RisiAlbania
Partner for Growth

A project of the Swiss Agency for Development and Cooperation SDC

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Agency for Development and Cooperation SDC

Innovation for employment in Albania's ICT sector

Strengthening the ecosystem for the provision of information security services

In partnership with:

REPUBLIKA E SHQIPËRISË
MINISTRIA E FINANCAVE DHE EKONOMISË

Implemented by:

HELVETAS ALBANIA

PARTNERSALBANIA FOR CHANGE AND DEVELOPMENT

Author: Tim Sparkman

This document has been produced by RisiAlbania.
The views and conclusions contained here do not necessarily reflect neither those of the Swiss Government nor the Swiss Agency for Development and Cooperation SDC.

February 2021

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

This case study forms part of a series of analyses of RisiAlbania's market systems interventions in Albania's ICT, Tourism and Agricultural sectors. It focuses on Risi's efforts to take advantage of emerging changes in the market for information security services – namely, increased regulatory attention to cybersecurity and data protection in several areas of the Albanian economy – to spur process upgrades and generate significant job creation for young Albanians.

At the start of the interventions described in the report, Albanian actors were slowly moving to meet international standards regarding information security, which can be divided into cybersecurity (or protection from hacking threats) and data protection (or the safeguarding of client data from theft). Compliance with these standards was vital for protecting the existing market share of many financial service providers and other firms, as well as for positioning them to grow into new markets.

Risi first supported a government agency, the National Authority for Electronic Certification and Cyber Security (NAECCS), to produce bylaws and publicize new standards for information security. But it quickly recognized that a lack of capacity to help firms comply with NAECCS and other data protection standards meant that getting the enabling environment right would not be sufficient – it needed to go deeper to help a small number of local firms provide advisory and certification services. By pivoting to focus on two promising partners, LegalCert and InfoSecurity, Risi was able to kickstart a faster process of uptake as more banks, insurers, software developers and other companies moved to comply with information security standards.

The case study describes the analytical and partnering tactics Risi used to achieve its goals, resulting in four interrelated lessons from its work in this sector:

1. Adaptability – Risi's adaptive approach was vital for helping it test its assumptions and find stronger leverage points as it came to understand the information security market better.

2. Targeting – Risi's sharp, well-targeted activity took advantage of a new trend in increased regulation and quickly identified two key leverage points (LegalCert and InfoSecurity) that could accelerate change in the market, without undermining the market for these services.

3. Pivoting from Labor Demand to Supply – By starting with the demand for new skills before it pivoted to supply, Risi has put in place the elements of an ecosystem that can sustain its own growth.

4. Vision for the Future – Risi and the Swiss Agency for Development and Cooperation had the patience to invest in an important priority for Albania's long-term economic development, even though it did not promise significant impact until several years into the future. At that point, however, the intervention would create a very large number (potentially thousands) of decent, technologically enabled jobs, and would position the Albanian economy to emerge

as a competitive service hub with a sophisticated set of domestic players and a tech-savvy workforce that can compete in an increasingly globalized economy.

2 INTRODUCTION OF RISIALBANIA AND ITS CYBERSECURITY INTERVENTION

Context

Digitalization is a cornerstone of Albania's strategy for modernizing its economy. It offers strong potential for upgrading the operations of businesses of all scales, boosting productivity, improving market access and laying the framework for rapid firm growth. However, it also carries dangers, as digital networks that involve client information and access to payment systems are also vulnerable to cyber-attacks, an increasingly common theft tactic for criminal groups. A digitalizing economy signals investment readiness to the global market but Albanian businesses with increasingly sophisticated operations also need to amply demonstrate compliance with modern cyber security and data protection standards.

While there is no public record of any serious information security breach in Albania, the increased adoption of digital technologies for communication and operations management – from the nation's electric grid to its healthcare facilities, financial sector and public services – places information security high on the government's list of priorities. In response to the very real threat posed by malicious domestic and international actors, as well as pressure to comply with similar steps already taken in the European Union (EU), Albania in 2017 adopted a cybersecurity law that requires companies with critical information infrastructure to create positions for IT security staff and adhere to international guidelines laid out by the ISO 27001 standard (see box, right).

