



# Ład korporacyjny

i jego wpływ na IT

Michał Kossowski (BOC IT Consulting)

# Treść

- ◆ Ład korporacyjny – definicje oraz przedstawienie projektu IRIGOV
- ◆ MIFID
- ◆ Basel II
- ◆ SOX
- ◆ Wdrożenie ładu korporacyjnego

# Ład korporacyjny - definicje

Definicje Corporate governance (ład korporacyjny władztwo korporacyjne):

"Corporate governance to system przez który firmy są kierowane i sterowane.,,

"Corporate governance... odnosi się do... instytucji zajmujących się konfliktem między interesami inwestorów pragnących otrzymać "gwarantowany" zwrot zainwestowanych funduszy oraz interesami "menedżerów", którzy chcą zwiększyć kontrolę nad użyciem tych funduszy przy jak najmniejszym możliwym udziale inwestorów."

Głośno o CG zrobiło się po bankructwach firm Enron, Worldcom w 2001 roku.

Źródło: Wiki

# ENISA i projekt IRIGOV

## Europejska Agencja Bezpieczeństwa Sieci i Informacji - ENISA (European Network Information and Security Agency)



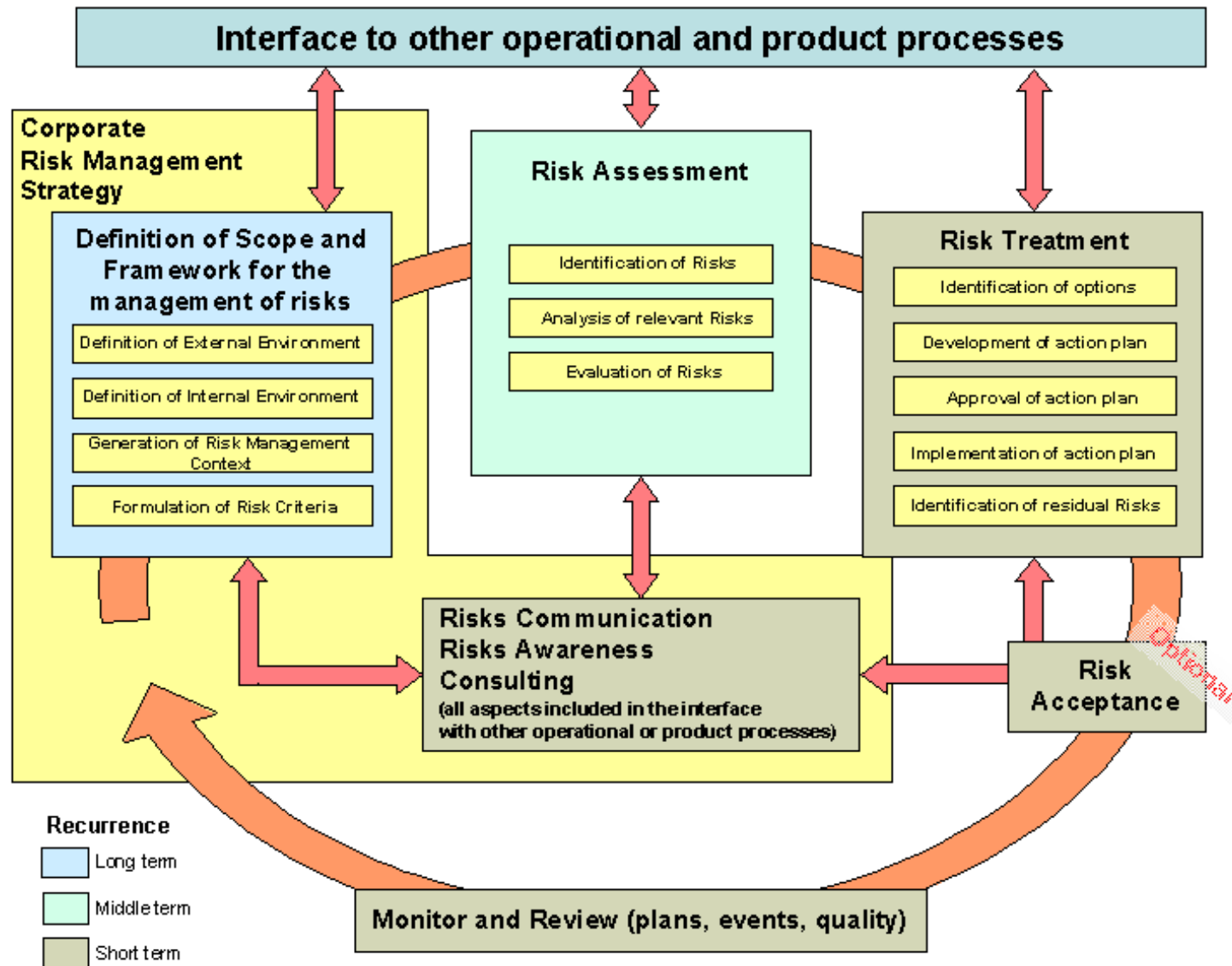
Ideą powołania agencji ENISA była potrzeba stworzenia europejskiego centrum wiedzy, które mogłoby służyć Komisji Europejskiej oraz krajom członkowskim. Ma stanowić wsparcie w postaci doradztwa i zaplecza służącego, w sposób skoordynowany, do rozwiązywania problemów rosnącego zagrożenia bezpieczeństwa komunikacji elektronicznej - w uzgodnieniu ze wszystkimi sektorami gospodarki, nauki i administracji publicznej.

