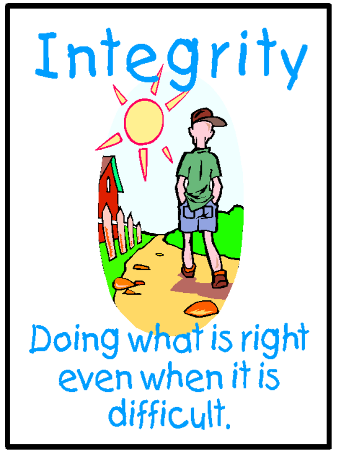
Bristol Bay
NATIVE CORPORATION ®

"Leading With Integrity"



What's all the hype about cybersecurity?

Business Data Confidentiality, Integrity, and Availability – The value proposition

BIG
BUSINESS IMPROVEMENT GROUP

Jim Bates: CEO Business improvement group

Jim Bates, LSSMBB, PMP, CISSP, CISA

- Master Certificates in Applied Project Management, Business Analysis, and Lean Six Sigma - Villanova University ~ currently earning MBA with JWMI
- Cybersecurity Expert
- 30 years professional experience:
  - IT Management – Former State of Alaska CIO
  - Business Consulting – Including F500s
  - Training, Coaching, Public Speaking - Nationwide
- PMIAK – Board Roles & PMP instructor
- Adjunct Professor, UAA

jlbates@go-big.com

(907) 854-6790

www.go-big.com

PMIAK President Elect

The Center For Technology – Executive Advisor

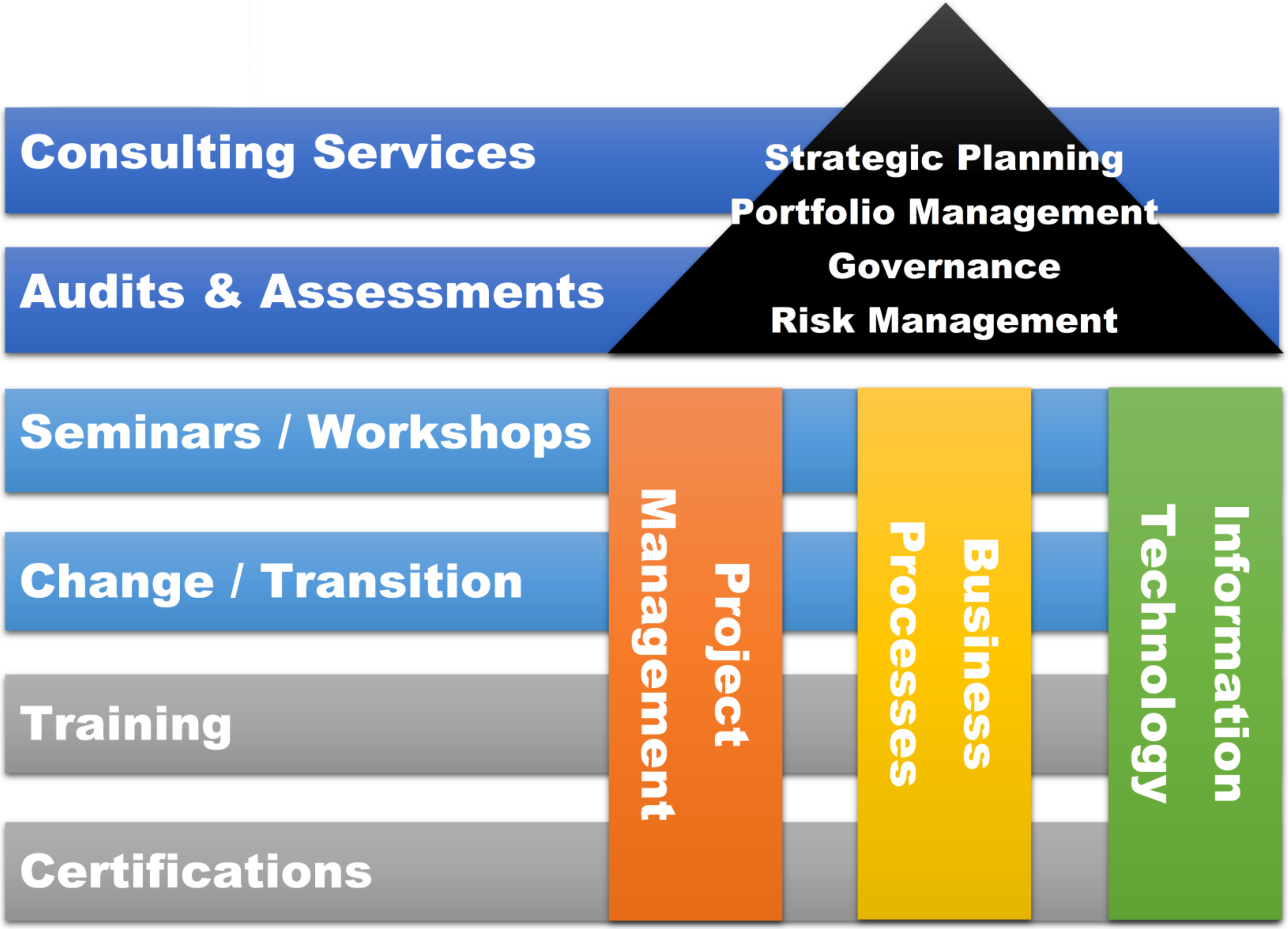
BIG

BUSINESS IMPROVEMENT GROUP

Founded 2010

Serving:

- Education
- Government
- Oil & Gas
- Utilities
- Native Corps
- Healthcare
- Manufacturing
- Transportation
- Technology
- Communications



Consulting Services

Audits & Assessments

Seminars / Workshops

Change / Transition

Training

Certifications

Strategic Planning

Portfolio Management

Governance

Risk Management

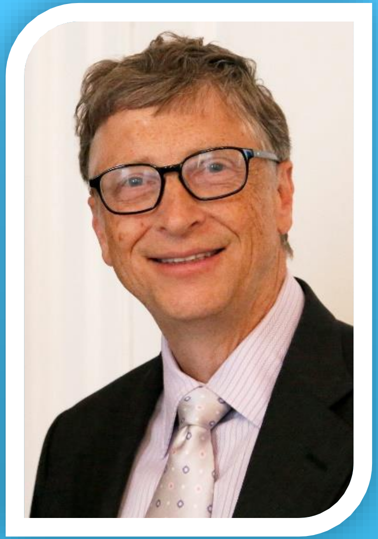
Project Management

Business Processes

Information Technology

“Information technology and business are becoming inextricably interwoven. I don’t think anybody can talk meaningfully about one without talking about the other”

Bill Gates – Chairman of Microsoft



$4.0B in potential costs from WannaCry ransomware attack that infected 200k computers in over 150 countries including 🇬🇧 🇷🇺 🇺🇸 🇮🇳

EQUIFAX

Category 5 breach compromises

145.5M

consumers' data

145.5M	209.0K
Names, Addresses, Social Security Numbers	Credit Card Numbers

$20.4B Total M&A Volume

$5.1B Total VC Investments

$6.5B

Private Equity ❤'s Cybersecurity

Blackstone, CLEARLAKE CAPITAL, EQT, FP FRANCISCO PARTNERS, ELLIOTT, LLR, MDP, MARLIN EQUITY PARTNERS, THOMA BRAVO, K1, WARBURG PINCUS