The law also granted the National Authority for Electronic Certification and Cyber Security (NAECCS) with authority for compliance oversight and the creation of by-laws to implement the new legal requirements. NAECCS used this authority to mandate the establishment of Computer Security Incident Response Teams (CSIRTs) housed within organizations designated as "critical and important information infrastructure operators."

This requirement acted as a trigger, creating strong incentives for a large number of actors to make significant new investments in cyber security. It required banks, insurers, hospitals and other firms to separate security-focused IT staff from the larger IT team, demonstrate compliance through the adoption of new standards (particularly ISO 27001), and invest in new hardware, software and auditing services that provide stronger defense against cyber-attacks.

ISO 27001 is an international quality standard developed to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system." Obtaining the certification guarantees that companies comply with the cybersecurity law. Companies certified in ISO 27001 undergo an initial audit and, if they pass, receive certification that is then checked annually for the next two years. After three years, companies need to go through the audit and recertification process again.

At the same time, the Albanian government was working toward adopting legislation that would harmonize its internal standards with the EU's recently adopted General Data Protection Regulation (GDPR), which established data protection standards for companies that served citizens of EU countries. When passed, this would require any company holding digital information about an Albanian citizen to demonstrate safeguards similar to the EU's GDPR rules. Meanwhile, the government had already established a High Commission for Data Protection under a more limited data protection framework.

There was just one problem: while there were many qualified IT personnel, there was very little human capacity in Albania to establish data protection safeguards and form the CSIRTs that build and maintain cyber security systems – let alone the capacity to build these systems within dozens (and eventually hundreds) of companies and government agencies. Without a significant investment in capacity building, it seemed unlikely that most actors would be able to comply with the new information security requirements in the foreseeable future.

However, **the flipside of that problem is a significant opportunity,** as the new regulatory environment also promised the possibility of creating hundreds of new, high-quality, technologically enabled jobs for Albania's young workforce.

3 RISIALBANIA

RisiAlbania is a project of the Swiss Agency for Development and Cooperation (SDC) implemented by a consortium consisting of HELVETAS Swiss Intercooperation and Partners Albania. The project's overall goal is to contribute to an increase in employment opportunities for young women and men (age 15-29) in Albania. Risi aims to achieve this goal by driving its interventions toward the accomplishment of **three broad outcomes:**

1. Enhanced growth and job creation by the private sector in the three selected subsectors of agribusiness, tourism, and ICT (labor demand),
2. Improved access to job opportunities and labor market information and services (intermediation), and
3. Improved skills of young people by improving the offer of private training providers in the three selected sectors (labor supply).

Risi pursues several lines of intervention within the ICT subsector, including supporting industry associations to improve access to information about the subsector, supporting non-formal training providers to build the ICT skills base among Albania's young workforce, and supporting ecommerce solution providers to expand their service offerings to non-ICT firms throughout the economy, among other activities.

As Risi learned more about the information security challenges facing NAECCS, the High Commission for Data Protection and the ICT subsector, it opened a new set of activities to respond to the opportunity to boost employment by promoting compliance with these new mandates. Thus, within its focus on cybersecurity and data protection, Risi developed three mutually supportive interventions:

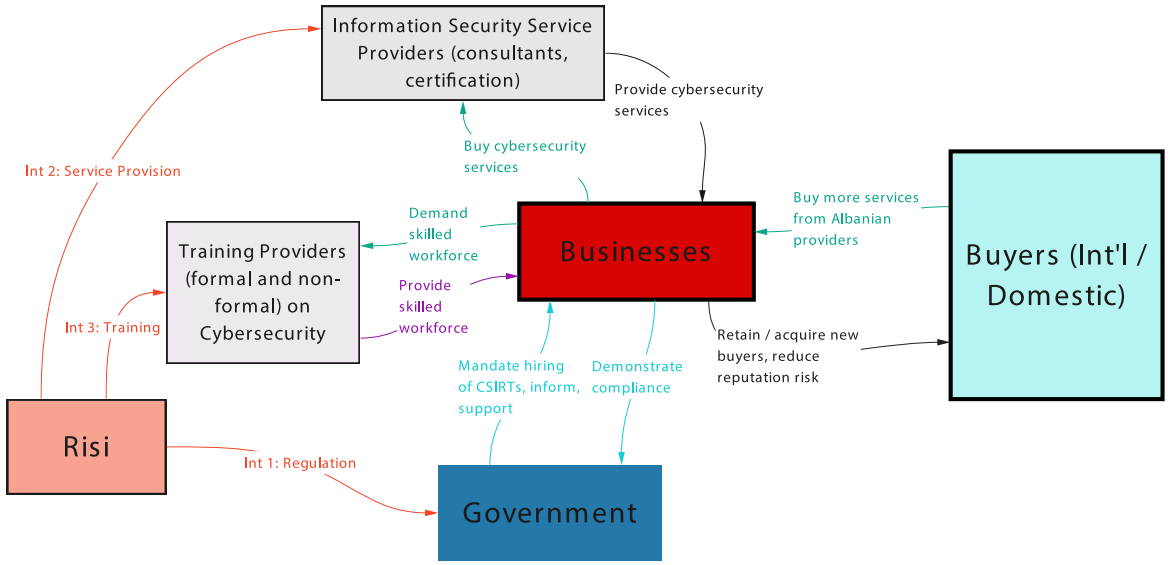
- **Intervention 1 – Regulation:**
Stimulating demand for cyber security services by working with Albania's National Authority for Electronic Certification and Cyber Security (NAECCS) to build a more robust regulatory environment that requires enhanced cyber security capacity within critical industries, such as banking and healthcare;

- **Intervention 2 – Service Provision:**
Supporting local service providers to develop cybersecurity and data protection advisory services (capacity building and auditing) that meet the increased demand created by greater oversight from NAECCS and the newly established High Commission for Data Protection;

- **Intervention 3 – Training:**
Preparing the workforce to meet increased demand for cyber and information security skills by working with non-formal training organizations and universities to develop and deliver relevant, modern training in this critical area.

The diagram below shows the complementarity of Risi's interventions. By helping NAECCS roll out more robust guidance on cyber security requirements (Int 1), Risi spurred demand for auditing and capacity building services. By helping Albanian businesses meet this new demand for auditing and capacity building services (Int 2), Risi further boosted demand for information security experts within those companies as well as boosting a much larger level of demand for experts within the industries affected by NAECCS regulation. Lastly, Risi recognized that it needed to plant the seeds for a new generation of information security experts to provide a ready workforce as more of the Albanian economy adopted digital business solutions, so it began raising awareness among universities and supporting non-formal trainers to devise and offer modernized cyber and information security training (Int 3).

Figure 1. Risi's Business Model for Influencing the Cybersecurity Market



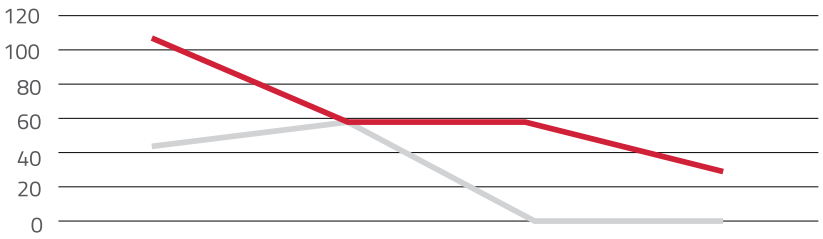
This case study focuses mostly on the first two interventions, as the third intervention started later and was therefore in an earlier stage of development at the time this case study was written.

4 THE MARKET SYSTEM FOR INFORMATION SECURITY SERVICES IN 2018

In partnership with NAECCS, Risi commissioned a **market analysis** in 2018 that assessed the supply and demand for cybersecurity skills and services in Albania. Completed by the end of 2018, the market assessment showed a stark deficit of capacity in almost all sectors, both public and private, with the sole exception of the banking and the telecommunications industry. Risi followed that analysis with a 2019 study examining the impact of implementing GDPR legislation on employment in Albania.