...

W zamierzeniach Unii Europejskiej agencja ma wzmocnić zdolność gospodarki unijnej do przeciwdziałania i reagowania na zagrożenia bezpieczeństwa ICT.

Źródło: [www.enisa.pl](http://www.enisa.pl)

# ENISA RA/RM framework

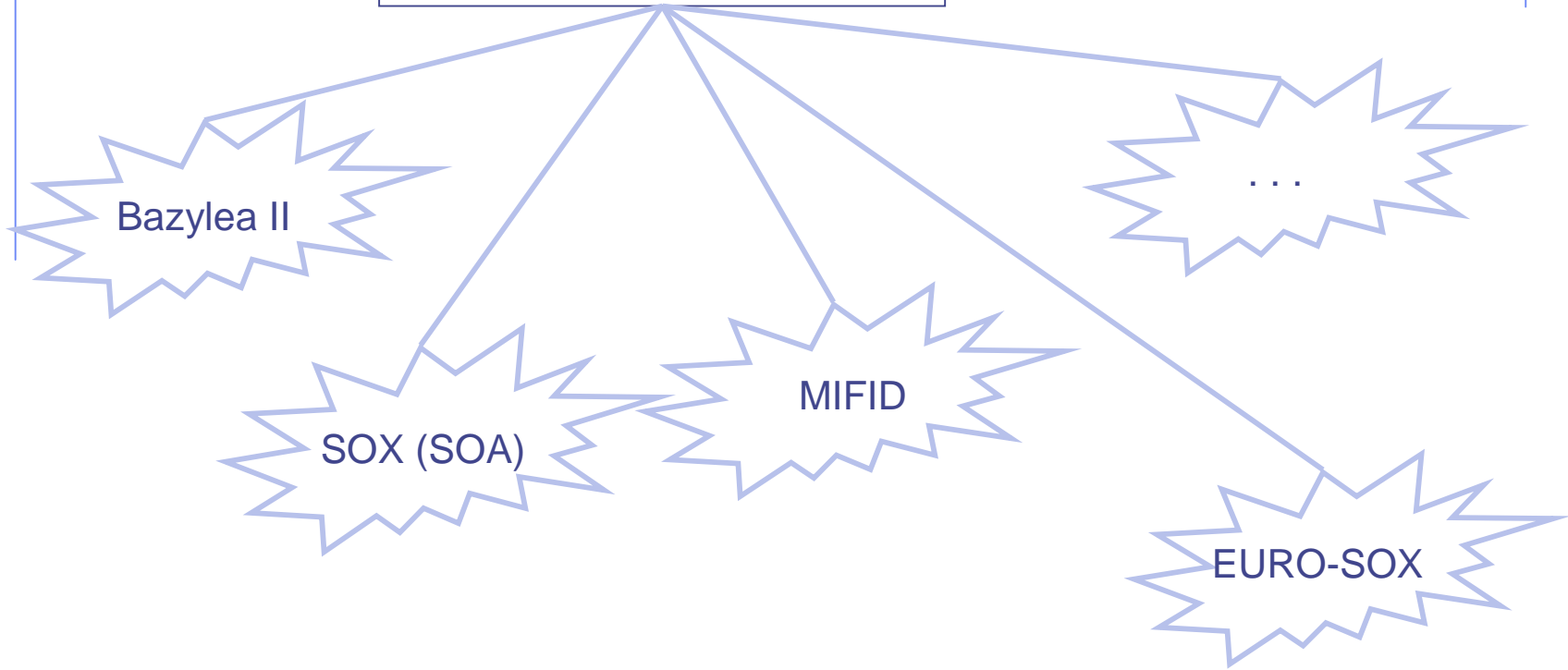


# ENISA i projekt IRIGOV



Projekt IRIGOV – integracja procesu zarządzania/oceny ryzyka (RM/RA process) z Ładami Korporacyjnymi

*Łady korporacyjne*



The slide features a blue patterned header bar at the top. On the left side, there is a blue L-shaped line with a small circle at its top-left corner. A vertical blue line runs down the right side of the slide.

# Basel II

# Basel II

## Tytuł

International Convergence of Capital Measurement and Capital Standards (Basel II)

## Opis

Basel II (Nowa Umowa Kapitałowa) - opublikowany przez Bazylejski Komitet Nadzoru Bankowego zbiór najlepszych praktyk rynkowych w zakresie zarządzania ryzykiem finansowym w sektorze Bankowym oraz utrzymywania bezpiecznego poziomu kapitałów przez Banki.

