infosecurity® ISACA®
NORTH AMERICA EXPO AND CONFERENCE
20-21 NOVEMBER 2019

Andrej Volchkov

How to articulate the value of information security to senior management

#INFOSECNA

Volchkov
consulting

Objectives of the session

CISOs / CIO must provide reports to articulate the value of security and solicit decisions from senior executives.

This session aims to provide elements needed to develop pragmatic security reports for governance and management.

The objectives of the session are:

1. Reminder of the importance of business-oriented communication.
2. Proposition of some key indicators to be included in security report.
3. Presentation of an information security reporting template that can be used in your own company.

Importance of reporting for governance / management?

Good governance relies on reports based on **strategic indicators** to assess the IS program.

Security reports will only be taken into consideration if they use the **language senior executives understand** in a holistic approach.

Senior level security report helps:

- Bridge the gap between technical and managerial perception.
- Demonstrate IS value in business terms.
- Provide elements to respond to questions of BoD or Senior Management.
- Bring strategic indicators based on universally accepted units of measurement such as cost, risk, budget, strategy, targets, etc.

Short exercise:

Think of examples of security reports you are currently using for your senior management.

- Mention some key indicators you use in these reports.
- What are the main issues while reporting on security?

Some key Strategic Indicators for IS Report

Strategic indicators are high-level indicators or aggregations of operational metrics.

Strategic indicator	Give response to questions…
1. Security Strategy	How does IS strategy contribute to achieving global strategy?
2. Security Risks	What are the main security risks and how do they evolve?
3. Security Posture	What processes/controls need to be improved and why?
4. Compliance and audit	What is the status of fixing audit and compliance gaps?
5. Security Program	What is the adequacy of our security program?
6. State of Governance	What improvements do we need in our IS governance?
7. Security Costs	What comprises the security costs and how the costs evolve?
8. Progression towards Goals	What is the status in achieving our objectives and do we have to change something?

1. Security Strategy

The security strategy encompass:

1. Security strategic objectives
2. Initiatives that supports business and security strategic objectives

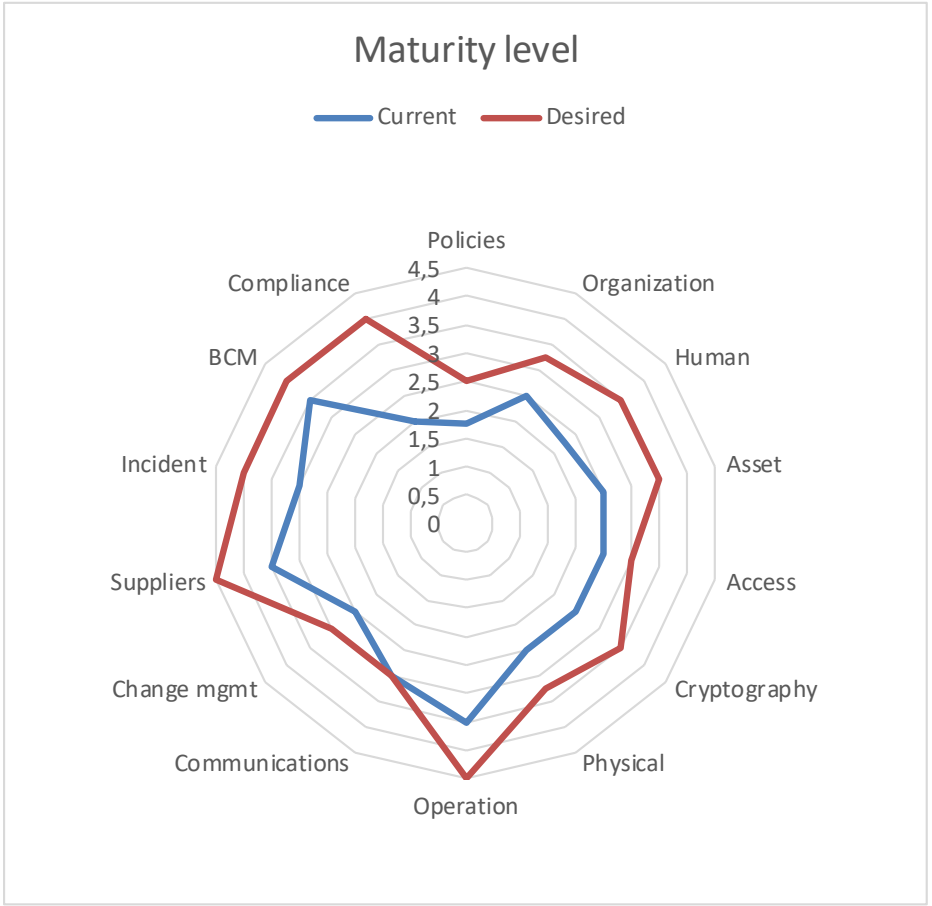
2. Security Risks

- Highlight the evolution of "High" and "Extremely high" security risks with Status and Actions Taken.

Risk	Residual Level	Trend	Key Indicators	Actions	Status	Planned Level
Extarnal fraud	H	↗	- Number of attempts - Damage suffered - Reaction time	- Awareness - Revision of guidelines - Means of detection - External coordination	According to plan 60%	M
Third party intrusion	H	→	- Penetration test results - External statistics	- Awareness - Elimination of vulnerabilities - Prevention improvement	According to plan 50%	M
Web server attack	H	→	- Result of penetration tests - Level of server updates	- Upgrade configurations	Late 20%	M
DDoS (Distributed Denial of service)	E	↗	- Obeservations in similar industry	- Migrate to DNS provider protection	Urgent	M

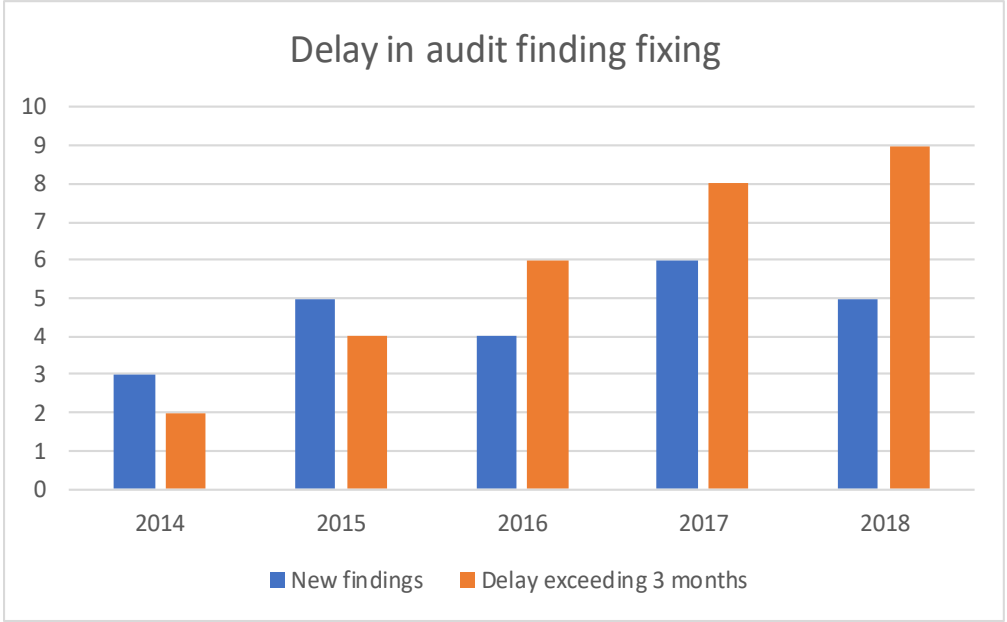
3. Security Posture

- Show, on one slide, the gaps between Actual and Desired state of IS Maturity.
- Maturity Assessment Process should be defined and explained.
- It can be conducted using some Maturity model, through a benchmarking study, by mandating an external audit, etc.