Within the private sector, the analysis estimated demand for IT security experts from surveys of 17 companies: 7 large international and local banks, 3 telecommunications operators, 3 insurance companies and the 4 largest private hospitals in Albania. The results are below – out of an optimal number of 257 IT security experts among these 17 companies, they currently only employed 107 staff. The telecommunications firms were far more advanced than the rest, with almost no expertise deficit, while banks employed less than half of the needed number of security experts and insurance and health-care companies employed almost none. Across all 17 firms, the assessment identified a deficit of 150 information security experts.

Report of current and optimal number of security employees in private sector (Risi's Market Analysis Report, 2018)



	Banking sector	Telephone companies	Insurance companies	Non - Publish health care
Current number	47	58	1	0
Optimal number	105	60	60	32

The public sector presented a wider gap. Out of seven government entities analyzed in the assessment, only the Bank of Albania, the Ministry of Interior and the High Inspectorate of Declaration, Audit of Assets and Conflicts of Interests had staff in their IT departments with training in cyber security. Only the Bank of Albania had a staff member that was certified in ISO 27001. Each of these three entities had about half the number of experts they needed to manage their systems in compliance with ISO 27001. Overall, none of the entities adhered closely to the security standards laid out by the 2017 law.

Between the lack of qualified experts and the low level of current compliance, the assessment made clear that raising the bar for information security in critical areas of the Albanian economy would take years and hundreds of newly trained technicians and auditors. To gauge **the workforce development system's capacity** to provide the experts that would fill this gap, the market analysis examined 8 IT-related faculties at 7 public universities and the IT programs of 9 private universities, at both the undergraduate and master's levels. It found that most of them were completely unprepared to provide the modern training that would build a qualified information security workforce. Most universities did not even have staff who could help develop the training.

Decent Jobs in the Information Security Market: "High labor market demand, salary, qualification opportunities, and ease of achieving qualifications, are… good reason[s] to seek certification as cyber security professionals."
Risi's Cybersecurity Market Analysis

The assessment proposed building new curricula for the two most in-demand profiles that were needed for placement within private companies and government agencies:

▪ **IT security technician** – responsible for building and managing IT security systems. Employers needed anywhere from a few to several dozen IT security technicians, depending on the size of their operations and the complexity and exposure of their systems.

▪ **IT security auditor** – responsible for providing advisory services and appropriate controls of information assets. Each employer needed at least one auditor.

To field these as quickly as possible, it proposed developing these qualifications at the master's level within universities, and also through non-formal training that could be accessed by mid-career professionals already working in Albania's IT sector.

5 THE PIECES RISI IS SUPPORTING – CHANGES IN PARTNER BEHAVIORS

By the time a **market assessment** that examined the impact that alignment with GDPR legislation would have on jobs was completed, Risi had a strong understanding of the constraints against, and opportunities for, building a more robust information security market system. The Risi team set about designing a set of interventions that would support the emergence of strong service providers and build the workforce needed for compliance with the 2017 cyber security law and GDPR alignment. The project focused on supporting three distinct actors: NAECCS, a Conformity Assessment Body called LegalCert, and a private cyber security firm called InfoSecurity.

NAECCS: While it waited for an Albanian IT security expert to conduct the market analysis, Risi immediately began supporting NAECCS directly to develop the administrative instructions that detailed standards for CSIRTs and staff training for companies to become compliant. Risi also paid for the cost of training NAECCS staff on ISO 27001 and other aspects of the new cyber security law. With its own resources, NAECCS also developed a system for incident reporting, by which any actor in Albania could inform the agency about a security incident.

Once the market assessment was finished, NAECCS used the information on labor supply and demand to begin cooperating with the Ministry of Education around the development of new cyber security-related curricula for university undergraduate and master's programs (Risi's third cyber security intervention area).

