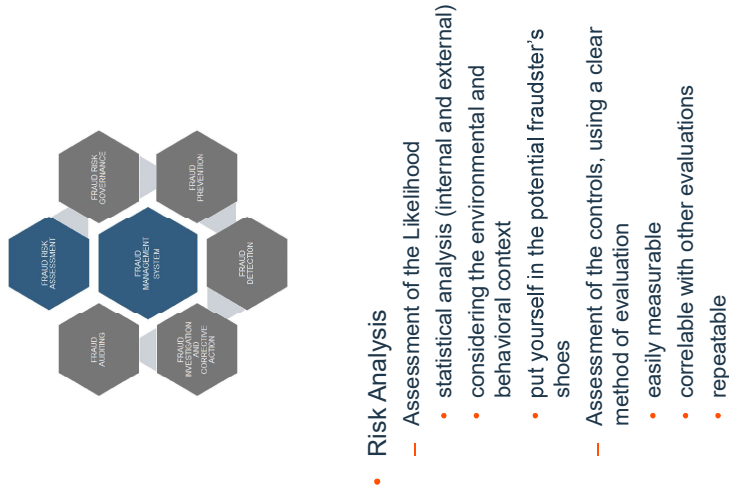


Figure 3 — Risk management process

ISO 31000



Fraud Risk Assessment

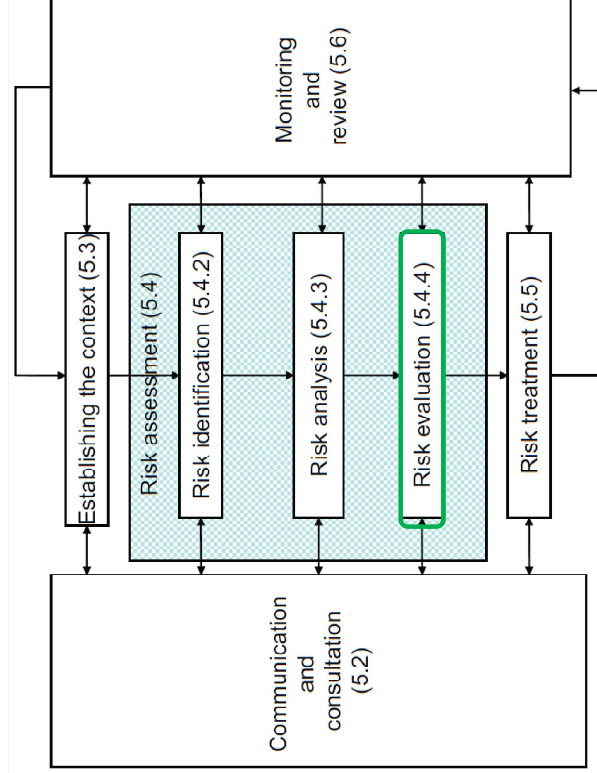


Figure 3 — Risk management process

ISO 31000



Fraud Risk Assessment

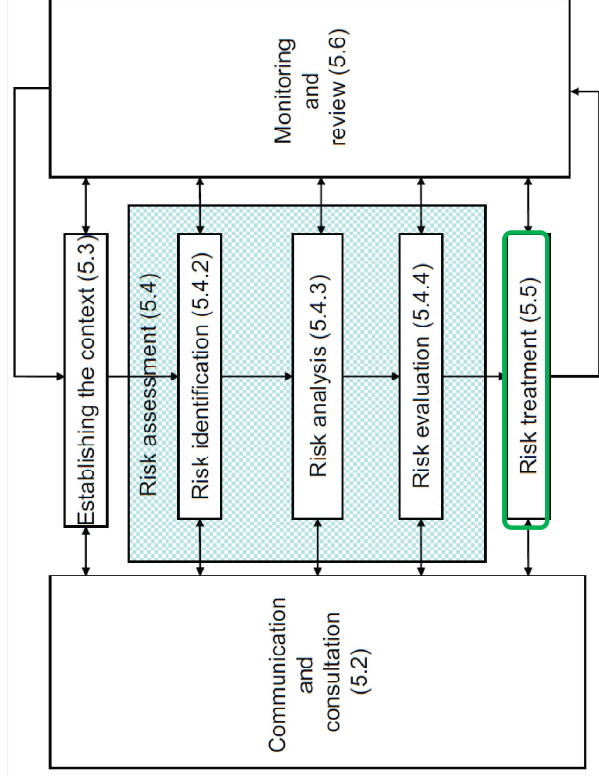
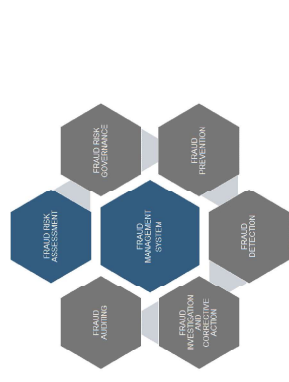