Physical crosses over to Cyber

ADT acquires DATASHIELD

7 Capital raises ≥ **$100M**

BlueteamGlobal	CROWDSTRIKE	cybereason
$125M	$100M	$100M

illumio	netskope	SKYBOX SECURITY	TANIUM
$125M	$100M	$150M	$100M

4.4x EV / Rev

Cybersecurity multiples continue to rise

SOPHOS	Qualys	TREND MICRO
101% ↑	83% ↑	49% ↑
RAPID7	splunk>	FireEye
35% ↑	34% ↑	32% ↑

3 IPOs

okta, SailPoint, ForeScout

Cyber IPO market rebounded to form

$1.4B

acquisition of Barracuda® by THOMA BRAVO

Barracuda goes private again after 12 quarters as a public company

26 MSSP M&A Transactions

DATASHIELD, esentire, morphick, open systems

Symantec led all acquirers

5 Acquisitions Completed

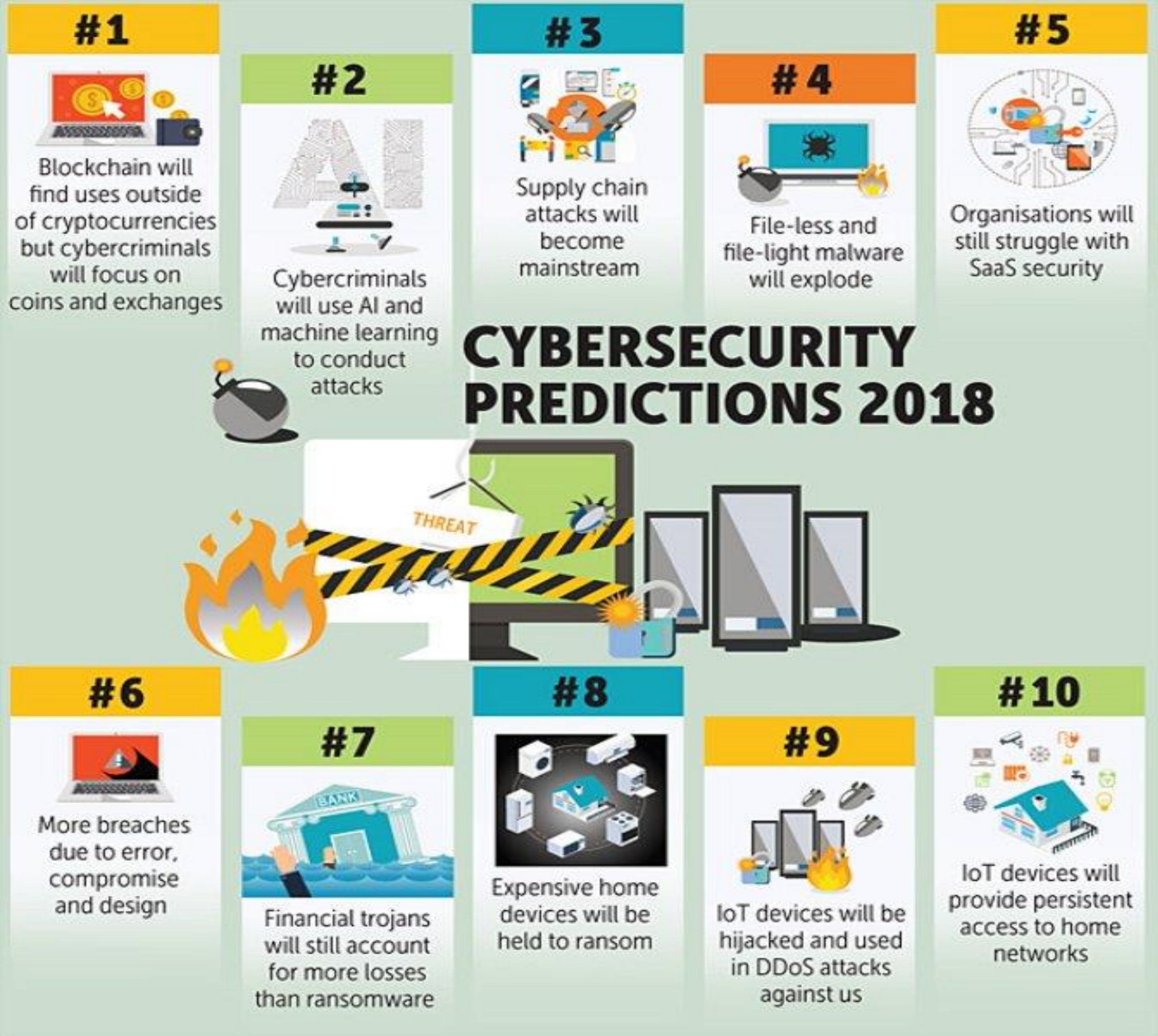
fireglass, Watchful, OUTLIER, Skycure, SURFEASY

$6.9B THALES bid tops

$5.0B AtoS bid for gemalto security to be free

.....2nd largest cyber transaction in history

Cyber Crime Focus



CYBERSECURITY PREDICTIONS 2018

#1 Blockchain will find uses outside of cryptocurrencies but cybercriminals will focus on coins and exchanges

#2 Cybercriminals will use AI and machine learning to conduct attacks

#3 Supply chain attacks will become mainstream

#4 File-less and file-light malware will explode

#5 Organisations will still struggle with SaaS security

#6 More breaches due to error, compromise and design

#7 Financial trojans will still account for more losses than ransomware

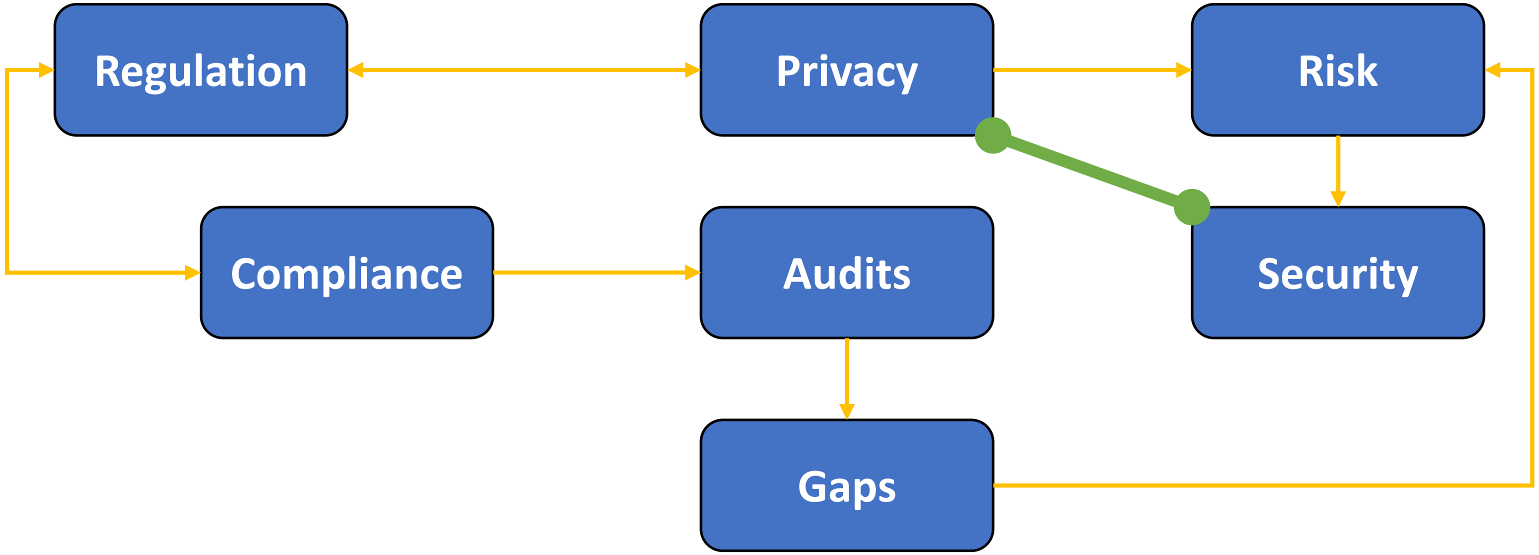
#8 Expensive home devices will be held to ransom