LegalCert: When it approached Risi in 2020, LegalCert was a Tirana-based firm that helped companies comply with a set of common international standards: ISO 9001, covering quality management for any product or service offering; ISO 14001, covering environmental management, and ISO 45001, covering workplace health and safety. It had a network of around 30 Albanian and Italian audit professionals that it used regularly and was looking to

build more capacity within the country. The legal representative of LegalCert, Alfisa Shahu, saw the opportunity created by the new GDPR law to be approved by the government in end of 2020, which would require companies working with EU citizens' data to be GDPR compliant. A new standard concerning GDPR compliance, 27701, an extension of the existing standard 27001, was developed by international consultants to certify companies on GDPR compliance. Hence, LegalCert applied to Risi for financial support to train a network of freelance auditors in ISO 27001 and focus on 27701, as the standard that would demonstrate business compliance with both cybersecurity and data privacy regulations.
Risi helped LegalCert by covering 40 percent of the cost of an international expert to train and certify 10 Albanian consultants. Due to the conditions caused by the COVID 19 pandemic, the training took longer to organize than expected and was conducted online. However, by the summer of 2020 all 10 of the consultants – five men and five women – had completed the course and were beginning to offer their services in the Albanian market.

At the same time, LegalCert received authorization from Albanian's High Commissioner for Data Protection to provide data protection certification mechanisms and data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of Processing Operations. The authorization essentially means that LegalCert's certification of compliance for its clients is taken more seriously by domestic and international counterparts. Because ISO certifications serve to signpost the safety and quality of an entity's operations, having an actor like LegalCert authorized to provide this level of certification for Albanian companies was an important step in establishing the international legitimacy of ISO 27701 compliance certified by Albanian experts.

InfoSecurity: In early 2019, as a small IT security firm in a nascent market, InfoSecurity had a strong idea of the potential for growth and an equally strong understanding of the barriers to realizing that growth. After all, its founder had conducted Risi's cybersecurity market analysis. What he lacked was a team with internationally certified capacity and name recognition for his company.
InfoSecurity provides a basic set of four services that help IT-using companies establish and maintain robust cyber security protection:

- **Penetration testing** – simulating cyber-attacks to explore weaknesses in a client's cybersecurity system.

- **Forensic audits** – in the wake of a cyber-attack, following the trail left by attackers to uncover data thefts or other exposures.

- **Security auditing** – validating existing cybersecurity policies and procedures.

- **Security awareness and training** – building client capacity to maintain proper cybersecurity systems.

Risi knew that there was no other actor in the local market that specialized in these services apart from the Big Four and regional companies. Nevertheless, the project issued a competitive tender, and selected InfoSecurity as a partner after reviewing all available options. It moved forward with a package of support for InfoSecurity to cost-share training for its in-house experts (addressing the capacity issue) and cost-share the expense of marketing its new services in Albania (addressing the name brand issue).

With Risi's help, five InfoSecurity staff attended online trainings and obtained certifications from various international training centers on ethical hacking, CISCO security, MicroTik security, LINUX security, ORACLE and MicroSoft Security certifications, such as Windows Server Security or Azure Security. Unfortunately, two of the trainees promptly emigrated with their freshly certified skills, but the other three remained.

"Signaling is important," Mr. Tafa says. Albania (in addition to some of its neighbors) suffers from a bad reputation generated from "a few bad actors" who have perpetrated cybercrimes, including information theft. Because of this, Risi also helped it collaborate with NAECCS which granted InfoSecurity access to the agency's international networks, an essential step for building a solid reputation. "What can you do?" he asks, "we're trying to do our best." Infosecurity also had the opportunity to share the results of the cybersecurity market assessment to industry stakeholders, including IT-focused training centers, during a NAECCS-sponsored event.

