**BIT Risk Management Report**

**Group 17**

**Monstrosity Inc. Network**

rev. 3/15/2020

**Team Members**

Ryan Shepherd

Andrew Taylor

Liam Floyd

Document Control

**Change History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Change Date** | **Completed by** | **Description of changes** |
| V1.0 | 3/15/2020 | RS, AT, FL | Initial baseline release |
|  |  |  |  |

**Document Storage**

This document is stored in the project’s repository at: <https://github.com/umkc-cs-451-2020-spring/semester-project-group-17>

**Document Owner**

Ryan Shepherd is responsible for maintaining this document. Ryan Shepherd, Andrew Taylor, and Liam Floyd are responsible for updating this document.**Table of Contents**

**TABLE OF CONTENTS****3**

[**1**](#_3znysh7) **OVERVIEW 4**

[**1.1 Purpose and Scope 4**](https://docs.google.com/document/d/1v3zfw3C-j67FhjSSlj-h5J4gQ3V5ulg1pER7lm29qdI/edit#heading=h.23ckvvd)

[**1.2 Goals and Objectives 4**](https://docs.google.com/document/d/1v3zfw3C-j67FhjSSlj-h5J4gQ3V5ulg1pER7lm29qdI/edit#heading=h.ihv636)

[**1.3 Project Deliverables 5**](#_4d34og8)

[**1.4 Assumptions and Constraints**](https://docs.google.com/document/d/1v3zfw3C-j67FhjSSlj-h5J4gQ3V5ulg1pER7lm29qdI/edit#heading=h.32hioqz) **5**

**1.5 Definitions 6**

[**2 Risk Summaries**](https://docs.google.com/document/d/1v3zfw3C-j67FhjSSlj-h5J4gQ3V5ulg1pER7lm29qdI/edit#heading=h.41mghml) **7**

[**2.1**](https://docs.google.com/document/d/1v3zfw3C-j67FhjSSlj-h5J4gQ3V5ulg1pER7lm29qdI/edit#heading=h.26in1rg) **Priority High Risk 7**

**2.2 Priority Medium Risk 10**

**3.3 Priority Low Risk 11**

[**3 Risk Exposure**](https://docs.google.com/document/d/1v3zfw3C-j67FhjSSlj-h5J4gQ3V5ulg1pER7lm29qdI/edit#heading=h.z337ya) **13**

[**3**](https://docs.google.com/document/d/1v3zfw3C-j67FhjSSlj-h5J4gQ3V5ulg1pER7lm29qdI/edit#heading=h.3j2qqm3)**.1 High Exposure 13**

**3.2 Medium Exposure 13**

**3.3 Low Exposure 14**

**4** [**Risk**](https://docs.google.com/document/d/1v3zfw3C-j67FhjSSlj-h5J4gQ3V5ulg1pER7lm29qdI/edit#heading=h.z337ya) **Response Plan 14**

**4.1 Server Overheating 14**

**4.2 Hardware Failure 15**

# **Overview**

## *Purpose and Scope*

This document outlines the anticipated risks in implementing the requirements set forth in the design of the information technology infrastructure for Monstrosity Inc., its employees, and customers. The purpose of this document is to present the risks the project team may encounter during the design iterations. These risks also include inherent risks the client, Monstrosity Inc, will encounter. The purpose of this report is to make known how impactful these risks are as well as how to handle the risk should it arise.

Monstrosity Inc. has contracted with our firm to design and recommend an infrastructure package that will provide high-speed wireless internet connectivity for their employees and customers, access to apps such as secure email, and a database system to manage the real estate companies information. This system will be used by approximately 200 employees of Monstrosity Inc. as well as its customers and will have to be implemented in 5 satellite offices and 1 corporate office.

This document doesn’t address the requirements of the project in detail as this is addressed in a separate project document. Additionally, this document does not address detailed user interface implementation which would be accomplished at the software level.

It is important to note that this is not an exhaustive list of all the risks this project may encounter. Some scenarios are unforeseen or will be developed as more information becomes known. It is up to the design team, Monstrosity Inc management, and IT professionals to update this report frequently as risk reduction plans can save the company money, time, and resources.