#9 IoT devices will be hijacked and used in DDoS attacks against us

#10 IoT devices will provide persistent access to home networks

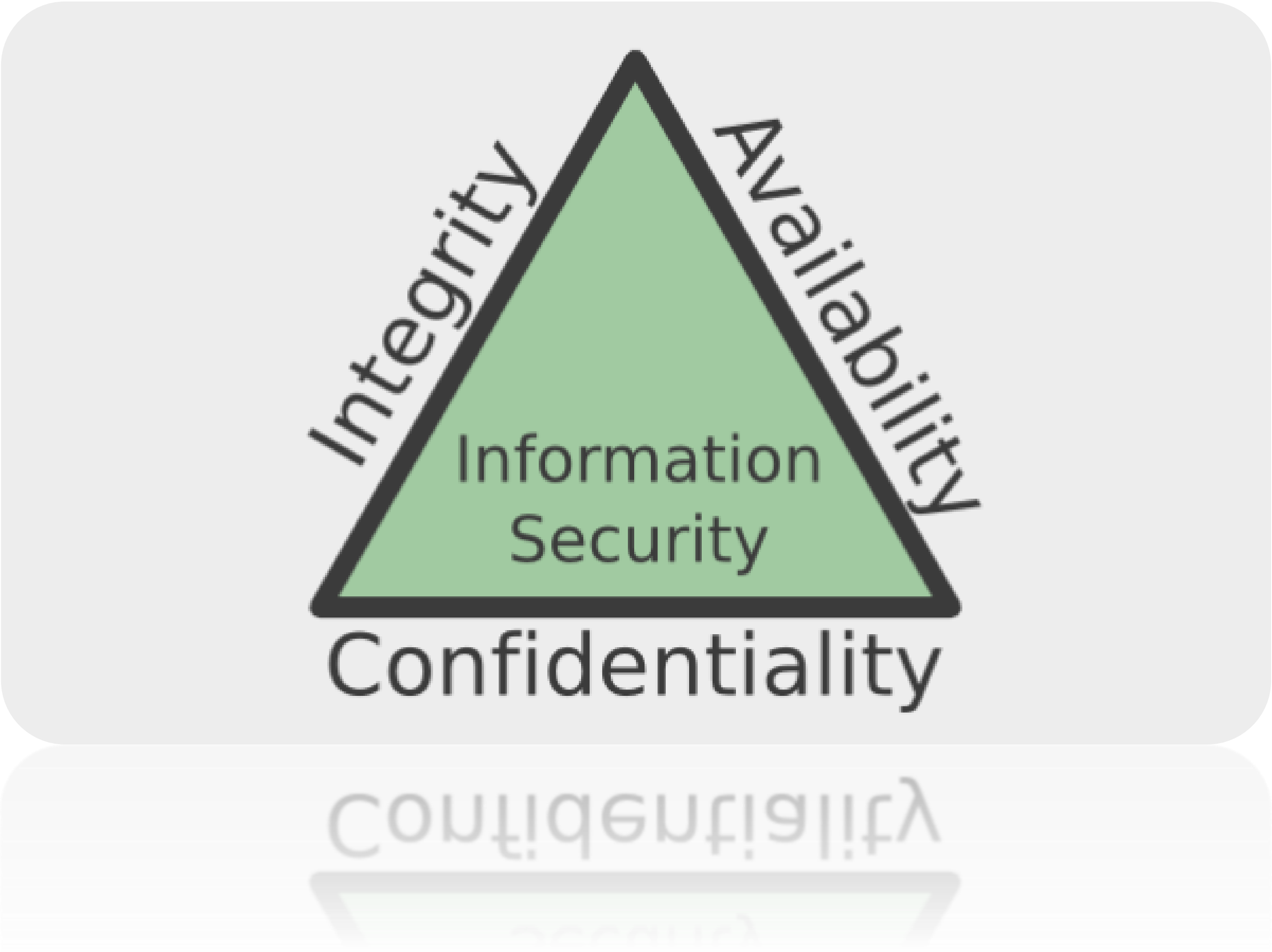
Events close to home

Regulation & compliance



Often organizations focus on being "compliant" in silos that have expertise for a specific regulation. Being compliant often means taking measures to avoid specific monetary penalties – a check-in-the-box approach.

What About Our Data / Information?



Privacy & Security

- Security and Privacy are intertwined. An organization cannot protect the **privacy** of confidential or personal information in its possession unless it maintains the **security** of the information.

- Organizations must protect confidential or personal information against both intentional disclosure in violation of an entity's privacy rights and inadvertent disclosure because of an attacker's unauthorized access to confidential or personal information.