Zapisy Basel II zostały przekształcone w prawo obowiązujące we wszystkich państwach Unii Europejskiej poprzez:

- \* Dyrektywę Parlamentu Europejskiego i Rady nr 48/2006; oraz
- \* Dyrektywę Parlamentu Europejskiego i Rady nr 49/2006

zwane łącznie Capital Requirements Directive (CRD).

Do polskiego porządku prawnego Nową Umowę Kapitałową / dyrektywy CRD transponują Uchwały Komisji Nadzoru Bankowego z dnia 13 marca 2007 r.

# Basel II

## **Cel**

- Zapewnienie, że alokacja kapitału jest bardziej czuła na ryzyko;
- Oddzielenie ryzyka operacyjnego od kredytowego;

## **Dotyczy**

Banków

# Basel II

Basel II używa koncepcji „trzech filarów”:

## Pierwszy filar

The first pillar deals with maintenance of regulatory capital calculated for three major components of risk that a bank faces: credit risk, operational risk and market risk. Other risks are not considered fully quantifiable at this stage.

The credit risk component can be calculated in three different ways of varying degree of sophistication, namely standardized approach, Foundation IRB and Advanced IRB. IRB stands for "Internal Rating-Based Approach".

For operational risk, there are three different approaches - basic indicator approach or BIA, standardized approach or STA, and advanced measurement approach or AMA.

For market risk the preferred approach is VaR (value at risk).

## Drugi filar

The second pillar deals with the regulatory response to the first pillar, giving regulators much improved 'tools' over those available to them under Basel I. It also provides a framework for dealing with all the other risks a bank may face, such as systemic risk, pension risk, concentration risk, strategic risk, reputation risk, liquidity risk and legal risk, which the accord combines under the title of residual risk.

## Trzeci filar

The third pillar greatly increases the disclosures that the bank must make. This is designed to allow the market to have a better picture of the overall risk position of the bank and to allow the counterparties of the bank to price and deal appropriately.

# Basel II – focus: safety

| IT processes\functions  | HW and SW requirements  |
|---|---|
| <u>Confidentiality and Access control</u><br>Only eligible individuals should gain access to confidential information. No unauthorised transactions can take place.   | Encryption software and authentication mechanisms.<br>Security policies (e.g. auto logoff after period of idle time)                                    |
| <u>Integrity</u><br>Transaction data needs to be transmitted in a safe way so that it cannot be intercepted or modified.  | Encryption software   |
| <u>Availability</u><br>Interruptions of the service should not take place.  | System redundancy (for critical systems at least twice).<br>If possible – using heterogeneous environment.  |
| <u>Change Management</u><br>It should be impossible to change a system in a way that it would allow lowering security level (executing transactions without authorisations, executing transactions without necessary checks, turning off logging mechanism) | Code needs to undergo review, changes in the code need to be controlled in order to prevent unauthorised changes. All changes should leave audit trail. |

# Basel II

SOX

# SOX

## Nazwa

Ustawa Sarbanesa-Oxleya (nazywana też SOX lub SarOx)

## Krótki opis

Ustawa Sarbanesa-Oxleya obejmuje jedenaście rozdziałów. Wprowadza wymóg dodatkowych ujawnień dokonywanych przez zarząd, dotyczących efektywności systemu kontroli wewnętrznej. Nakłada obowiązek kontroli jakości usług audytorskich, dodatkowe sankcje (finansowe i karne) dla władz spółek w przypadku wykrycia błędów w sprawozdaniach finansowych oraz wprowadza bezwzględny wymóg niezależności audytora. Porusza też temat powołania Rady Nadzoru nad Rachunkowością Spółek Publicznych (Public Company Accounting Oversight Board - PCAOB).

## Cel

Ustawa ma celu odbudowanie zaufania inwestorów poprzez poprawę jakości i wiarygodności sprawozdawczości finansowej.

# SOX – focus: Data integrity and support for audits

| <b>IT processes\functions</b>   | <b>HW and SW requirements</b>   |
|---|---|
| <u>Confidentiality and Access control</u><br>Only eligible individuals should gain access to confidential information.  | Encryption software.<br>Existing solutions need to be audited in order to determine whether sensitive data is stored and presented only in a controlled way (e.g. no unencrypted logs with confidential data) |
| <u>Integrity</u><br>It should be possible to prove that data is not modified.   | Integrity checks and hashing.   |
| <u>Availability</u><br>Data needs to be available to entitled entities.   | Inspections of code reliability, resistance to DOS attacks, reliable data storage and failover mechanisms.  |
| <u>Auditing and Logging</u><br>Events processing sensitive data need to be logged.                                      | Mechanism of logging available in all applications handling sensitive data. Logs need to provide info about all relevant system events while not disclosing sensitive info.                                   |
| <u>Change Management</u><br>Companies need to provide info concerning changes in procedures of handling financial data. | Systems that allow customising of the workflow need to provide logs of changes.   |

Źródło: <http://msdn2.microsoft.com/en-us/library/aa480484.aspx>

The slide features a blue patterned header bar at the top right. On the left side, there are blue lines forming an L-shape, with a small circle at the top-left corner. A vertical blue line runs down the right side of the slide.