## *Goals and Objectives*

Our project goal is to research, design, and propose the infrastructural solution to the technical needs of Monstrosity Inc which includes designing the following objectives:

1. secure network with intrusion detection, as well as wireless internet services for employees and customers,
2. cloud services hosting for secure email,
3. onsite database hosting infrastructure.

We will complete this over the course of 5 planning and design iterations that will end with the final proposal being presented by May 4, 2020. A 6th iteration will cover the physical build-out and will take place after this project has been completed and approved by stakeholders. This infrastructure will give Monstrosity Inc employees consistent access to company tools and digital resources across its many locations and while out in the field, thus allowing employees to be more productive, knowledgeable, and effective in their jobs. Additionally, from a customer experience perspective, customers will benefit from limited internet access

## *Project Deliverables*

This section lists the outputs of the project that will be delivered to Monstrosity Inc.

The following design items and their implementation recommendations will be delivered to the customer on or before 5/4/2020 as a proposal document:

1. The network infrastructure spanning across all offices
2. The database infrastructure, fully connected to the network
3. Customers and Employees have access to the internet with varying permissions for access
4. A comparison of cloud hosting platforms and a recommendation of which platform will best fit Monstrosity Inc’s requirements.
5. A document detailing how security will be maintained for the product
6. Network (and other necessary infrastructure) diagrams
7. Any necessary configuration considerations
8. Hardware recommendations that will be necessary to implement the product
9. Other general recommendations

## *Assumptions and Constraints*

Assumptions:

1. It is assumed that Monstrosity Inc is a local real estate company with all offices residing in the same state, managing several properties that are for sale to the public and businesses.
2. Monstrosity Inc is being considered a small to medium-sized business.
3. It is assumed that Monstrosity has a limited budget, characteristic of a small/medium real estate company. For example, they may look more to hosted services instead of building extensively in house applications and on-prem infrastructure.
4. It is assumed that this project will be treated as a simulation of a “real-world” scenario, making decisions based on considerations of likely consequences in a practical implementation.
5. Due to the technical nature of physical infrastructure (hardware configurations), the average user (customers, managers, employees) will not be able to manage this system should problems arise and that Monstrosity Inc will likely need to contract with a third party IT support professional who will be on-call to provide maintenance and assistance with operations.

Constraints:

1. We are designing a network layout for a purely hypothetical company with no actual finances, existing infrastructure, or offices.
2. With no offices, we must rely heavily on assumptions developed by the team.
3. We are also operating as a group for a school project, giving limited time with schedules involving work, other courses, and more.
4. Operating with no defined financial constraints of the infrastructure. In general, we will try to keep the costs to a minimum as to what we feel would be logical costs/budget constraints of a business of this size.
5. As students, we have limited experience and knowledge in applying architectural design and will require research to complete this project. All variables that would affect a real-world design such as this may not be considered due to inexperience.
6. As a hypothetical company with no ability for physical implementation, testing designs is limited.
7. The database system will be based on MySQL.
8. The system will need to be accessible from a variety of devices (desktops, laptops, tablets, phones, etc) that run on various operating systems (Windows, Mac, Android, etc).
9. Due to the technical nature of physical infrastructure (hardware configurations), the average user (customers, managers, employees) will not be able to manage this system should problems arise.

## *Definitions*

## This section defines potentially unfamiliar or ambiguous words, acronyms, and abbreviations.

**Team/Design Team** - refers to the design team of Ryan Shepherd, Andrew Taylor, and Liam Floyd.

**On-Prem** - “on-premises”, infrastructure that is on-prem will be hosted physically on-site at the physical location opposed to hosted in the cloud through a third-party provider.

**TBD** - To be determined. When used in this document, this refers to material facts or decisions that will need to be made at a later date and will be added to this document as an addendum.

**Component** - the features of the product/system that is being designed. The system is being divided into the following components:

1. Network Infrastructure
2. Database and Server infrastructure
3. Security Infrastructure
4. Cloud Hosting Infrastructure

**Prototype** - a high-level, early draft of the implementation of the product components. This prototype will give stakeholders a general idea of the implementation.

**Use case** – describes a goal-oriented interaction between the system and an actor. A use case may define several variants called scenarios that result in different paths through the use case and usually different outcomes.

**Actor** – user or another system that receives value from a use case.

**Product** – what is being described here; the system specified in this document.

**Project** – activities that will lead to the production of the product described here. Project issues are described in a separate project plan.