A Hierarchy Of Data Categories

- Level 1
- Level 2
- Level 3
- Level 4

File Cabinet

Living Room

Safe

Cyber Compliance

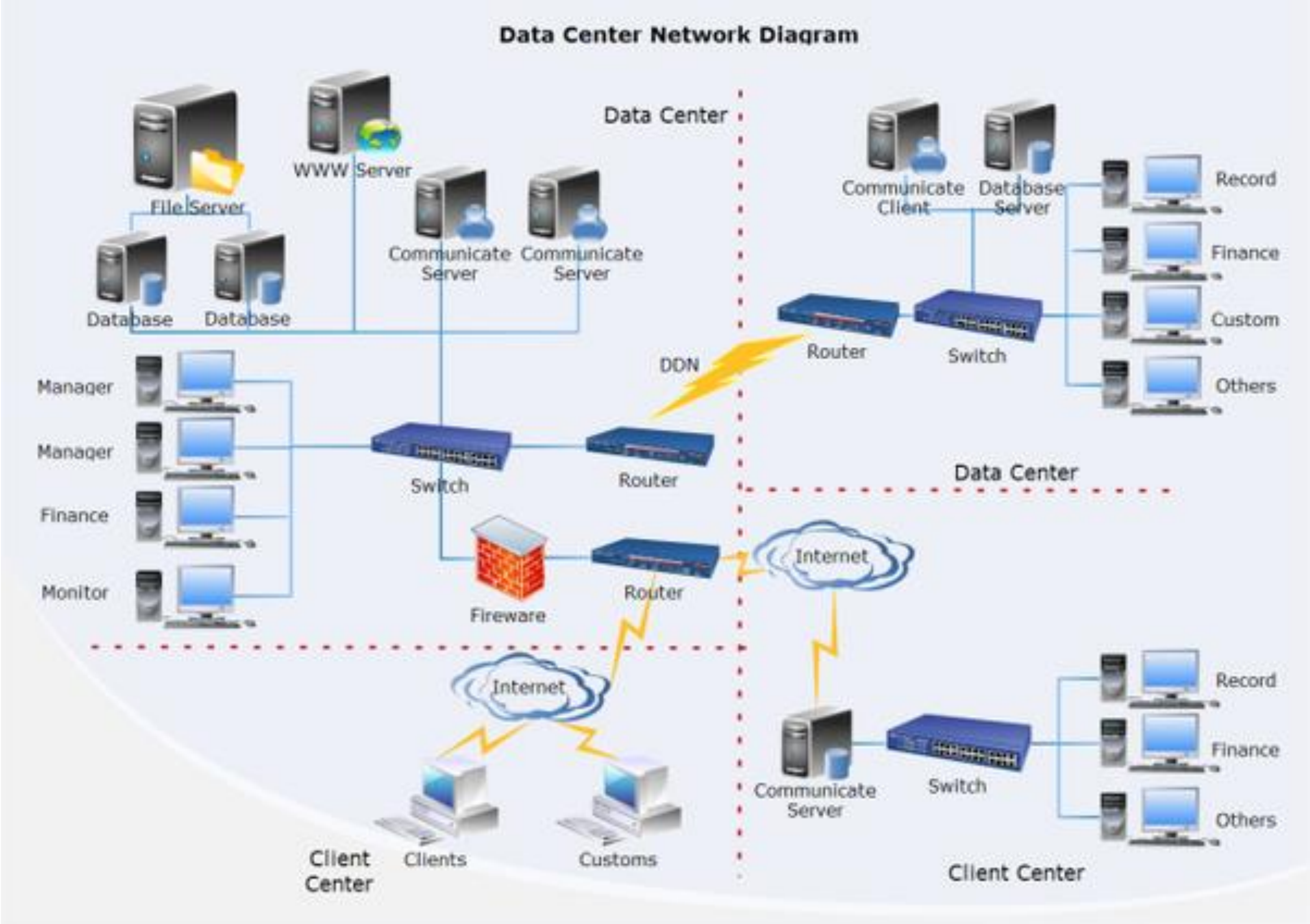
Comply with what? How fast is it changing?

- Financial Services Modernization Act, a.k.a., the Gramm Leach Bliley Act (“GLBA”)
- Health Insurance Portability and Accountability Act (“HIPAA”)
- Defense Federal Acquisition Regulation Supplement (“DFARS” – NIST 800-171)
- Payment Card Industry – Data Security Standard, Version 3.1 (“PCI-DSS”)
- The Sarbanes-Oxley Act (Sarbanes-Oxley or “SOX”)
- HHS 45 CFR 46 Protection of Human Subjects Subparts A-E
- Alaska Personal Information Protection Act § 45.48

Cybersecurity with Data Classifications

DATA:

- **Level 1**
- **Level 2**
- **Level 3**
- **Level 4**



User

Group

Minimum Standards & Data Classifications

DATA:

- Level 1
- Level 2
- Level 3
- Level 4

What are the Minimum Standards For:

- How we Store Data based on Classification
- How we Retrieve Data
- How we send Data
- Who can Access Data
- How we Respond to Incidents / Breaches
- How, When, and Where we Report

User

Group

A Better Approach

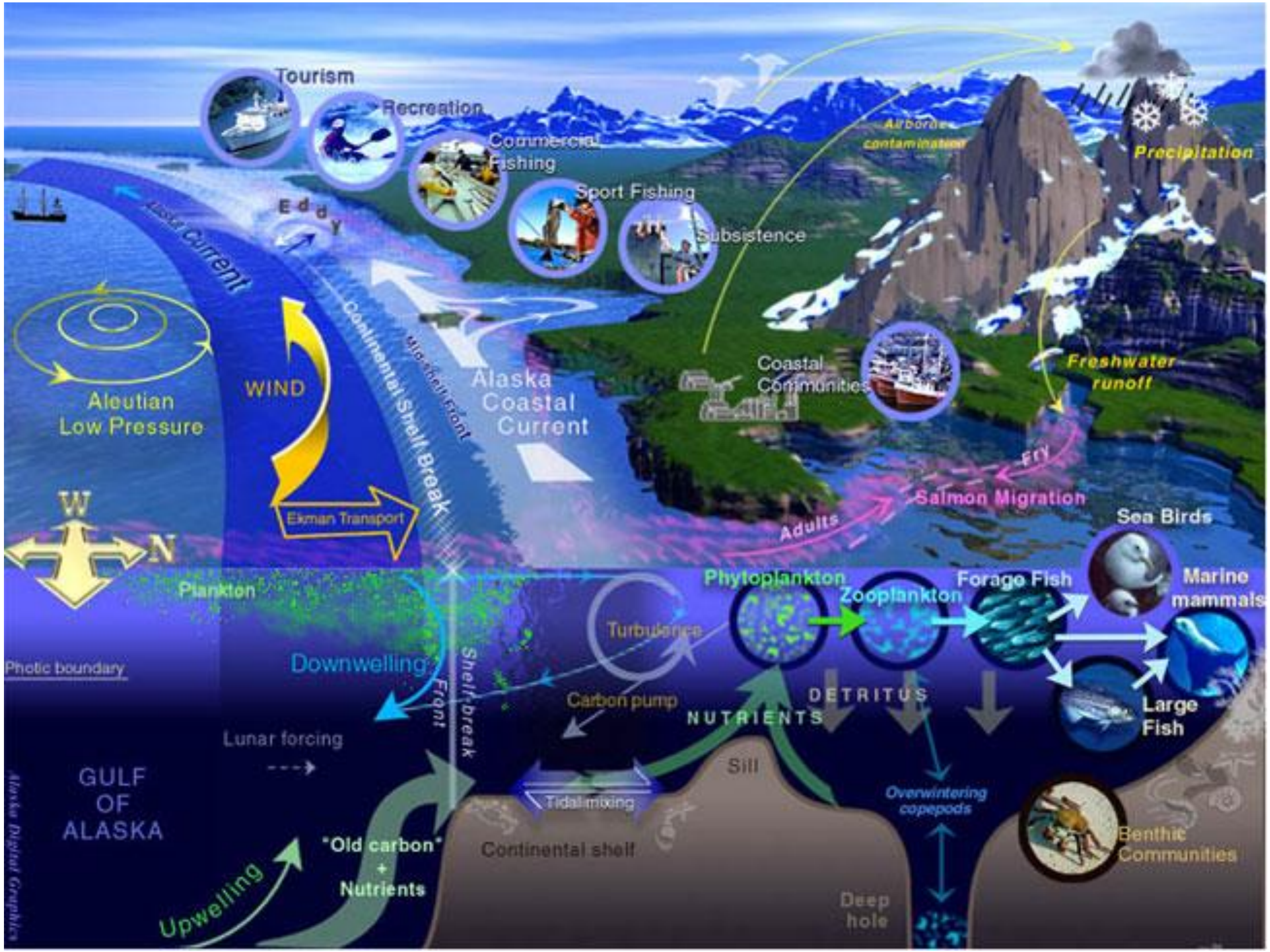
A more excellent approach is one that looks at the organization holistically and includes an **ethical** platform.