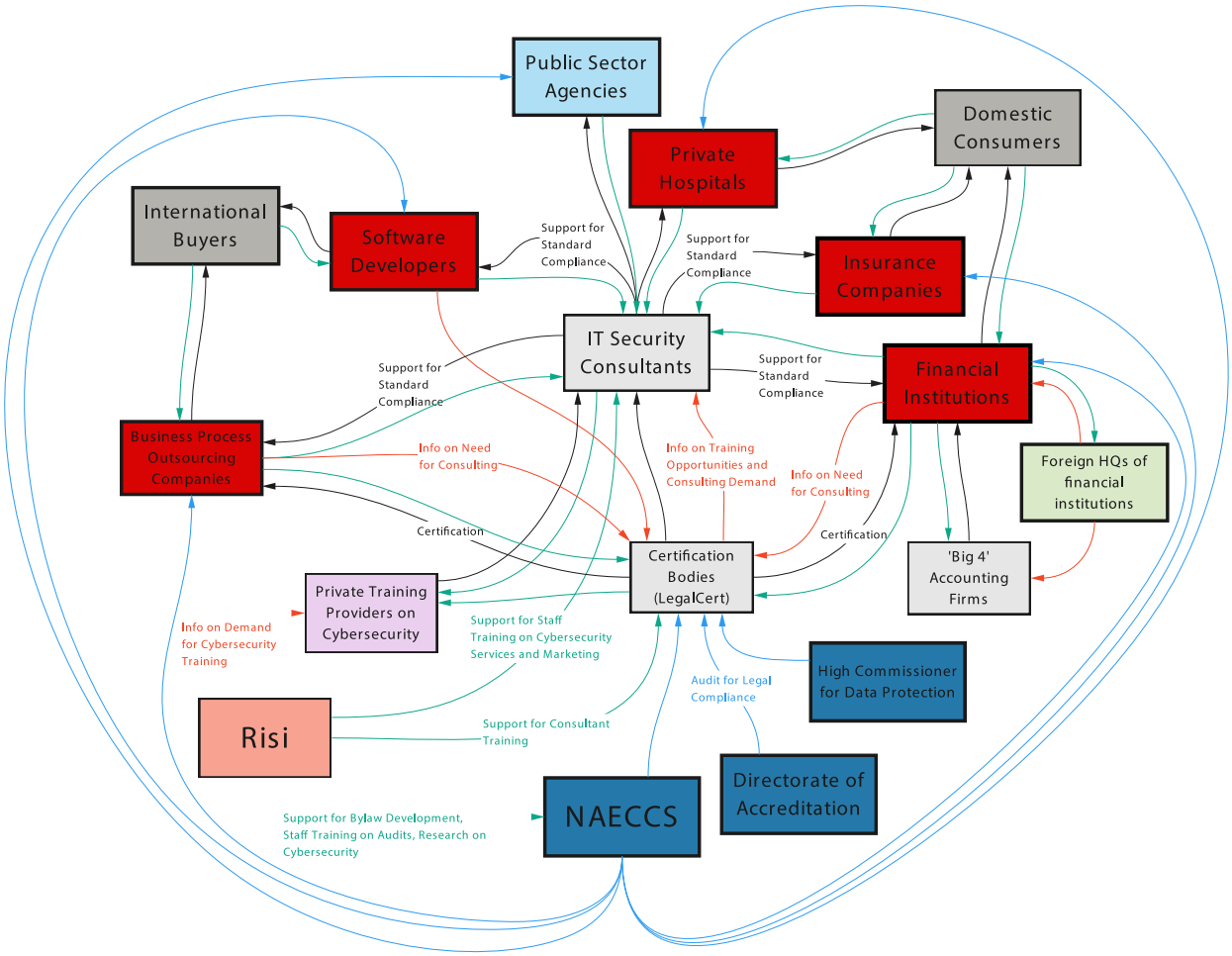
Beyond cost-sharing training and marketing for InfoSecurity and LegalCert, in addition to the abovementioned support to NAECCS, **Risi did not provide any additional financial support for specific client engagements**. It did not distribute vouchers for their services or in any other way subsidize the consulting and certification costs for their clients – after all, its analysis never identified willingness to pay for these services as a constraint. Instead, with these pieces built into the ecosystem, it allowed the market to progress at its own pace.

6

SIGNS OF CHANGES IN SYSTEM PERFORMANCE – THE MARKET RESPONSE

The financial services sector is moving most quickly to comply with the cyber security requirements laid out in the 2017 law. This is partly because they have the largest budget available for IT-related operations, and partly because competition among financial service providers in Albania has pivoted to competition over IT-related services, such as bank access, money transfers and retail payments via mobile phone. The compliance requirements spelled out by NAECCS also provided a strong incentive, since it focused early on financial institutions as critical service providers who needed to move quickly to come into compliance with cyber security requirements.

Figure 2. Information security market systems map



The market system map (Figure 2) illustrates the emerging dynamic in the Albanian information security market. Regulatory pressure (blue lines) from NAECCS acted as a market trigger, influencing businesses (green boxes) and public sector agencies (dark blue box) to demand the services of IT security consultants like InfoSecurity and certification bodies like LegalCert (grey boxes). In this map, green lines illustrate payments between actors, black lines illustrate service provision, and red lines illustrate the transfer of key information.