Figure 3 — Risk management process

ISO 31000



- **Risk Treatment**
 - Determine possible options for treatment
 - Avoid,
 - Transfer
 - Reduce
 - Accept
 - Decide on best treatment option
 - Cost/benefit analysis
 - Prioritization and road map
 - Assigning action and timetable

Fraud Risk Governance: establish a framework

- **Top Management**
 - Defining objectives and provide commitment
 - Fraud Risk Assessment Review
 - Understand fraud risks
 - Oversee the internal controls
 - Monitor management's reports on fraud risks, policies, and control activities (KPI's)
 - Involving experts and specialized companies
 - Provide commitment for external audit
- **Fraud Management Committee**
 - Respect independence
 - Guarantee competence
 - To be proactive
 - Review audit objectives and results
- **Management**
 - Support in risk management program
 - Promote culture
 - Monitoring of internal controls
 - Reporting to the board on actions
- **Staff**
 - Have a basic understanding of fraud and be aware of the risks
 - Read and understand policies and procedures
 - Understand when noncompliance may create an opportunity for fraud
 - Participate in the process of creating, implementing and monitoring a fraud control environment
 - Report suspicions or incidences of fraud.
 - Cooperate in investigations
- **Internal Auditing**
 - Objective is the assurance and consulting activity on fraud control
 - Consider the organization's assessment of fraud risk
 - Planning and execute Internal audit
- **Fraud awareness**
 - It should define and describe fraud and fraud risks.
 - Consider who should attend, frequency and length, cultural sensitivities, guidance on how to solve ethical dilemmas, and delivery methods
- **SoD Management Process**
 - A process should be implemented for directors, employees, and contractors to internally self-disclose potential or actual conflicts of interest.
- **Reporting Procedures and Whistleblower Protection**
 - The channels to report suspected fraud issues should be clearly defined and communicated
- **Process Evaluation and Improvement (Quality Assurance)**



Fraud Prevention

- Human Resources Processes
 - One of the most important prevention activities is to define behavioral rules and make staff aware of the company's ability to control compliance with the rules themselves. The **communication** is therefore decisive in terms of deterring from internal fraud.
 - Other controls: Performing Background Investigations, Anti-fraud Training, Evaluating Performance and Compensation Programs, Conducting Exit Interviews
- Access control
 - an accurate definition of the **access profiles** carried out through an analysis of roles and responsibilities protects against abuses and unwanted actions
 - strict **access management** limits improper use and fraud attempts
- Transaction protection
 - authorization **processes** and checks on the correctness of data flows reduce the risk of fraud on transactions
- Fraud prevention techniques
 - Methods and tools for prevention should be documented in such a way as to make their application measurable in terms of effectiveness and efficiency

https://www.acfe.com/uploadedfiles/acfe_website/content/documents/managing-business-risk.pdf



- Test procedures and tools
 - periodic tests should be performed to assess the adequacy of the organizational and technical measures prepared
- Performance evaluation and monitoring
 - management should evaluate the effectiveness and efficiency of preventive measures through the continuous evaluation of indicators