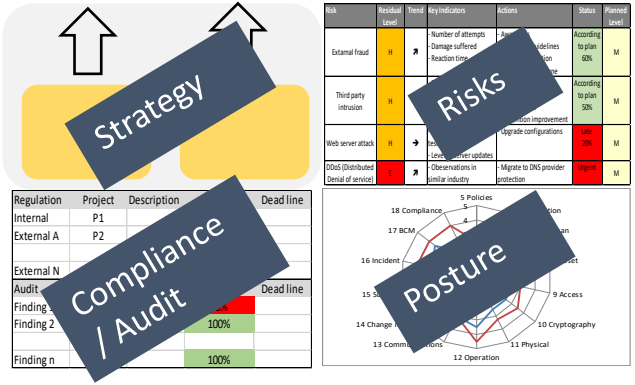
4. Compliance and Audit

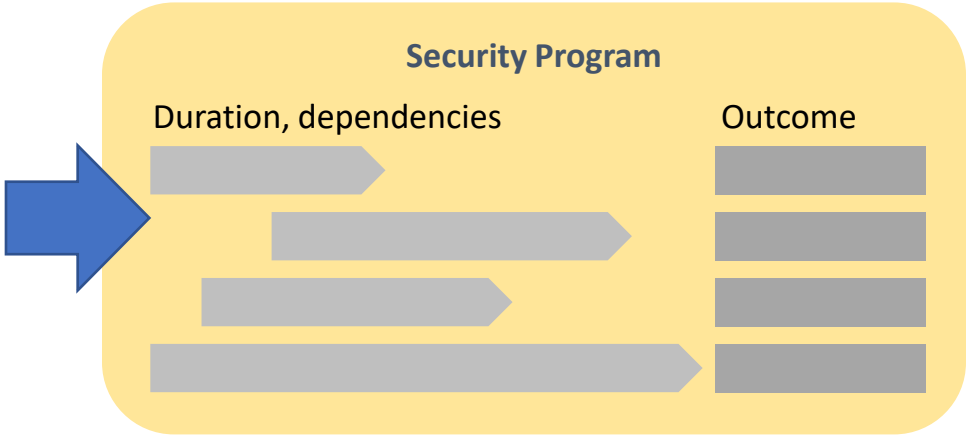
- Audit findings and Compliance gaps are easily understandable by senior executives.
- Remind the audience of some major corrective actions (and their costs).
- The delays in fixing the gaps can be used as indicators to foster decision by governing bodies.



5. Security Program

- IS program contains controls and projects (within strategic initiatives) to mitigate risks, improve maturity and bridge the gaps.
- Sometimes called: Business Plan, Road Map, etc.
- Respond to question: "What are we doing and why?"





6. State of Governance

Governance

Management

Operations

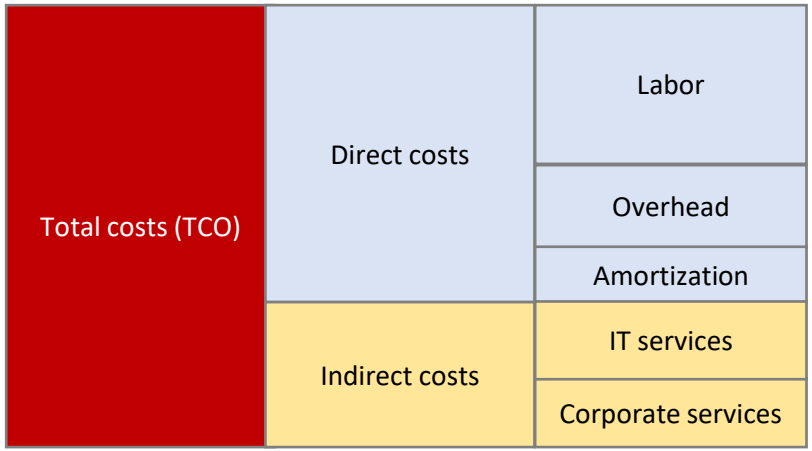
6. State of Governance

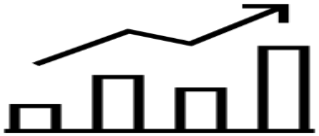
- Use a simple model to represent main IS Governance processes and their status (here: TLCF – Three Level Control Framework)

Policies ●	Strategy ✓	Organization / People ✗	Strategic Level
Risk mgmt ✓	Program ●	Reporting ●	Tactical Level
Asset mgmt ✗	Compliance ✓	Metrics ✓	
Security Operations			Operational Level

7. Security Costs Analysis

- Depicts the structure of IS costs using standard Cost Accounting principles.
- Explain the evolution over time and major changes.
- Compare trends (IT budget, IS budget, Overall budget, Headcount, etc.)