Often, the focus is on one set of regulation and commonalities are not leveraged. If “personally identifiable information” (PII) or “confidential information” is compromised, it is not only a question of compliance, but brand, reputation, and trust of the individuals and communities you serve.

An **ethical** **responsibility** to protect private/confidential information, regardless of regulation, emerges that surpasses regulatory compliance. This requires a robust cybersecurity strategy **that balances** with business requirements, investment, and risk management.

Ecosystems

A complex network of interconnected systems



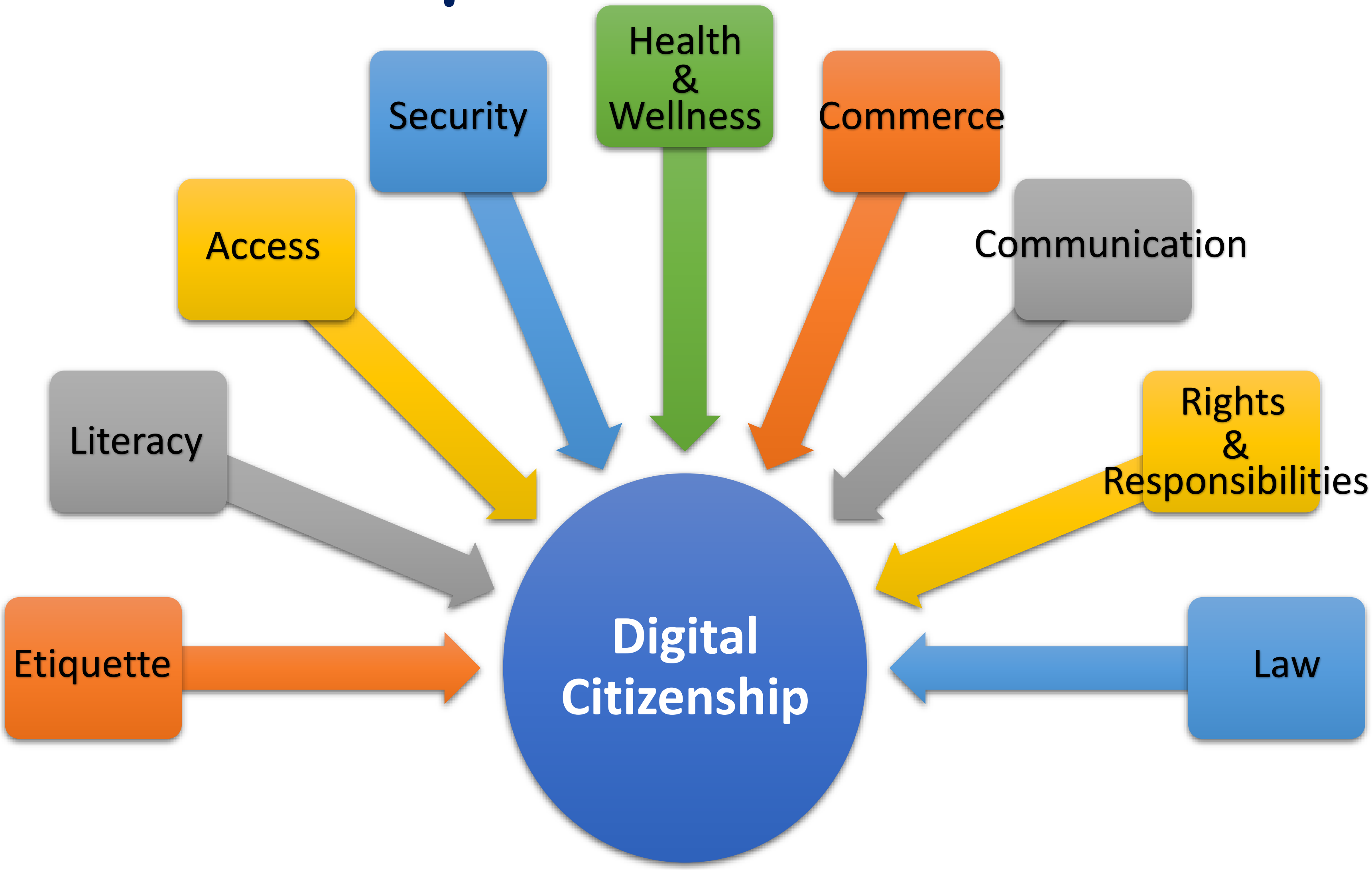
There is a Yup’ik term:

“upterrlainarluta”

Which Means:

“always getting ready”