In some cases, international banks with branches in Albania had already made significant steps toward ISO 27001 compliance and in information security systems – especially those banks with EU-based headquarters, where cybersecurity and data privacy laws had already caused them to put strong safeguards in place. But even in those circumstances, their Albanian branches had lagged somewhat behind the mother offices. However, rather than using local providers, some international banks brought preferred certification auditors, such as the 'Big 4' accounting firms – KPMG, PwC, Deloitte and Ernst & Young – who were contracted in lieu of Albanian actors like InfoSecurity and who generally hired non-Albanian experts to conduct the audits, limiting employment opportunities for Albanians and hiking up prices.

For Albanian banks, however, **InfoSecurity and LegalCert are now the go-to choices for information security auditing and certification**. All financial institutions in Albania are moving quickly to adopt the enhanced measures that will put them in compliance with NAECCS's mandate, although at different speeds.

> **Exponential Demand Growth:** "In the first 6 months, I had no clients at all. I thought about closing the business. After the first client and the collaboration with Risi… my clients increased to 8. I hope that next year I'll double the number of clients to 16."
> ***Igli Tafa, CEO, InfoSecurity***

One of the financial services sector's early adopters is **Credins Bank**, an InfoSecurity client with a presence across Albania and a recently opened branch in neighboring Kosovo. Credins has about 60 branches and 950 employees, with 27 people in its IT department. It reached out to InfoSecurity in 2019 for help identifying the gaps it needed to fill in order to come into compliance with NAECCS requirements. This step helped Credins document its internal policies and procedures. Credins then engaged InfoSecurity to build a more robust cybersecurity system and reach compliance with ISO 27001, including setting up a unified incident management system, a vulnerability management system, and stronger information security, overall. This required a continuous engagement that lasted about a year and resulted into Credins creating a dedicated team responsible for information security. As the second largest Albanian bank in the market, these investments were necessary for Credins to maintain its competitive position in the face of strong domestic and international rivals. **Credins expects to continue hiring information security experts as it grows, while its newly certified operations also help it preserve its existing market share in Albania.**

Software development shops that serve the financial services sector are another growing source of demand for cybersecurity consulting and certifications. One example is Helios **Systems,** a 60-employee software house that builds core banking systems, e-payment applications and enterprise resource planning (ERP) tools for financial service providers and other clients in Albania, the US, Europe and Africa. One of Helios' first customers was the Albania Post, for which Helios built a banking system in 2002. In 2012 Albania Post engaged Helios again to build accounting, HR, data warehousing, e-banking and e-wallet applications.

Helios' strongest competition comes from international rivals, driving the firm to reach the same level of cybersecurity standards that its European and US-based rivals boasted.
Helios chose InfoSecurity on the basis of Mr. Tafa's background and experience in the Albanian market. Given the popularity of products like its e-wallet application, Helios specifically sought help with network security and the documentation of new policies and procedures required to demonstrate compliance with both ISO 27001 and GDPR (the latter makes it easier for Helios to compete in the EU).

InfoSecurity's support sharpened Helios' competitive edge. "[B]y investing in adding these functions and [complying with] these laws or regulations required in our products, we will be able to increase our revenue by selling to EU market," said Gjergji Mulla, Helios' CEO. **Helios has an elaborate market expansion strategy, offering services to new clients directly while also pitching its products through international consultancies like Deloitte and PWC. Its compliance with ISO 27001 is an essential part of this strategy, giving it greater market access and parity with competitors, and putting it in position to add significantly to its 60-strong workforce in the near future.**

Other sectors with increasing demand for these cybersecurity services include **hospitality** and **healthcare**. Hotels that cater to travelers from the EU are often asked to present their data protection policies, while hospitals capture vast amounts of sensitive patient information. Albania's myriad, smaller public sector agencies are also slowly moving to go through the process of complying with ISO 27001 and GDPR, though NAECCS estimates that this will be a long process.