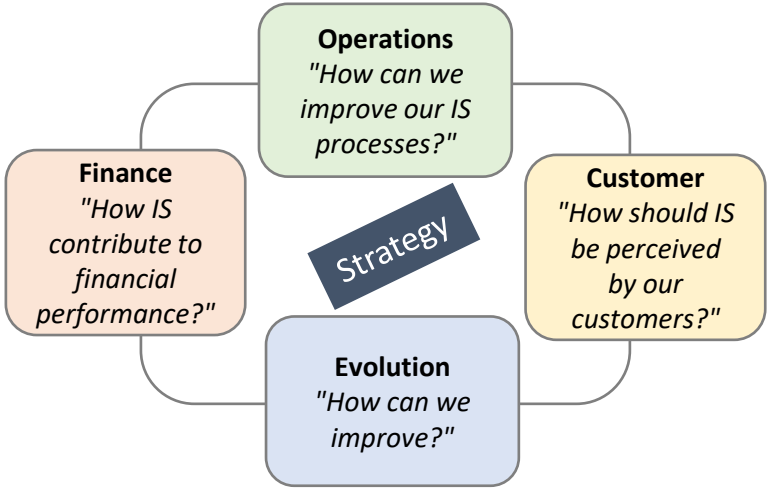




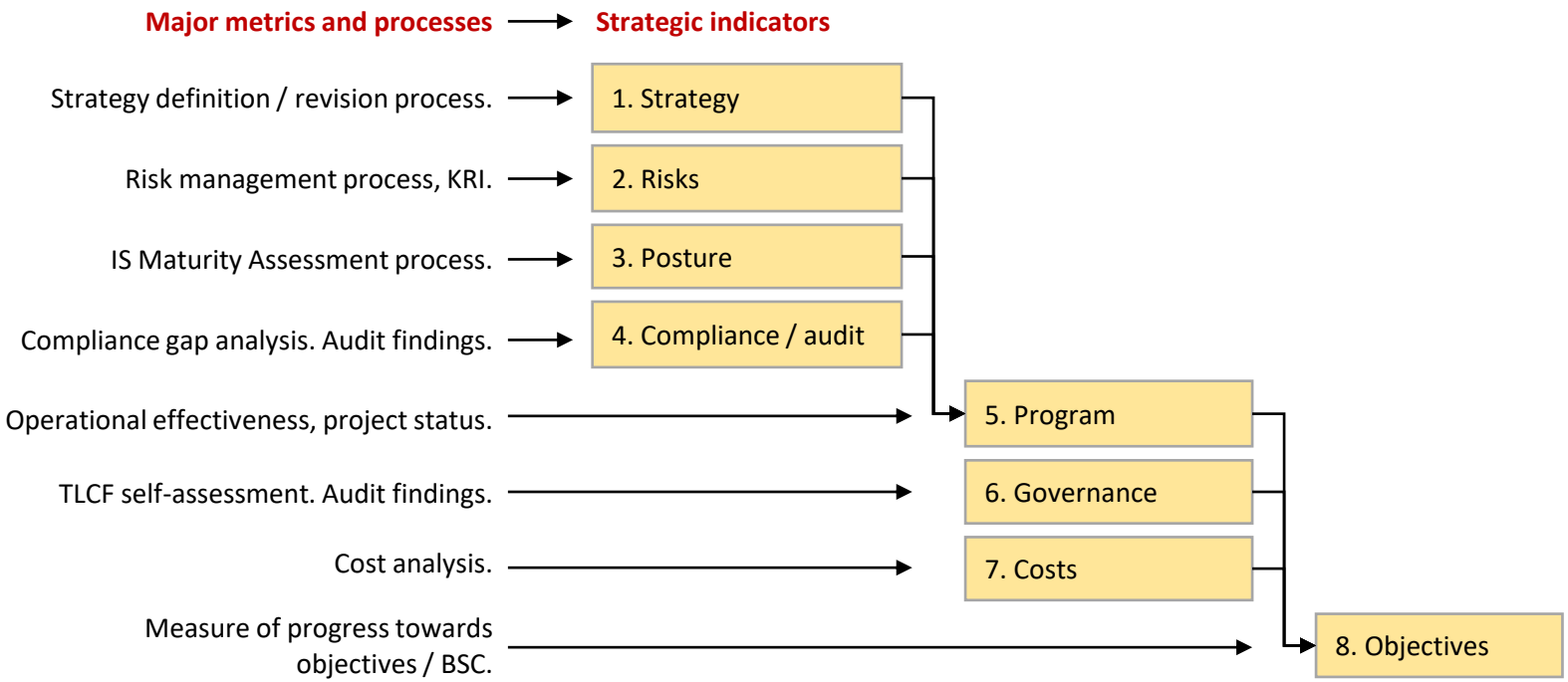
8. Progression towards Goals

- Use Balanced Scorecard for tracking IS objectives.