# MIFID

# MIFID

## Nazwa

Markets in Financial Instruments Directive (MIFID)

## Opis

The Markets in Financial Instruments Directive (MiFID) is a European Union law which provides a harmonised regulatory regime for investment services across the 30 member states of the European Economic Area (the 27 Member States of the European Union plus Iceland, Norway and Liechtenstein). The main objectives of the Directive are to increase competition and consumer protection in investment services. As of the effective date, 1 November 2007, it replaced the Investment Services Directive (Directive 93/22/EEC). MiFID is a part of the EU Financial Services Action Plan (FSAP).

## Regulacje

- DIRECTIVE 2004/39/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 21 April 2004
- COMMISSION DIRECTIVE 2006/73/EC of 10 August 2006 (implementing Directive 2004/39/EC of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive)
- COMMISSION REGULATION (EC) No 1287/2006 of 10 August 2006 (implementing Directive 2004/39/EC of the European Parliament and of the Council as regards recordkeeping obligations for investment firms, transaction reporting, market transparency, admission of financial instruments to trading, and defined terms for the purposes of that Directive)

Source [2008.01.05]: <http://en.wikipedia.org/wiki/MiFID>

# MIFID

## Obszary biznesowe (1/2)

- Conflicts: MiFID takes a broad approach to conflicts of interest and less reliance can be placed on client disclosure. MiFID requires firms and credit institutions to identify all actual or potential conflicts of interest and to maintain and operate organisational and administrative arrangements to prevent conflicts from adversely affecting clients. A written conflicts policy is required.
- Best Execution: MiFID extends the Best Execution requirement to all products. Seeking the best possible result means obtaining the best combination of price and costs subject to other considerations relevant to the execution of a client's orders.
- Client Categorisation: The current client base will have to be (re)classified into MiFID retail client, professional client and eligible counterparty categories.
- Systems and Controls: MiFID requires firms to establish policies and procedures to ensure compliance with MiFID obligations including internal audit, risk management and compliance function. Responsibility rests on senior management to ensure compliance with MiFID obligations.

# MIFID

## Obszary biznesowe (2/2)

- Outsourcing: Outsourcing of “portfolio management” for retail clients to firms in countries outside the EEA will be permitted only where outsourcee is authorised or registered in its home country and subject to prudential supervision, or where prior notification to the competent authority is given and it has not objected. Outsourcing of all “critical and important operational functions” is subject to regulation under MiFID.
- Pre-trade Transparency: “Systematic internalisers”, i.e. firms which deal in equity on own account on an “organised, frequent and systematic basis”, will have to publish prices and, effectively, deal as market maker with their clients.
- Post-trade Transparency: MiFID will require for the first time, investment firms to publish the price and volume of all completed trades undertaken outside a regulated market or MTF.
- Costs, fees transparency: MiFID requires increased fees transparency. This raises pricing issues in relation to structured products where it may be necessary to provide information on how profit on each element of product is generated to allow clients to “verify” the total price.
- Risk warnings: Where risk warnings are required, the Level 2 Directive provides that in relation to a structured product or service the firm must provide an adequate description of the risks of each component of a product as well as describing risks arising from interaction of the component parts taken together.

# MIFID

## Cele

- Increased transparency across all trading venues
- Enhanced protection for the retail investor
- Greater competition between markets
- Opportunity for cross border competition
- Increased levels of disclosure, in particular to the retail investor

## Zakres

Companies performing investment services and activities (Investment Banks, Asset Managers, Broker Dealers, Corporate Banks, Retail Banks, Futures&Options Firms, Commodities Traders)

# MIFID – focus: Performance, data storage and extended analytics

| <b>IT processes \ functions</b>   | <b>HW and SW requirements</b>   |
|---|---|
| <p><b>Data processing</b></p> <p>Customer and market data need to be analysed and processed in a timely manner.</p> <p>Additional analysis are necessary to prove „best execution” of customer orders.</p> <p>Potential conflicts of interests need to be analysed.</p> | <p>Applications need to provide results (also based on data from many sources) within short time frame – possible need for more processing power and more demand for bandwidth along with faster access to data from other systems/external data providers.</p> <p>Deals need to be checked against set of rules provided by customer – need for additional analytical tools.</p> |
| <p><b>Availability</b></p> <p>Historical data needs to be stored up to 5 years.</p> <p>More customer data needs to be stored and used in analysis.</p>  | <p>Safe storage of archival data and more storage for processing data for current transactions.</p>   |
| <p><b>Auditing and Logging</b></p> <p>Trading data need to be properly recorded.</p> <p>New transaction reports are needed.</p>   | <p>Applications need to support new type of electronically transmitted transaction reports.</p>   |

Source [2008.01.05]: <http://www.ftfnews.com/files/File/Schmitt.pdf>

[http://misysbanking.com/files/file8747\\_Impact%20on%20End%20to%20End%20Processes.pdf](http://misysbanking.com/files/file8747_Impact%20on%20End%20to%20End%20Processes.pdf)

The slide features a light blue dotted pattern in the top right corner. A thin blue vertical line runs down the right side of the slide. On the left side, there is a blue L-shaped graphic consisting of a vertical line and a horizontal line meeting at a small circle.