**Shall** – adverb used to indicate importance; indicates the requirement is mandatory. “Must” and “will” are synonyms for “shall”.

**Should** – adverb used to indicate importance; indicates the requirement is desired but not mandatory.

**May** – adverb used to indicate an option. For example, “The system may be taken offline for up to one hour every evening for maintenance.” Not used to express a requirement, but rather to specifically allow an option.

**ISP** - Internet service provider, a third party company that will provide the infrastructure needed to access and utilize internet capabilities

**IT Professional** - It is assumed that Monstrosity INC will not have a full time IT manager on staff to maintain the system and that this will be contracted out to a third party who will be on-call.

**Cloud Service Provider** - A third party provider who maintains and manages their own data center who provides cloud services to the public

**Network** - refers to the physical infrastructure of a group of two or more computer systems linked together. There are many types of computer networks, including Local Area Networks (LAN), Wireless Internet (wifi), and Wide Area Networks (WAN).

**SLA** - Service Level Agreement. A service-level agreement is a commitment between a service provider and a client. Particular aspects of the service – quality, availability, responsibilities – are agreed between the service provider and the service user. As used in this document, SLA’s refer to agreements between the cloud service provider and Monstrosity Inc.

**UI** - User interface. Any number of front-end software that will allow users to interact with the system.

# **Risk Summaries**

* 1. High-Risk Priority
     1. Risk: Overheating of the server cluster
* Priority: high
* Probability of turning into a problem: 90%
* Consequences of risk turning into a problem: Fire, a shutdown of systems, loss of access to resources, company costs to loss of productivity, costs to repair/replace hardware, data loss
* Actions to minimize risk: Mitigate risk
* Contingency plan: Implement industry-standard cooling systems to keep equipment at correct operating temperatures. Engage IT professionals ASAP if downtime occurs to repair equipment
  + 1. Risk: Hardware failure
* Priority: High
* Probability of turning into a problem: 85%
* Consequences of risk turning into a problem: Loss of access to system resources, employee downtime and decreased productivity, increased costs to repair or replace hardware.
* Actions to minimize risk: Accept
* Contingency plan: Contact IT professionals to repair failures ASAP
  + 1. Risk: Design team being inexperienced in architecture design
* Priority: High
* Probability of turning into a problem: 80%
* Consequences of risk turning into a problem: Bad grade, incorrect final recommendations in proposal leading to additional costs, lowered productivity, and increased time to rectify any problems
* Actions to minimize risk: Buy information
* Contingency plan: Ask questions of sponsor and stakeholders when anything is unclear, present multiple options to solve problems, discuss as a team to come to a consensus on decisions. Conduct complete and thorough research.
  + 1. Risk: Viruses, phishing, other malicious acts contracted through email
* Priority: High
* Probability of turning into a problem: 75%
* Consequences of risk turning into a problem: Loss of access to systems, confidentiality breaches, unauthorized access to resources, employee downtime and reduced productivity, costs to repair damage
* Actions to minimize risk: Mitigate risk, Transfer risk, avoid the risk
* Contingency plan: Have secure systems in place that will automatically detect and protect the system from malicious software. Have a robust firewall system in place. Have email security drills to educate employees on these risks and how to avoid them. Engage IT to support professionals to repair the damage.
  + 1. Risk: Design team goes past schedule
* Priority: High
* Probability of turning into a problem: 70%
* Consequences of risk turning into a problem: Increased costs exceeding budget
* Actions to minimize risk: Buy Information, Accept, Mitigate, Transfer
* Contingency plan: Adhere to deadlines and engage consultants as available to ensure timely completion
  + 1. Risk: Design team goes over budget
* Priority: high
* Probability of turning into a problem: 70%
* Consequences of risk turning into a problem: Requires executive decision to continue the project or make trade-offs to lower costs
* Actions to minimize risk: Buy information, Accept, Mitigate
* Contingency plan: Adhere to deadlines, conduct complete and accurate research to recommend the best solutions to stay within budget, research alternative solutions.
  + 1. Risk: Unauthorized access within the system
* Priority: High
* Probability of turning into a problem: 50%
* Consequences of risk turning into a problem: Data integrity changed producing incorrect information being used in decision making, systems being held hostage for ransom, access to confidential information causing the company legal problems, etc
* Actions to minimize risk: Avoid Risk
* Contingency plan: Set up stringent access control systems to avoid risk. Once there is unauthorized access, have IT professionals follow a plan that details action steps to remedy the problem (for example, change passwords and rectify the hole in the system when access was gained)
  + 1. Risk: Design team does not perform adequate research
* Priority: high
* Probability of turning into a problem: 50%
* Consequences of risk turning into a problem: Any number of various problems could result, some foreseen and some unexpected. For example, possible compromised system security, loss of productivity, additional costs to rectify holes in the system, increased time to fix the issues, etc
* Actions to minimize risk: Mitigate risk
* Contingency plan: Perform complete research, research multiple alternative recommendations, engage consultants and other resources to verify accuracy
  + 1. Risk: Design team does not propose an optimal implementation recommendation in the final report
* Priority: high
* Probability of turning into a problem: 50%
* Consequences of risk turning into a problem: Any number of various problems could result, some foreseen and some unexpected. For example, possible compromised system security, loss of productivity, additional costs to rectify holes in the system, increased time to fix the issues, etc
* Actions to minimize risk: Mitigate risk
* Contingency plan: Perform complete research, research multiple alternative recommendations, engage consultants and other resources to verify accuracy