Digital Citizenship



Etiquette

Literacy

Access

Security

Health & Wellness

Commerce

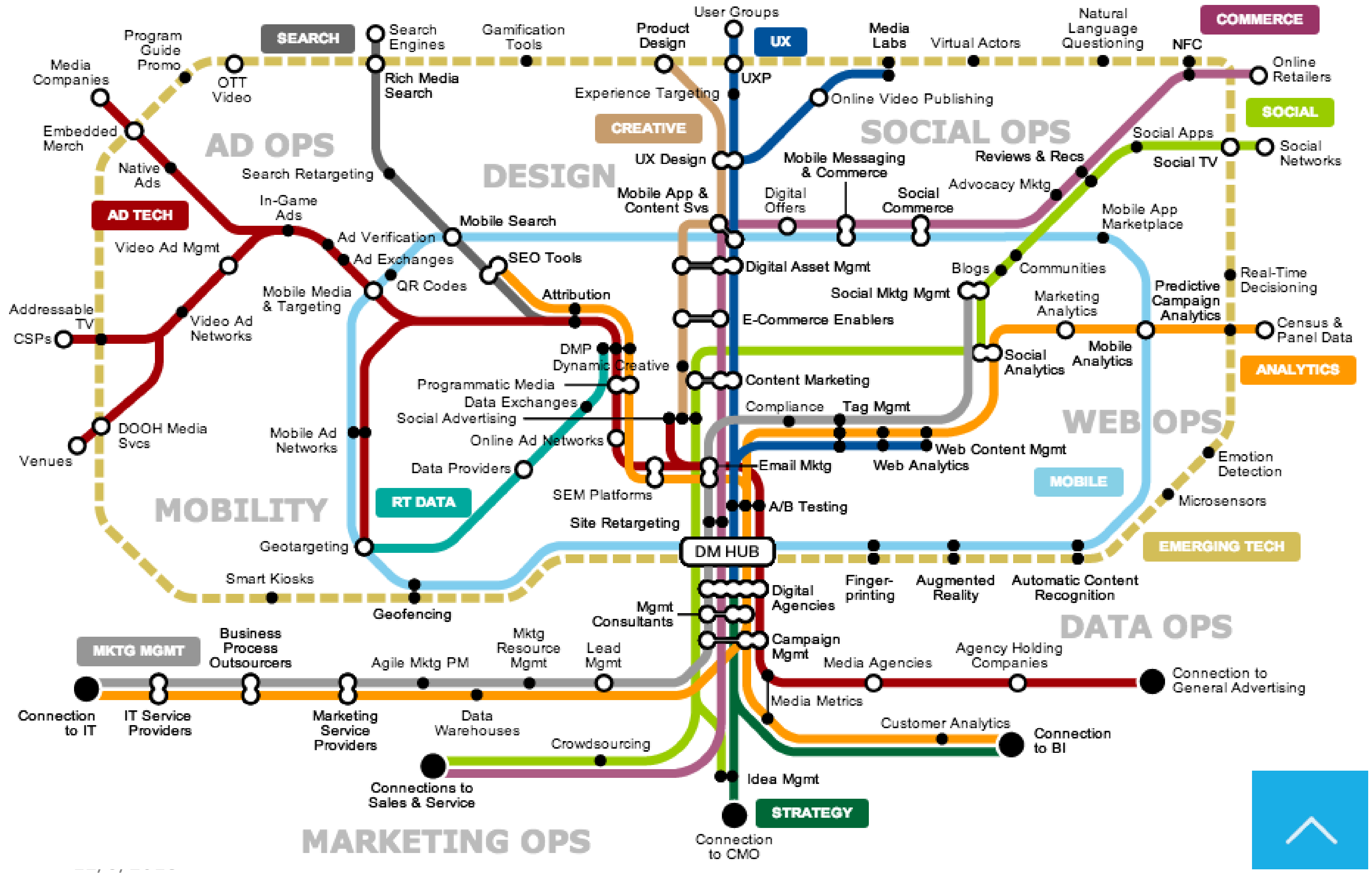
Communication

Rights & Responsibilities

Law

Digital Citizenship

The Complexity of Emerging Digital Ecosystems



Bristol Bay NATIVE CORPORATION®

BIG BUSINESS IMPROVEMENT GROUP

What Guides Us? What Do We Stand For?

Bristol Bay NATIVE CORPORATION ®

Our Mission: Enriching our Native way of life.

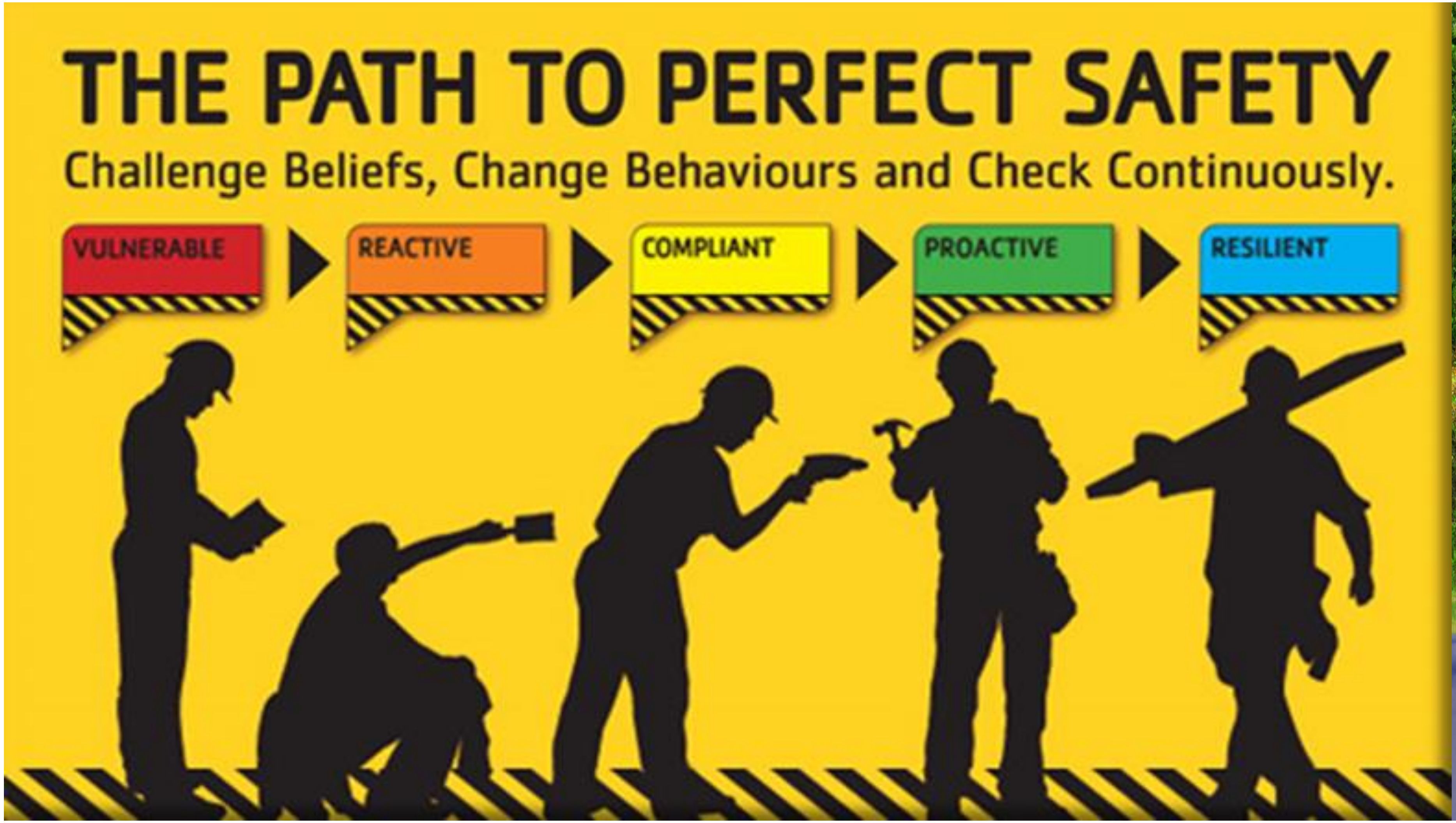
Our Vision: To **protect** the land in the Bristol Bay region, celebrate the legacy of its people, and **enhance** the lives of BBNC shareholders.

BBNC Statement:

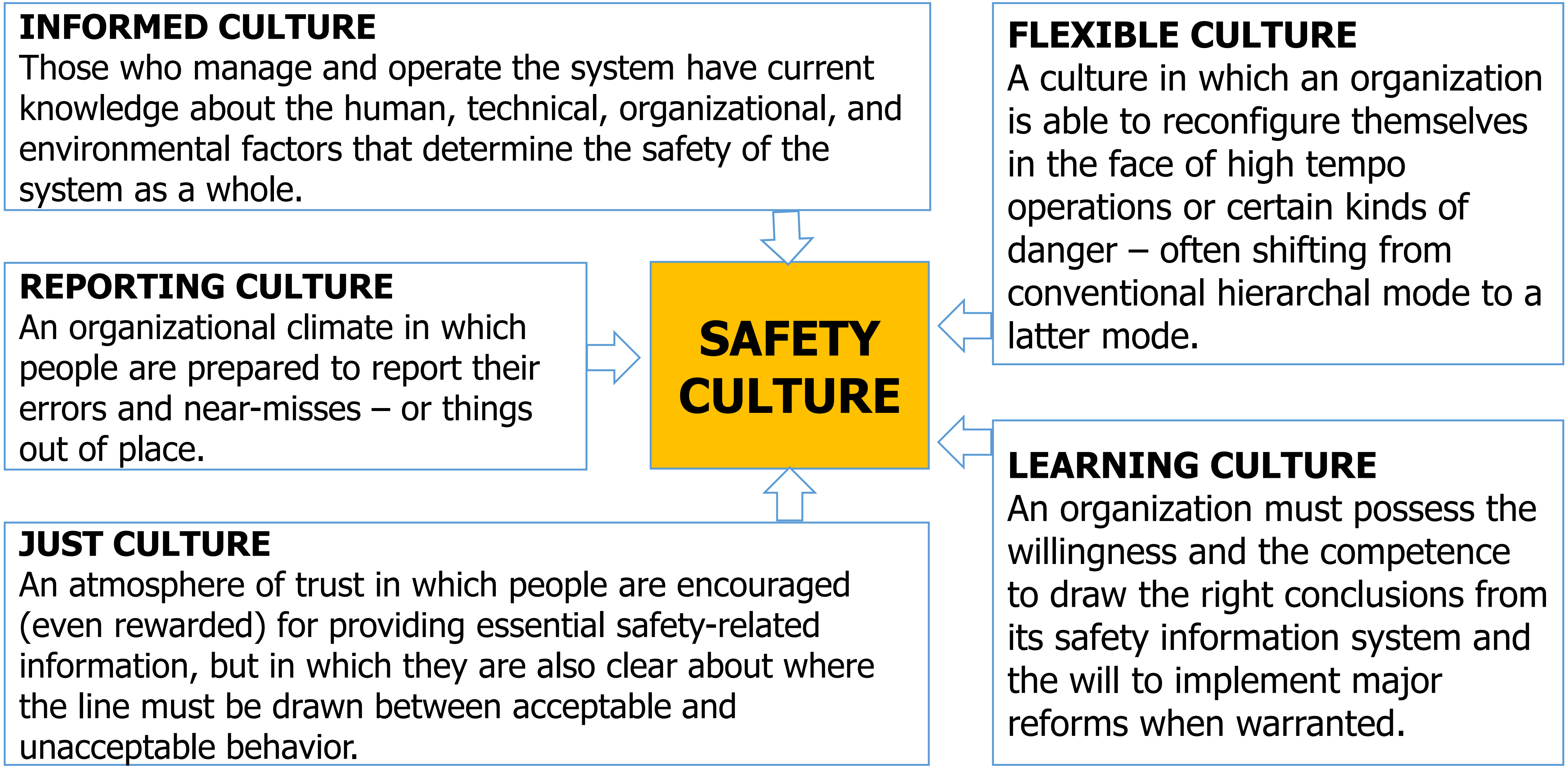
"It's not an accident that our forward-looking corporate **strategy** leads to the **greater good** of our shareholders. It's our **commitment**."

Bristol Bay
NATIVE CORPORATION ®

Comparisons To The “Safety Culture”


THE PATH TO PERFECT SAFETY
Challenge Beliefs, Change Behaviours and Check Continuously.
VULNERABLE
REACTIVE
COMPLIANT
PROACTIVE
RESILIENT

Comparisons To The "Safety Culture"



INFORMED CULTURE
Those who manage and operate the system have current knowledge about the human, technical, organizational, and environmental factors that determine the safety of the system as a whole.

REPORTING CULTURE
An organizational climate in which people are prepared to report their errors and near-misses – or things out of place.

JUST CULTURE
An atmosphere of trust in which people are encouraged (even rewarded) for providing essential safety-related information, but in which they are also clear about where the line must be drawn between acceptable and unacceptable behavior.

SAFETY CULTURE

FLEXIBLE CULTURE
A culture in which an organization is able to reconfigure themselves in the face of high tempo operations or certain kinds of danger – often shifting from conventional hierarchal mode to a latter mode.

LEARNING CULTURE
An organization must possess the willingness and the competence to draw the right conclusions from its safety information system and the will to implement major reforms when warranted.

How much safety is enough?
How do we decide?
Is there a minimum standard for safety?

480 VOLTS
DANGER HIGH VOLTAGE
DANGER
This Energy Source is LOCKED OUT!
This Lockout Device May Only be Removed by the Person Who Signed the Reverse Side.
Remarks:
DANGER
LOCKED OUT DO NOT REMOVE

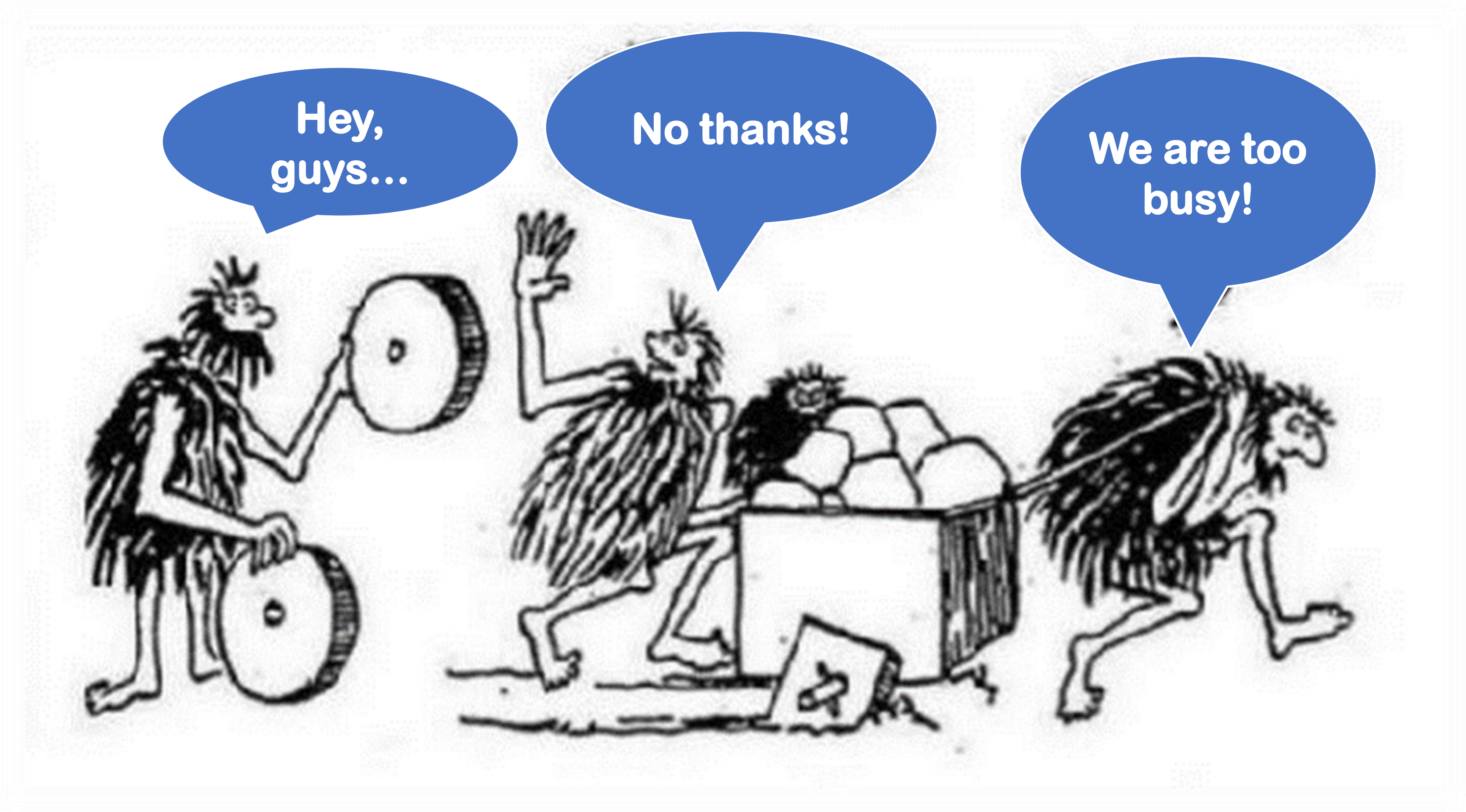
What Are Our Response & Reporting Requirements for Safety?