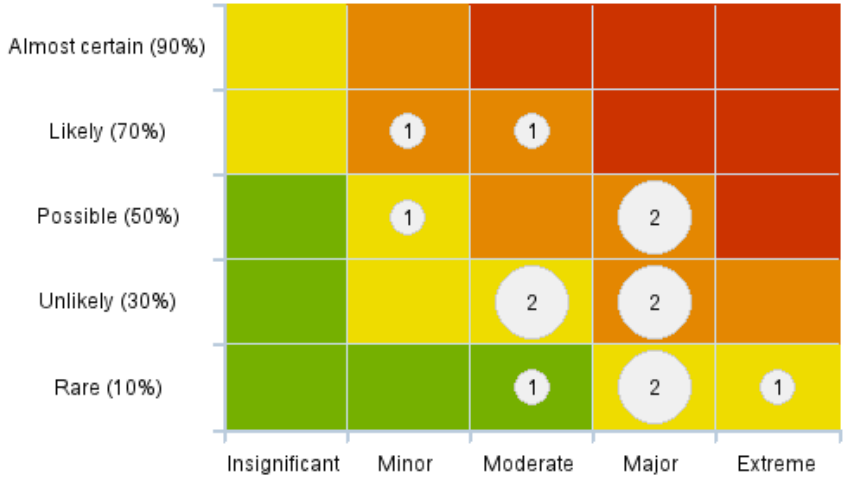
Perspective	Objective	Metrics
Finance	• Reduce x%	• Cost
Operations	• Detect • Enable	• Number • Ratio
Customer	• Delay • Strategy	• Time • Gaps
Evolution	• Policies • Awareness	• Evaluation • Readiness



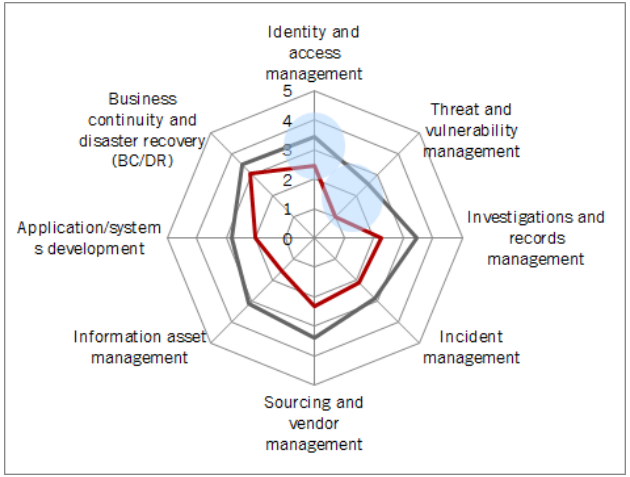
What metrics do we need to build Strategic Indicators?