# EURO-SOX

# EUROSOX

## Title

Name „EURO-SOX” is not liked by the EU. It is set of directives: 8th Company Law Directive (similar to the US Sarbanes Oxley Act) together with the 4th and 7th directives.

## Short description

There is no common description of EURO-SOX. In addition EU directives are much less strict (so called „principle based”) than US ones („rules-driven”) which makes it much harder to analyse in context of IRIGOV project. In Inet and literature focus is put on 8th Directive.

## Regulations

- The 4th directive Annual Accounts of specific type of companies (78/660/EEC) amended by 2006/46/EC
- The 7th directive Consolidated accounts (83/349/EEC) amended by 2006/46/EC
- The 8th directive of Company Law 1984 (84/253/EEC) and 2006 (2006/43/EC)

Some consulting companies even extend this list to [Source, 2008.01.05, [www.eurosox.dk/files/TheComponentsofEuroSox.pdf](http://www.eurosox.dk/files/TheComponentsofEuroSox.pdf)]:

1. The European Union’s Financial Services Action Plan (FSAP)
2. The 4th directive Annual Accounts of specific type of companies (78/660/EEC)
3. The 7th directive Consolidated accounts (83/349/EEC)
4. The 8th directive of Company Law 1984 (84/253/EEC) and 2006 (2006/43/EC)
5. The Consolidated Admissions and Reporting directive (CARD) (2001/34/EC)
6. The Transparency directive (2004/109/EC)
7. The Insider Dealing directive (1989/592/EEC) & The Market Abuse directive (2003/6/EC)
8. The interaction between EU directives and other regulatory initiatives

# EUROSOX

## Goals

- restoring investor confidence in the EU (the same as SOX in US).

## Scope

Companies listed on EU stock exchanges

# EUROSOX

## **Business areas**

### The 4th directive Annual Accounts of specific type of companies

This Directive coordinates Member States' provisions concerning the presentation and content of annual accounts and annual reports, the valuation methods used and their publication in respect of all companies with limited liability.

### The 7th directive Consolidated Accounts

• This Seventh Company Law Directive coordinates national laws on consolidated (i.e. group) accounts. Together with the Fourth Directive on the annual accounts of public limited liability companies, it belongs to the family of "accounting directives" that form the arsenal of Community legal acts governing company accounts.

- The Directive sets out the methods of drawing up consolidated accounts
- The Directives also regulate the contents of the consolidated annual report
- The Directives establish a system of auditing
- The Directives lay down rules on disclosure

### The 8th Company Law Directive

- clarifies the duties of statutory auditors and provides for their independence and ethical standards;
- introduces a requirement for external quality assurance; and
- provides for public oversight of the audit profession, including third country auditors, and improved cooperation between oversight bodies in the EU

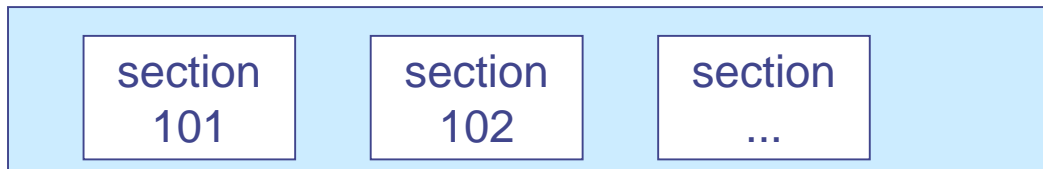


# Wdrożenie ładu korporacyjnego

# Wdrożenie wymagań ładu korporacyjnego

Każdy ład korporacyjny zawiera zestaw wymagań (w formie sekcji, paragrafów, artykułów) adresowanych do grupy docelowej.

## Przykład SOX



Z punktu widzenia IT wymagania te mogą być podzielone na 3 grupy:

- Brak wpływu na IT

(Przykład SOX, sekcja 109: Aby móc przeprowadzić audit firmy notowanej na giełdzie, firma audytująca musi zarejestrować się w Radzie (ang. „Board”)

- Pośredni wpływ na IT

Przykład SOX, sekcja 401: „Każdy finansowy raport roczny i kwartalny ... musi zawierać wszystkie transakcje pozabilansowe ...

- Bezpośredni wpływ na IT

Jeżeli, ..., firma inwestycyjna dostarcza klientowi informacji poprzez stronę www... informacja ta musi być dostępna w sposób ciągły przez okres czasu jakie będzie rozsądny z punktu widzenia klienta.