A Cyber Community – United We Stand

Bristol Bay NATIVE CORPORATION ®

A Place That's Always Been ™

What About Improvement?



How Do We Create Value?

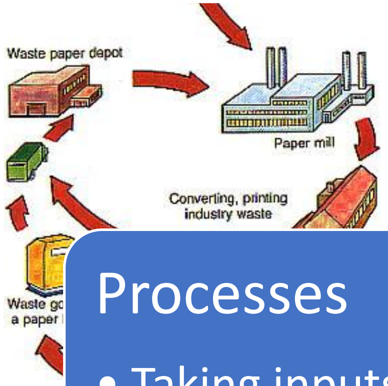
Your **People** depend on **Partners**, **Processes**, and **Products** to create **Outcomes** for your consumers. All 4 Ps must be looked at as potential areas for improvement in the value stream.

Partners

- Suppliers
- Sub Contractors

People

- Staff
- Faculty



Processes

- Taking inputs
- To make outputs

Products

- Technology
- Tools

Service and Service Management

- **Services:** Delivering outcomes that Customers value without them having ownership of cost and risk
  - Utility
  - Warranty
  - Asset/Resources

- **Service Management :** A set of specialized organizational capabilities for providing value to customers in the form of services

Service Value Creation – Other Factors

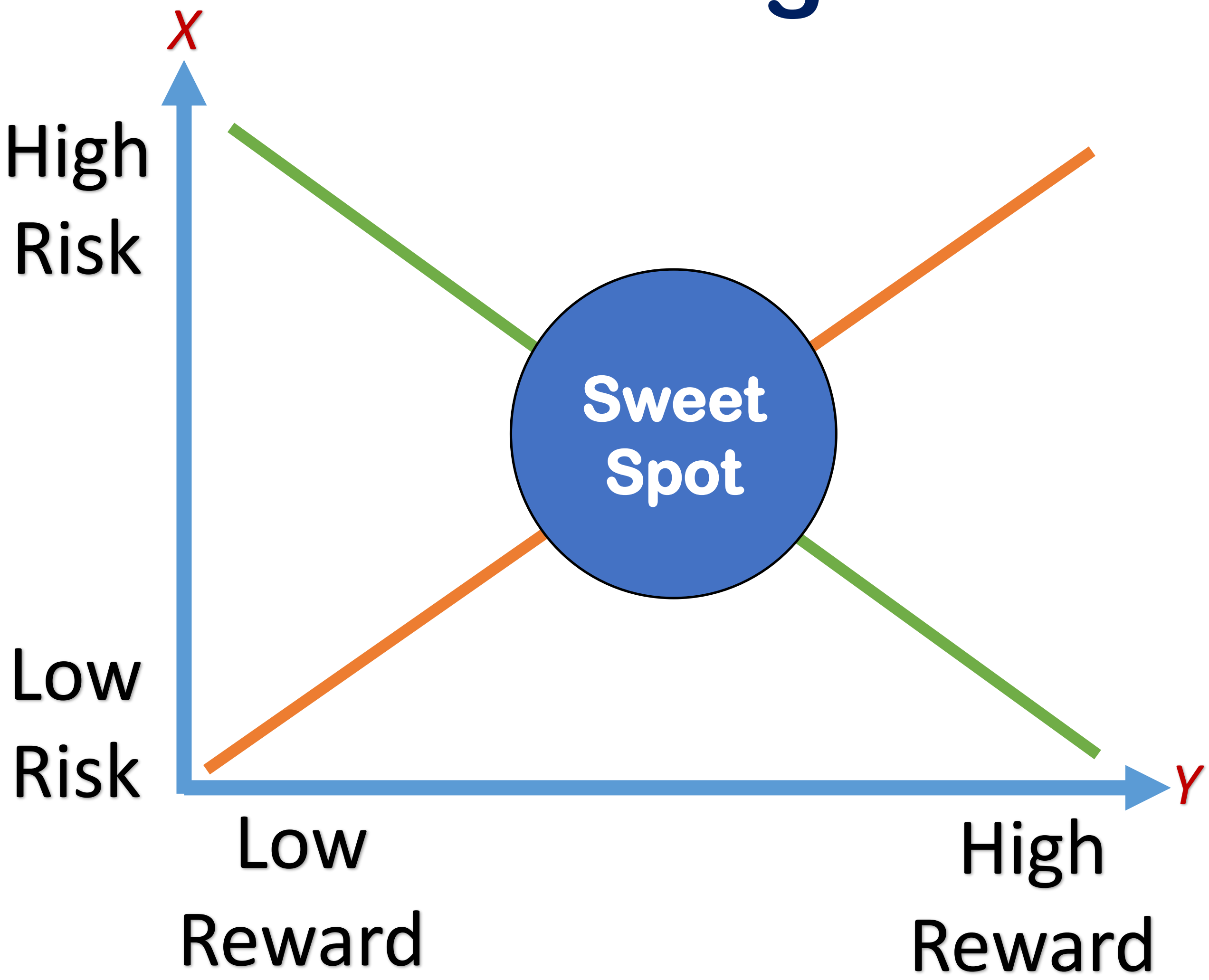
- **‘People do not want quarter-inch drills, they want quarter-inch holes’**
  Professor Emeritus Theodore Levitt
  Harvard Business School
- **‘The essence of strategy is choosing what not to do’**
  Michael E. Porter

Source: Iqbal, Majid; Nieves, Michael; Taylor, Sharon, ITIL Service Strategy, First impression, Published by The Stationary Office (TSO) for the Office of Government Commerce under license from the controller of Her Majesty’s Stationery Office, United Kingdom, © Crown Copyright 2007, page 31.

What About This “Risk” Management Thing?

- What does Risk Management mean to you?
- To your boss, shareholders, and/or customers?
- What is your organization’s risk appetite?
- How good has IT been at understanding this?
- Why do you think this exists?
- What can we do about it?

Finding the Balance



The Importance of the Risk Management Dialogue

- Corporate boards can no longer be content in solely hearing about metrics, resources, and compliance when evaluating corporate success.
- They must also consider what an organization is doing to protect the business’ **existence**, including its information assets, the risk to those assets and their criticality to ongoing business operations.

Every Business Has Risk

- What is the company’s risk appetite?
- Have threat and vulnerability assessments been conducted to evaluate company risk?
- Does the organization have the expertise and resources needed to reduce risk?
- Have mitigations (controls) and countermeasures been adequately deployed?
- What risk has the organization mitigated, removed, transferred, or accepted?

Takeaways

- Get engaged in your business purpose
- You’re in a relationship – communicate effectively and work together to build a cyber safe culture – united we stand.
- Measure the right things – those that align to the business purpose
- It’s more that just compliance – Remember ‘SAFETY’
- Understand risk holistically – communicate honestly