  + 1. Risk: Compromised private data
* Priority: High
* Probability of turning into a problem: 50%
* Consequences of risk turning into a problem: Possible legal ramifications of disclosure of confidential information, increased costs to rectify the problem.
* Actions to minimize risk: Mitigate risk
* Contingency plan: Implement a full security suite of tools/systems that will detect and prevent unauthorized access before it happens. Once there is unauthorized access, have IT professionals follow a plan that details action steps to remedy the problem (for example, change passwords and rectify the hole in the system when access was gained)
  + 1. Risk: Unauthorized access to the system
* Priority: High
* Probability of turning into a problem: 40%
* Consequences of risk turning into a problem: Data integrity changed producing incorrect information being used in decision making, systems being held hostage for ransom, access to confidential information causing the company legal problems, etc
* Actions to minimize risk: Mitigate risk
* Contingency plan: Implement a full security suite of tools/systems that will detect and prevent unauthorized access before it happens. Once there is unauthorized access, have IT professionals follow a plan that details action steps to remedy the problem (for example, change passwords and rectify the hole in the system when access was gained)
  + 1. Risk: Database misuse
* Priority: High
* Probability of turning into a problem: 40%
* Consequences of risk turning into a problem: Incorrect or inconsistent information being in database results in lowered employee performance which will impact the service their customers receive
* Actions to minimize risk: Mitigate risk
* Contingency plan: Have access control systems in place to control various levels of authorized access to make changes to the database. Have employees and managers trained on how to use the database correctly. Have an easy to use and intuitive front end UI for users of the database.
  1. Medium-Risk Priority
     1. Risk: Vague project details (specifications and client requirements) leading to incorrect assumptions
* Priority: Medium
* Probability of turning into a problem: 70%
* Consequences of risk turning into a problem: Incorrect assumptions leading to wrong proposal recommendations resulting in increased costs to rectify, reduction in security, efficiency reduction, and decreased productivity.
* Actions to minimize risk: Buy information
* Contingency plan: Ask questions of sponsor and stakeholders when anything is unclear, present multiple options to solve the problem, discuss as a team to come to a consensus on decisions
  + 1. Risk: Miscommunication within the design team
* Priority: medium
* Probability of turning into a problem: 40%
* Consequences of risk turning into a problem: Any number of various problems could result, some foreseen and some unexpected. For example, possible compromised system security, loss of productivity, additional costs to rectify holes in the system, increased time to fix the issues, etc
* Actions to minimize risk: Mitigate risk, accept the risk
* Contingency plan: Conduct regularly scheduled meetings and progress reviews to make sure everyone is on the same page.
  + 1. Risk: Monstrosity Inc reduces budget
* Priority: Medium
* Probability of turning into a problem: 25%
* Consequences of risk turning into a problem: Increased project time as changes to requirements will affect proposal outcomes, increased costs due to increased project timelines requiring additional time spent on project re-working what has been completed, loss of quality of a robust system
* Actions to minimize risk: Accept the risk
* Contingency plan: Have this risk in mind from the beginning when doing research and be prepared to implement alternative system recommendations.
  + 1. Risk: Fire
* Priority: Medium
* Probability of turning into a problem: 20%
* Consequences of risk turning into a problem: Damage to equipment and facilities, rendering equipment unusable and costs to replace equipment and costs due to downtime of resources.
* Actions to minimize risk: Mitigate risk
* Contingency plan: Implement fire control systems (sprinklers) to put out the fire if it takes place. Avoid risk as much as possible by following industry standards of cooling systems and electrical systems safety standards.
  + 1. Risk: Monstrosity Inc cancels the project
* Priority: Medium
* Probability of turning into a problem: 20%
* Consequences of risk turning into a problem: Wasted time and costs of the design team and Monstrosity Inc, increased exposure to risks of maintaining the current system
* Actions to minimize risk: Accept the risk
* Contingency plan: Close the project and turn what has been completed over to Monstrosity Inc.
  1. Low-Risk Priority
     1. Risk: Internet failure (ISP related)
* Priority: Low
* Probability of turning into a problem: 20%
* Consequences of risk turning into a problem: System will go down with no access to resources across sites, decreased employee productivity
* Actions to minimize risk: Accept the risk
* Contingency plan: Contact ISP and Network Management company to resolve the problem ASAP
  + 1. Risk: Power Failure
* Priority: Low
* Probability of turning into a problem: 20%
* Consequences of risk turning into a problem: Loss of data, loss of access to resources, decreased employee productivity
* Actions to minimize risk: Avoid risk
* Contingency plan: Have a backup power system in place that will kick in automatically and secure a backup of data resources
  + 1. Risk: Cloud service provider changes terms of service
* Priority: low
* Probability of turning into a problem: 15%
* Consequences of risk turning into a problem: Increased costs, loss of services, decreased employee productivity
* Actions to minimize risk: Buy information
* Contingency plan: Fully research and understand the services that cloud service providers do and do not provide. Have contracts in place to ensure a consistent level of agreed-upon services
  + 1. Risk: Monstrosity Inc changes requirements to project
* Priority: Low
* Probability of turning into a problem: 10%
* Consequences of risk turning into a problem: Increased project time as changes to requirements will affect proposal outcomes, increased costs due to increased project timelines requiring additional time spent on project re-working what has been completed, loss of quality of a robust system
* Actions to minimize risk: Accept the risk
* Contingency plan: Have this risk in mind from the beginning when doing research and be prepared to implement alternative system recommendations.