For now, Mr. Tafa says, "We're lucky, we feel alone in this sector… [we are] definitely the only company 100% focused on cyber security." The only competition InfoSecurity faces at the moment is from international service providers, both from the Western Balkans and from further abroad, including Israeli firms. With a steadily increasing number of computers and networking systems in most industries in Albania, there will be an increased need for cyber security. InfoSecurity is confident that it has found sure footing in the Albanian market.

In the near future, a very promising sign for Risi (if not necessarily for InfoSecurity) will be **when new local competitors arise in the market in response to increased demand.** Risi helped the first one build its capacity and market itself, experimenting with the market for this new set of services. New entrants will prove the attractiveness of the market – in market systems terms, this will qualify as "crowding in," a sure sign that fundamental changes in the market system are underway.

6 LESSONS AND CONCLUSION

In conclusion, Risi's work supporting the information security market system yields four lessons for market systems projects:

1

Adaptability – Risi's adaptive approach helped it test its assumptions and find stronger leverage points as it came to understand the information security market better

Starting with the market triggers provided by the government's new information security rules, Risi at first operated under the assumption that helping the government build out and publicize information security regulations that mandated investment would be enough to spur significant changes in the private sector. It quickly learned, however, that the companies that needed to comply with the new rules needed guidance and services that would help them achieve that goal. In other words, **the Risi team quickly realized that success was not as simple as they thought it would be at the beginning of the intervention, so they quickly pivoted to focus on the supporting services** (provided by InfoSecurity and LegalCert) that would help industry players establish strong information security protections.[1]
"It's not just the enabling environment" that needs support, according to Risi staff, "you also need to build capacity in the system to help actors come into compliance with new regulations."

2

Targeting – Targeting – Risi's sharp, well-targeted and opportunistic activity took advantage by strengthening and enforcing the regulatory framework to create jobs. It also quickly identified two key leverage points (LegalCert and InfoSecurity) that could accelerate change in the market, without undermining the market for these services.

Many development projects that focus on access to new services automatically look to lower the cost of accessing those services at the same time, assuming that market actors will be unwilling to pay the full price for something they had not previously experienced. However, Risi resisted the common urge to subsidize client access to the services it supported. If it had subsidized LegalCert's and InfoSecurity's services, through vouchers or a similar scheme, it may have created the appearance of faster uptake, but it also could have harmed the market's appreciation of the real price of the services. Instead, **Risi stood quietly behind NAECCS, LegalCert and InfoSecurity and allowed the market to develop organically.** While this approach may be slower to show results than an uptake scheme fueled by donor subsidies, it promises a more sustainable change in the market system, in the long run. Risi partners have contributed to the creation of new jobs as their clients were able to attract new customers or retain existing business, as shown below:

[1]A related Helvetas blog by Risi staff also makes this point clearly, see: https://www.helvetas.org/en/switzerland/how-you-can-help/follow-us/blog/inclusive-systems/spotting-and-grabbing-opportunities

3

Pivoting from Labor Demand to Supply – Risi is putting in place the elements of an ecosystem that can sustain its own growth

With a strong regulatory function and high-capacity service providers in place, Risi is confident that it has supported long-term actors in the information security market system to sustainably transition vital sectors of the Albanian economy toward international compliance with cybersecurity and data privacy standards. The project's 2020 midterm review, conducted by an external consultant, agrees with this belief, observing that these services are "sustainable and likely to reach scale."

It also noted that the one missing piece was an "insufficient supply of cybersecurity/GDPR specialists," which the project would address "by supporting development of a cybersecurity course with one of its Outcome 3 partners." Thus, the third intervention (supporting formal and non-formal trainers) is the last complementary piece of the broader information security puzzle. When this concept note was written, Risi was pivoting to focus on building, on a large scale, the human capital development capacity needed to staff these positions. **This pivot toward skills development would also constitute Risi's major contribution to in the information security market**, now that it had laid the conditions for a huge increase in demand for these skills.

Risi Partner	Number of Jobs Reported as of 2020	Expected jobs by end of 2021
NAECCS	16[i]	30
Infosecurity	25	45
Legalcert	36	60
Total	77	135

[i]This is the number of jobs created in the private sector, while there were 17 new jobs created in the public sector, which Risi does not include in its results because its logframe indicators consider only jobs created in private sector.