Risks



Maturity



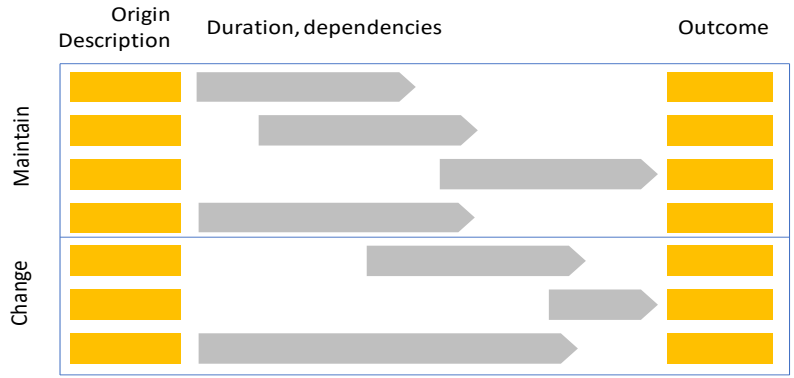
Strategic Initiatives

Initiative 1
Initiative 2
Initiative 3

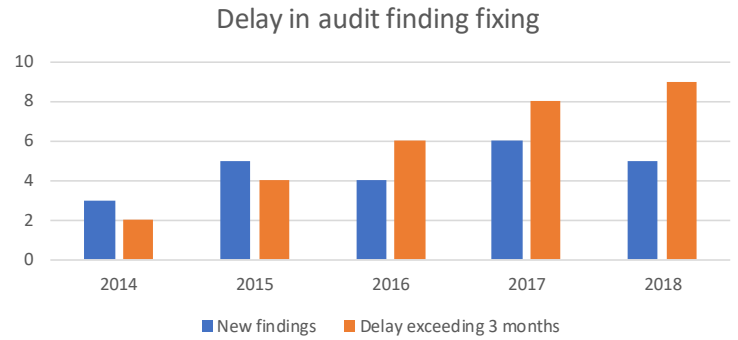
Strategy

Initiative 4
Initiative 5
Initiative 6

Program



Compliance



Gouvernance

Policies ●	Strategy ✓	Organization ●
Risks ✓	Program ●	Reporting ✗
Assets ✗	Compliance ✓	Metrics ✗

Security Costs

Security Costs (TCO)	Direct Costs	Work
	Indirect Costs	IT
		Corporate

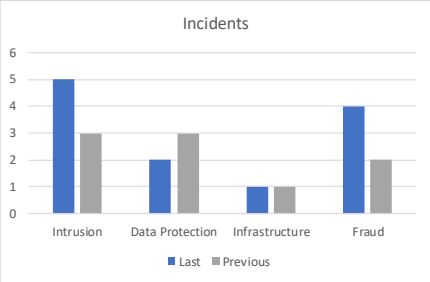
Short exercise:

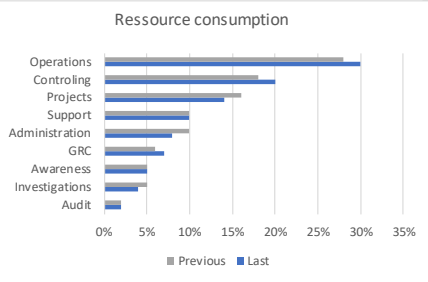
What kind of strategic indicator would you suggest for following purposes:

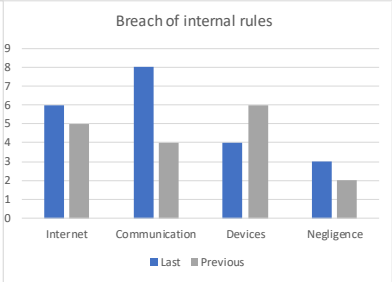
		Strategic indicator
1.	Demonstrate the alignment of security strategy.	→ IS Strategy (Initiatives)
2.	Explain the necessity to strengthen IAM processes.	→ Posture / Maturity
3.	Review IS team objectives.	→ Progression towards Goals
4.	Evolution (trends) in IS Costs.	→ Security Costs Analysis
5.	Justify security projects (business plan).	→ Program
6.	Provide a big picture of management / governance gaps	→ State of Governance
7.	Validate action plan to mitigate high risks.	→ Risks

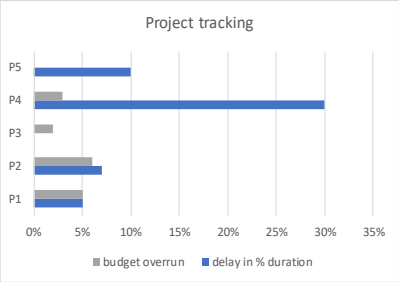
What is the difference (if any) between Report and Dashboard?

- Dashboard is primarily a real-time monitoring tool to track operational events (CISO / CIO).
- Report is designed for review purpose and decision making (BoD / Management)









TAKEAWAYS

1. *Provide business-oriented indicators.*
   Speak in the language senior management understand.
2. *Do "so what" exercise: your figures should stimulate decisions.*
3. *Be pragmatic in choosing strategic indicators: respond to real needs.*
4. *Don't try to use available (technical) metrics unless they clarify your statement.*
5. *If accepted by the management, security reports will become highly valuable governance and management tool to foster operations.*

Andrej Volchkov

www.volchkov.ch

avolchkov@volchkov.ch