Fraud Detection

- Why do you need fraud detection?
 - Prevention will never eliminate the risk of fraud. Therefore **techniques for detecting fraud** should be implemented. The acquisition of these tools will have to be evaluated on the basis of a cost-benefit analysis that will take into account the context in which it operates.
- Whistleblower Hotlines
 - A **person can expose** any kind of information or activity that is deemed illegal, unethical, or not correct within an organization that is either private or public through a system that could also be anonymous
- Process and procedures controls
 - Definition of criteria for the identification of potential fraud and use of **data mining**.
 - **Cognitive** analysis for the analysis of big data can facilitate the search for fraud using information such as the specific industry
- Fraud detection techniques
 - Implementation of **monitoring and detection tools** in real time of potentially risky events allow proactive actions by management



- Test procedures and tools
 - periodic tests should be performed to assess the adequacy of the organizational and technical measures prepared
- Performance evaluation and monitoring
 - management should evaluate the effectiveness and efficiency of preventive measures through the continuous evaluation of indicators

https://www.acfe.com/uploadedfiles/acfe_website/content/documents/managing-business-risk.pdf

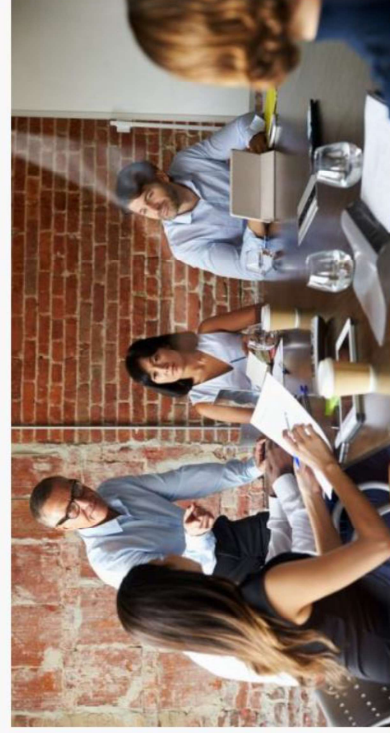
Fraud Investigation and corrective action

- Fraud investigation process
 - The process should include
 - a timely **reporting mechanism** for both potentials and actual frauds.
 - a fraud management **team** definition
 - an **assessment process**
 - an investigation **protocol**
 - and finally a **corrective action process**
 - The process should be integrated and managed in accordance with the process of Security Incident Management and Data Breach Management.
- Which information do you need?
 - To allow an adequate management you should prepare **a form for gathering all the information** necessary for the investigation (Categorizing issues, Defining the severity, Escalation criteria, Listing types of information that should be kept confidential, ...)
- Who evaluates the information collected?
 - The **board** will have to decide who will evaluate the information by designating the team and in some cases also requiring external staff to the organization (especially when managers are involved)
- Investigation protocols
 - some factors to consider in the definition of the management methods concern the confidentiality, time-sensitive, evidences, Objectivities...
 - Responsibility for overseeing an investigation should be given to an individual with a level of authority at least one level higher than anyone potentially involved in the matter



- Conduction and reporting
 - The investigation team should establish the investigation tasks and assign each task to the appropriate team members.
 - **The investigation team should report its findings to the senior management, directors, or legal counsel.**
- Corrective Action
 - Any action taken should be appropriate under the circumstances and should be taken only after consultation with individuals responsible for such decisions.
 - Management consultation with legal counsel is strongly recommended

Building the Best Incident Response Team



- Incident response is one of the final frontiers of security that the majority of businesses have yet to explore. Although most have the written policies and the proper technologies, many enterprises are ill-prepared for that unexpected and often undetected security incident. This general lack of preparedness has created a “wing it” attitude over the years. Even worse, IT and security teams frequently lack clear goals, and executive management and board members are too disconnected from the security function to bridge this gap.
- Management often assumes that IT and security have everything under control. After all, good money was spent on security, so things should be locked down and incidents shouldn't occur, right? On the other hand, many IT and security professionals believe they can handle an incident and everything that comes with it. That may be true from a technical perspective, but dealing with the people and business side of a security incident is an entirely different matter that requires different people and various skill sets within the organization.