# MIFID – bezpośrednie i pośrednie wymagania dla IT

## Biznes/procesy biznesowe

Article 25, pt 2, 2004/39/EC

Member States shall require investment firms to keep at the disposal of the competent authority, for at least five years, the relevant data relating to all transactions in financial instruments which they have carried out...

pt. 3

Member States shall require investment firms which execute transactions ... to report details of such transactions to the competent authority as quickly as possible, and no later than the close of the following working day.

pt.4

The reports shall, in particular, include details of the names and numbers of the instruments bought or sold, the quantity, the dates and times of execution and the transaction prices and means of identifying the investment firms concerned.

## IT/procesy IT



**Safe storage of archival data**



**Processing power, bandwidth**



**Processing power, bandwidth, additional data in reports**

## Bezpośrednie wymagania IT

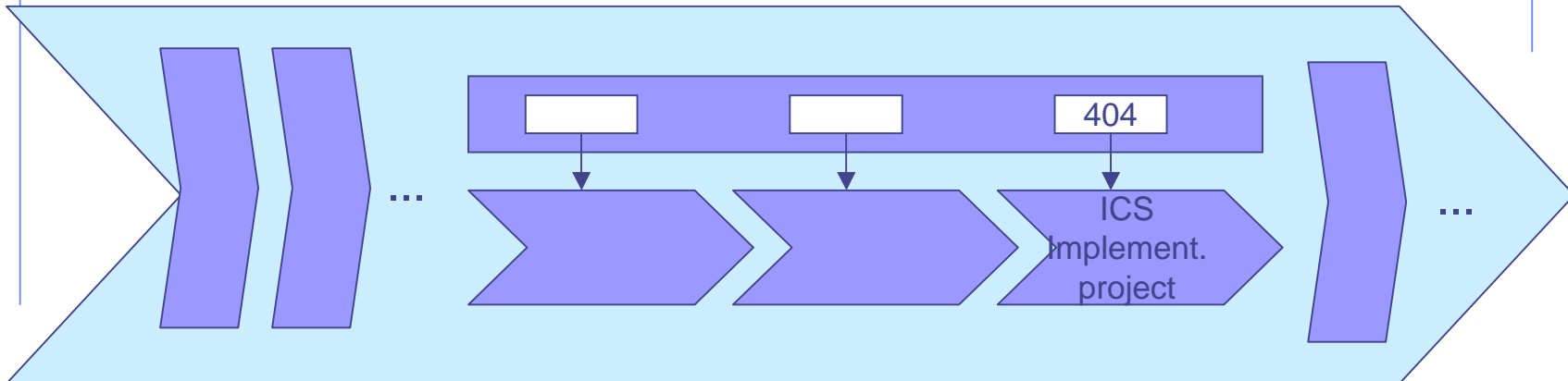
Article 3, pt 2, 2006/73/EC

2. Where, ..., an investment firm provides information to a client by means of a website and that information is not addressed personally to the client, Member States shall ensure that the following conditions are satisfied:

- (c) the client must be notified electronically of the address of the website, and the place on the website where the information may be accessed;
- (d) the information must be up to date;
- (e) the information must be accessible continuously by means of that website for such period of time as the client may reasonably need to inspect it.