# **Risk Exposure**

* 1. High Risk

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rank | Risk | Probability | Size of Loss (1-10) | Risk Exposure |
| 1 | Server cluster overheating | 90% | 10 | 9.0 |
| 2 | Hardware failure | 85% | 10 | 8.5 |
| 3 | Design team being inexperienced in architecture design | 80% | 3 | 2.4 |
| 4 | Viruses, phishing and other malware | 75% | 4 | 3.0 |
| 5 | Design team goes past schedule | 70% | 3 | 2.1 |
| 6 | Design team goes over budget | 70% | 3 | 2.1 |
| 7 | Unauthorized access within the system | 50% | 4 | 2.0 |
| 8 | The design team does not perform adequate research | 50% | 3 | 1.5 |
| 9 | The design team does not propose an optimal implementation recommendation in the final report | 50% | 3 | 1.5 |
| 10 | Compromised confidential data | 50% | 5 | 2.5 |
| 11 | Unauthorized access to the system (external attack) | 40% | 4 | 1.6 |
| 12 | Database Misuse | 40% | 1 | 0.4 |

* 1. Medium Risk

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rank | Risk | Probability | Size of Loss (1-10) | Risk Exposure |
| 1 | Vague project details leading to incorrect assumptions | 70% | 5 | 3.5 |
| 2 | Miscommunication within the design team | 40% | 2 | 0.8 |
| 3 | Monstrosity reduces budget | 25% | 3 | 0.75 |
| 4 | Fire | 20% | 9 | 1.8 |
| 5 | Monstrosity cancels the project | 20% | 6 | 1.2 |