<https://securityintelligence.com/building-the-best-incident-response-team/>

Who Is Involved?

- Still, it is security, so there's going to be politics, resistance and downright ignorance among those involved. Here are the roles that I've seen taking part in the response process in fully functioning security programs:
 - **Legal counsel** to provide oversight and guidance on steps to take or not take;
 - **Executive management** for decision-making at the executive/board level;
 - **IT and security** teams for technical guidance and execution of the initial incident response phases;
 - **Compliance** for assistance with incident oversight and follow up, including any breach notification or reporting that may be required;
 - **Business operations** for guidance and communications across departments and teams;
 - **Human resources** for facilitating internal communications and assisting with user-centric security policies that may have been violated;
 - **Public relations** expertise from someone who has experience in this area and a prepared message;
 - **Outside consultants** who can provide incident response, forensics and security testing expertise;
 - **Vendors** such as internet service providers (ISPs), cloud service providers and managed security service providers (MSSPs); and
 - **Business partners** that have close technical ties to your environment.

<https://securityintelligence.com/building-the-best-incident-response-team/>

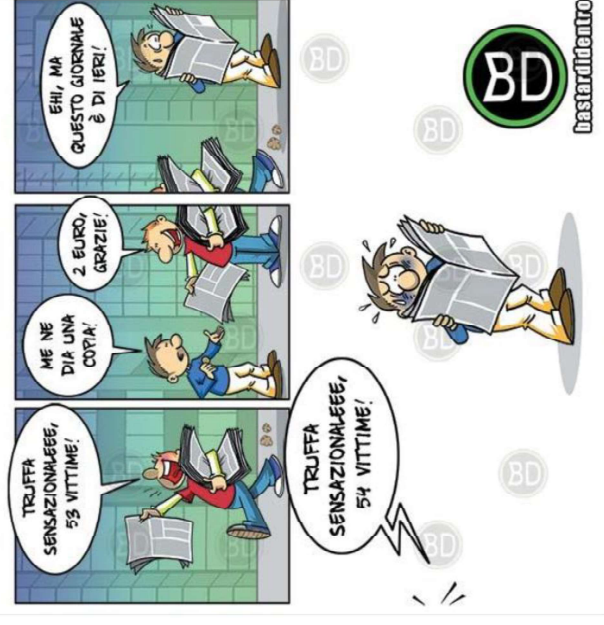
Fraud Auditing

- The organization shall conduct internal audits at planned intervals to provide information on whether the Fraud Management System:
 - conforms to
 - 1) the organization's own requirements for its information security management system; and
 - 2) the requirements of any regulation or standard in scope;
 - is effectively implemented and maintained.
- The organization shall:
 - plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;
 - define the audit criteria and scope for each audit;
 - select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;
 - ensure that the results of the audits are reported to relevant management; and
 - retain documented information as evidence of the audit programme(s) and the audit results.



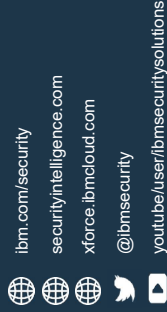
Conclusions

- A clear definition of **Roles**, **Responsibilities** and assigned **Actions** is fundamental for achieving the objectives of a fraud management system
- You can not eliminate the possibility of being a victim of fraud: the **risk management approach** guarantees the costs/benefit balance
- Fraud management (both preventive and reactive) is effective only if there is a **management system regularly tested and monitored**
- The **awareness process** of any stakeholders (employees, suppliers, partners) is the most important deterrent together with the use of **technologies** able to provide the right alarms (analytics, SIEM, investigations)
- The team to be involved should **know the business processes and have adequate skills** (cybersecurity, fraud management, auditing, legal requirement)



THANK YOU

FOLLOW US ON:



© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems. Including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security strategy. IBM systems, products and services are designed to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.