# Wdrożenie jako projekt

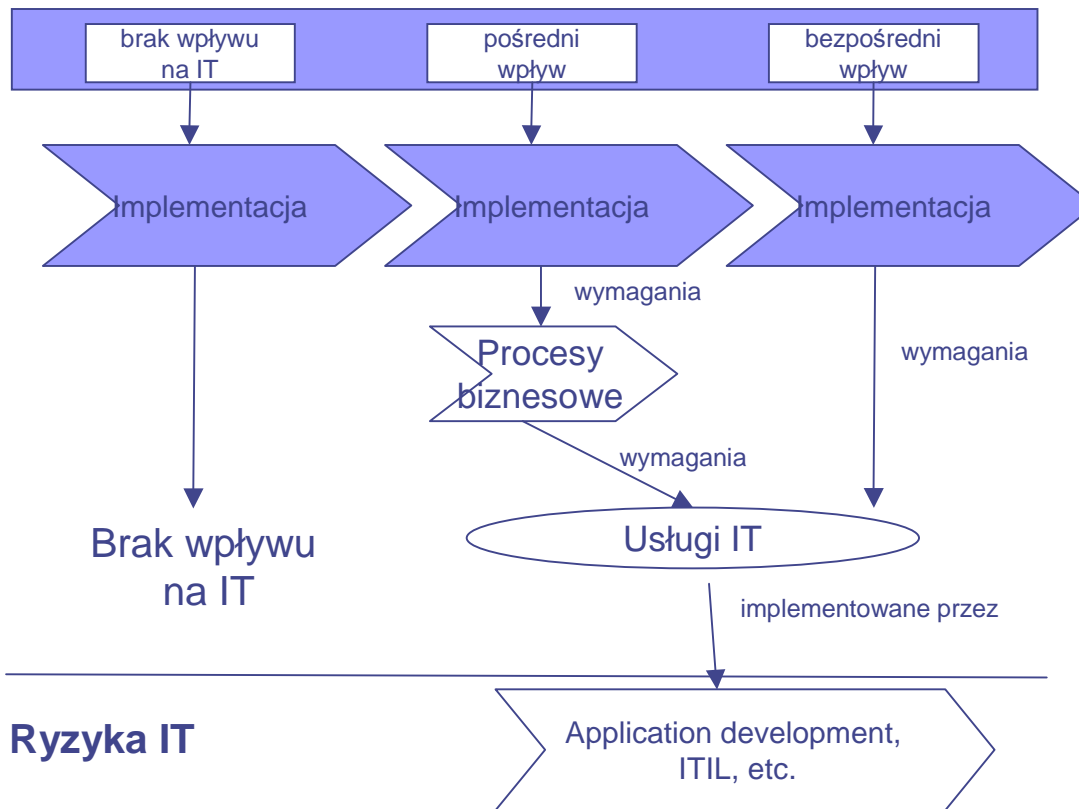
## Projekt wdrożenia CG Framework



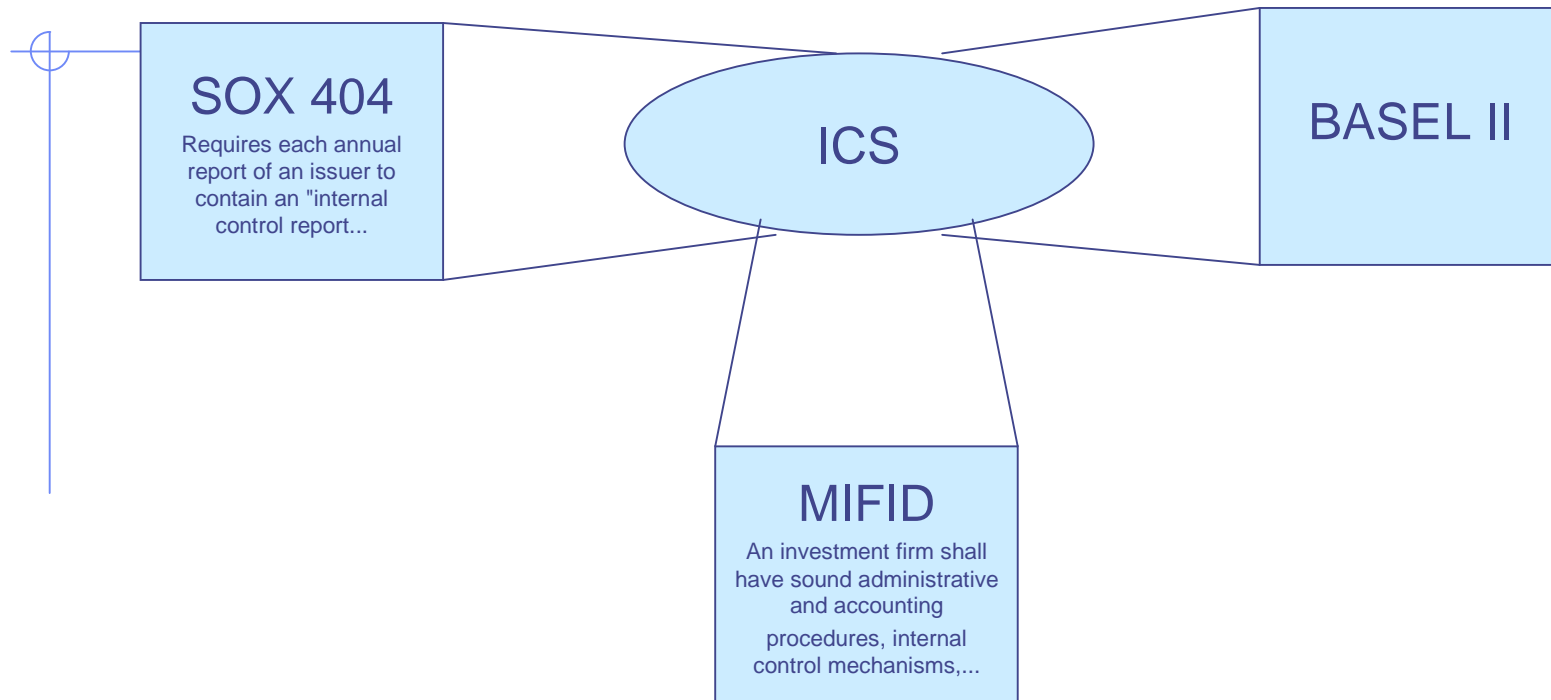
Regulacje ładu korporacyjnego są wdrażane w firmie w postaci projektu. Projekt ten można przedstawić jako etapy procesu. Oprócz standardowych kroków projektu (np. przypisanie menadżera projektu, analiza luk – gap, itd.) główną częścią projektu jest wdrożenie poszczególnych wymagań CG Framework. Ta część jest często dzielona na podprojekty.