* 1. Low Risk

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rank | Risk | Probability | Size of Loss (1-10) | Risk Exposure |
| 1 | Internet failure (ISP related) | 20% | 7 | 1.4 |
| 2 | Power Failure | 20% | 5 | 1.0 |
| 3 | Cloud service provider changes terms of service | 15% | 2 | 0.3 |
| 4 | Monstrosity Inc changes requirements to project | 10% | 4 | 0.4 |

# **Risk Response Plan**

* 1. Servers overheating

|  |  |  |
| --- | --- | --- |
| Risk ID: 2.1.1 | Title: Server’s overheating | Origination Date: 3/8/2020 |
| Status: (identified, assessed, planned, contingent, problem, crisis, resolved, closed) Planned | | Originator: Ryan Shepherd |
| Description: Servers generate a lot of heat and if not properly cooled, they will overheat and shutdown. Cooling systems must maintain functional at all times. | | Assessment: High Risk |
| Probability: 90% |
| Consequences: Servers shutting down, disabling resources for employees and possibly customers. There is potential for damage to hardware requiring repairs/replacement There would be costs to time, money, and productivity |
| Risk Exposure: 9.0 (out of 10) |
| Owner: IT Support Professional | | |
| Risk Response Alternatives:  Accept risk - overheating is a risk that is guaranteed to happen  Mitigate - we can mitigate the risk by implementing and maintaining industry-standard cooling systems | | |
|
|
|
| Risk Response Plan (Activities and Milestones): design and install efficient cooling systems. If there is a failure in the cooling system, IT Support Professionals will engage redundancy systems and shut down the server to prevent overheating and damage to systems. Next step would be to engage emergency repair procedures to repair the cooling system | | |
| Date | Actions | Responsibilities |
| 3/15/2020 | Establish risk response | The project manager will define the high-level plan needs |
| 6/1/2020 | Establish a contract with IT, Support Professionals | Monitor system performance and engage repair action when there is an incident |
| 6/15/2020 | Purchase and Install the cooling system from the vendor | Install the industry-standard cooling system to spec |
| Plan Status: Initiated | | |
| Date | Status | |
| 3/15/2020 | The high-level plan has been described by PM. Implementation details need to be resolved. | |
|  |  | |
| Resources: IT Support Professional, Cooling system repair, Cooling system installers | | |
|
|

* 1. Hardware Failure

|  |  |  |
| --- | --- | --- |
| Risk ID: 2.1.2 | Title: Hardware failure | Origination Date:3/8/2020 |
| Status: (identified, assessed, planned, contingent, problem, crisis, resolved, closed) | | Originator: Ryan Shepherd |
| Description: There is a lot of hardware involved in keeping networks and servers running. Sometimes hardware can fail for multiple reasons, but when they do, the servers or network can go down. Backups, failover, and redundancy must be in place in case this happens. Commonly failing parts like memory and HDD’s should be kept on hand to replace promptly | | Assessment: High Priority |
| Probability: 85% |
| Consequences: Loss of access to system resources.Server shutting down, Network shutting down, loss of data, costs to time money and productivity. Costs to replace /repair hardware |
| Risk Exposure: 8.5 |
| Owner: IT Support Professional | | |
| Risk Response Alternatives:  Acceptance: accept that hardware will fail at random times and fix the issues as soon as possible  Mitigate: have backup systems, failover systems, redundancy systems, and available extra hardware in place  Transfer: For the Network, the responsibility can be transferred to Windstream | | |
|
|
|
| Risk Response Plan (Activities and Milestones): Install redundancy and failover systems, purchase extra hardware (ie memory, fans, hdd’s) to keep on hand, engage IT Support professional to repair or hire technicians to repair extensive damage | | |
| Date | Actions | Responsibilities |
| 3/15/2020 | Establish risk response | The project manager will define the high-level plan needs |
| 6/1/2020 | Establish a contract with IT Support Professionals | Monitor system performance and engage repair action when there is an incident |
| 6/15/2020 | Purchase and Install the failover and redundancy systems | Install the industry-standard failover and redundancy systems |
| Plan Status: Initiated | | |
| Date | Status | |
| 3/15/2020 | The high-level plan has been described by PM. Implementation details need to be resolved. | |
|  |  | |
| Resources: IT Support Professional, Cooling system repair, Cooling system installers | | |
|
|