# Wdrożenie CGF a IT

## Wymagania zasad ładu korporacyjnego

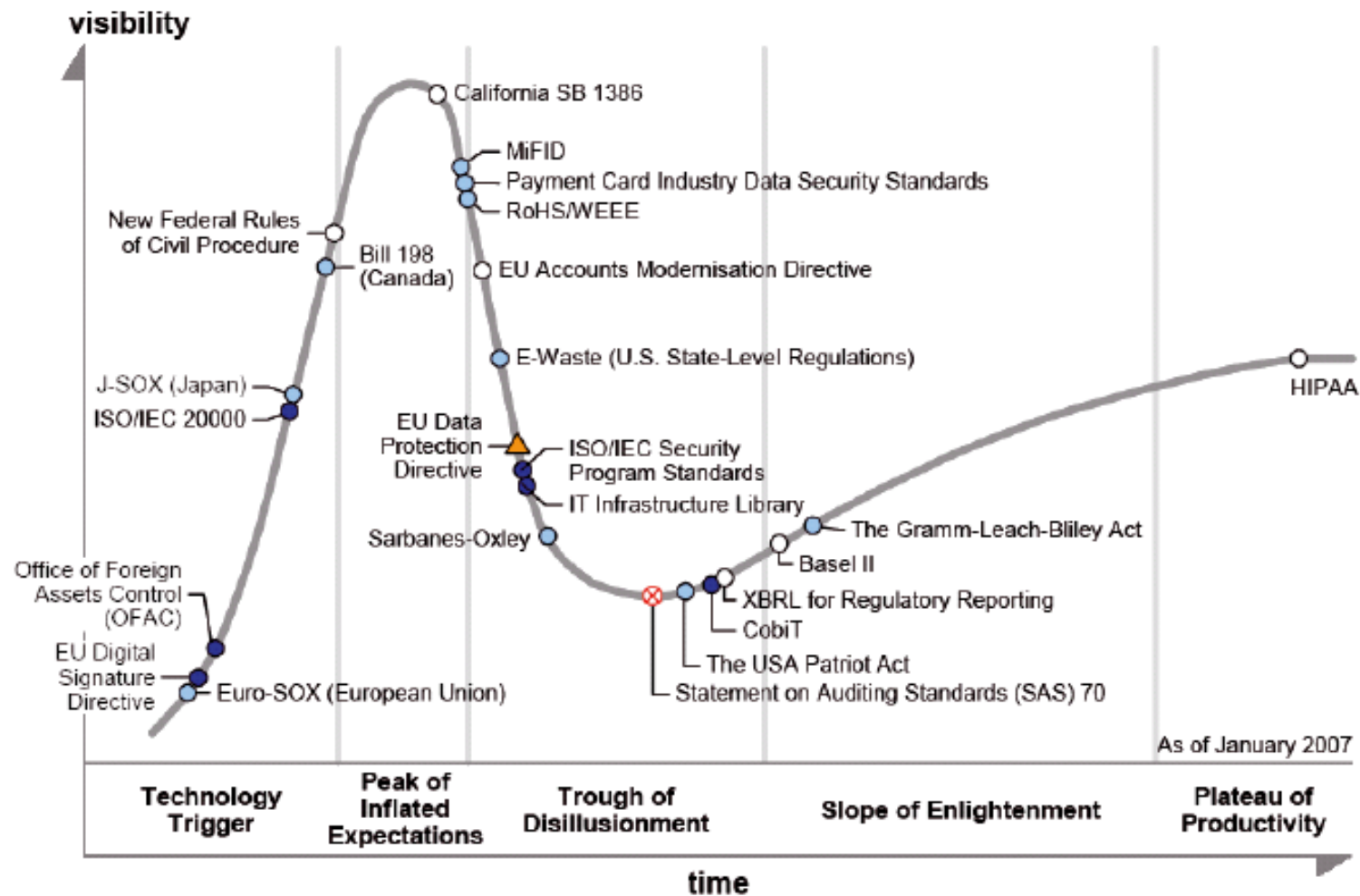


# System kontroli wewnętrznej (ICS)



Szczególną częścią wszystkich projektów wdrożenia zasad ładu korporacyjnego jest Wewnętrzny System Kontroli (ang. Internal Control System - ICS). System Kontroli musi zostać stworzony (lub dopasowany) w taki sposób, aby monitorował prawidłową realizację wymogów ładu korporacyjnego.

Figure 1. Hype Cycle for Regulations and Related Standards, 2007



Years to mainstream adoption:

- less than 2 years
- 2 to 5 years
- 5 to 10 years
- ▲ more than 10 years
- ⊗ obsolete before plateau

Source: Gartner (January 2007)



Dziękuję za uwagę!

Michał Kossowski

[michal.kossowski@boc-pl.com](mailto:michal.kossowski@boc-pl.com)